

Министерство науки и высшего образования Российской Федерации
 федеральное государственное бюджетное образовательное учреждение высшего образования
**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
 ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И ДИЗАЙНА»**

УТВЕРЖДАЮ
 Первый проректор, проректор по учебной
 работе

_____ А.Е. Рудин
 «30» июня 2020 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.22 <small>(Индекс дисциплины)</small>	Защита информации в компьютерных системах <small>(Наименование дисциплины)</small>
Кафедра: 20 <small>Код</small>	Интеллектуальных систем и защиты информации <small>Наименование кафедры</small>
Направление подготовки:	10.03.01 Информационная безопасность Безопасность компьютерных систем (в коммерческих структурах)
Профиль подготовки:	структурах)
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	288		
	Аудиторные занятия	153		
	Лекции	68		
	Лабораторные занятия	34		
	Практические занятия	51		
	Самостоятельная работа	99		
	Промежуточная аттестация	36		
Формы контроля по семестрам (номер семестра)	Экзамен	6		
	Зачет	5		
	Контрольная работа			
	Курсовой проект (работа)	5		
Общая трудоемкость дисциплины (зачетные единицы)		8		

Форма обучения:	Распределение зачетных единиц трудоемкости по семестрам											
	1	2	3	4	5	6	7	8	9	10	11	12
Очная					3	5						
Очно-заочная												
Заочная												

Программа государственной итоговой аттестации составлена в соответствии с федеральным
государственным образовательным стандартом высшего образования
по соответствующему направлению подготовки

и на основании учебного плана № 1/1/704

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

Сформировать компетенции обучающегося в области защиты информации в компьютерных системах

1.3. Задачи дисциплины

- Рассмотреть базовые дискреционные модели безопасности
- Рассмотреть базовую модель изолированной программной среды
- Рассмотреть базовые мандатные модели безопасности
- Рассмотреть базовые модели ролевого управления доступом
- Рассмотреть базовые модели безопасности информационных потоков
- Рассмотреть различные ДП-модели

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

Код компетенции	Формулировка компетенции	Этап формирования
ОПК-7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Второй
Планируемые результаты обучения Знать: 1) Предмет и объект защиты Уметь: 1) Анализировать угрозы информационной безопасности в компьютерных системах Владеть: 1) Средствами и системами аудита информационной безопасности		
ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты	Второй
Планируемые результаты обучения Знать: 1) Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе Уметь: 1) Сегментировать элементы администрируемой сети Владеть: 1) Навыками установки специализированных программных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа		
ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Второй
Знать: Виды и формы функционирования вредоносного программного обеспечения Уметь: Обосновывать правила безопасной эксплуатации программного обеспечения Владеть: навыками проведения организационных технических и программных мероприятий по защите информации		

Код компетенции	Формулировка компетенции	Этап формирования
ПК-12	Способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Второй
Планируемые результаты обучения		
Знать:		
1) Виды политик управления доступом и информационными потоками в компьютерных сетях		
Уметь:		
1) Выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях		
Владеть:		
1) навыками контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях		

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

- Информатика (ОПК-7)
- Сети и системы передачи информации (ПК-3)
- Основы информационной безопасности (ПК-12)

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Модели дискреционного управления доступом			
Тема 1. Основные понятия и определения	4		
Тема 2. Модели ХРУ	6		
Тема 3. Модель типизированной матрицы доступов	5		
Тема 4. Модель Take-Grant	5		
Тема 5. Расширенная модель Take-Grant	5		
Текущий контроль 1 (опрос)	1		
Учебный модуль 2. Модели ИПС и мандатного управления доступом			
Тема 6. Субъектно-ориентированная модель ИПС	4		
Тема 7. Модели Белла-ЛаПадулы	9		
Тема 8. Модель СВС	8		
Текущий контроль 2 (опрос)	1		
Учебный модуль 3. Безопасность информационных потоков и ролевое управление доступом			
Тема 9. Автоматная, программная и вероятностная модели безопасности информационных потоков	5		
Тема 10. Базовая модель ролевого управления доступом	8		
Тема 11. Модель администрирования ролевого управления доступом	9		
Тема 12. Модель мандатного ролевого управления доступом	6		
Курсовая работа	30		
Промежуточная аттестация по дисциплине (зачет)	2		
Учебный модуль 4. Базовая и ИПС ДП-модели			
Тема 13. Базовая ДП-модель	14		
Тема 14. ДП-модель без кооперации доверенных и недоверенных субъектов	8		
Тема 15. ФАС ДП-модель	10		
Тема 16. ПБА и ПАР ДП-модели	7		
Тема 17. ФПАС-модель	9		
Тема 18. Применение ФАС ДП-модели для анализа безопасности веб-систем, ФС ДП-модель	8		
Тема 19. Методы предотвращения утечки пав доступа в реализации запрещенных информационных потоков	6		

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Текущий контроль 4 (опрос)	1		
Учебный модуль 5. Мандатная ДП-модель и ДП-модели безопасности информационных потоков			
Тема 20. Правила преобразования мандатной ДП-модели	9		
Тема 21. Безопасность в смысле Белла-ЛаПадулы и условия повышения субъектом уровня доступа	10		
Тема 22. ДП-модель с блокирующими доступами доверенных субъектов	8		
Тема 23. Мандатная ДП-модель с блокирующими доступами доверенных субъектов и с отождествлением порожденных субъектов	9		
Тема 24. Мандатная ДП-модель КС, реализующих политику строгого мандатного управления доступом	9		
Текущий контроль 5 (опрос)	1		
Учебный модуль 6. Мандатная сущностно-ролевая ДП-модель			
Тема 25. Состояние системы МРОСЛ	8		
Тема 26. Параметризация модели МРОСЛ	9		
Тема 27. Задание мандатного управления доступом и контроля целостности для состояний системы МРОСЛ	9		
Тема 28. Правила преобразования состояний МРОСЛ	8		
Текущий контроль 6 (опрос)	1		
Промежуточная аттестация по дисциплине (экзамен)	36		
ВСЕГО:	288		

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	4				
8	5	4				
9	5	2				
10	5	4				
11	5	4				
12	5	4				
13	6	4				
14	6	2				
15	6	2				
16	6	2				
17	6	2				
18	6	2				
19	6	2				
20	6	2				
21	6	2				
22	6	2				
23	6	2				
24	6	2				
25	6	2				
26	6	2				
27	6	2				
28	6	2				

Номера изучаемых тем	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
ВСЕГО:		68				

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	Решение задач на математические основы моделей безопасности (практическое занятие)	5	1				
2	Построение и использование моделей ХРУ (практическое занятие)	5	1				
3	Построение и использование моделей ТМД (практическое занятие)	5	1				
4	Построение и использование модели Take-Grant (практическое занятие)	5	1				
5	Построение и использование расширенной модели Take-Grant (практическое занятие)	5	1				
6	Построение и использование модели ИПС (практическое занятие)	5	1				
7	Построение и использование модели Белла-ЛаПадулы (практическое занятие)	5	2				
8	Построение и использование модели СВС (практическое занятие)	5	2				
9	Построение и использование модели безопасности информационных потоков (практическое занятие)	5	1				
10, 11	Построение и использование модели ролевого управления доступом (практическое занятие)	5	4				
12	Построение и использование модели мандатного ролевого управления доступом (практическое занятие)	5	2				
13, 14	Построение и использование базовой ДП-модели (практическое занятие)	6	6				
15, 16	Построение и использование ФАС ДП-модели (практическое занятие)	6	4				
17, 18	Построение и	6	4				

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)
	использование ФПАС-модель (практическое занятие)						
19	Построение и использование ФС ДП-модели (практическое занятие)	6	2				
20, 21	Решение задач преобразований мандатной ДП-модели (практическое занятие)	6	4				
22, 23, 24	Построение и использование ДП-моделей безопасности информационных потоков (практическое занятие)	6	6				
25, 26	Построение и использование системы МРОСЛ (практическое занятие)	6	4				
27, 28	Решение задач на правила преобразования состояний МРОСЛ (практическое занятие)	6	4				
ВСЕГО:			51				

3.3. Лабораторные занятия

Номера изучаемых тем	Наименование лабораторных занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
2, 3	Решение задач модели ХРУ	5	3				
4, 5	Решение задач моделей Take-Grant	5	3				
7, 8	Решение задач моделей с мандатным управлением доступом	5	4				
9, 10, 11	Решение задач моделей безопасности информационных потоков	5	4				
12	Решение задач моделей с ролевым управлением доступом	5	3				
13	Решение задач базовой дискреционной ДП модели	6	3				
15, 17	Решение задач ДП-моделей ИПС	6	3				
20, 21	Решение задач мандатной ДП-модели	6	3				
22, 23, 24	Решение задач ДП-моделей безопасности информационных потоков	6	4				
25, 26, 27, 28	Решение задач модели МРОСЛ	6	4				
ВСЕГО:			34				

4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

4.1. Цели и задачи курсовой работы

Целью курсовой работы является приобретение знаний и навыков программного построения моделей информационной безопасности и анализа безопасности с их использованием.

Перед обучающимся ставятся следующие задачи:

- 1) освоить теоритические основы построения модели;
- 2) разобраться в способе анализа безопасности системы с использованием модели;
- 3) построить реализующий модель программный пакет;
- 4) создать набор тестов для проверки работоспособности программного пакета и использовать их;
- 5) сформировать отчет по проделанной работе.

4.2. Тематика курсовой работы

Работа посвящена изучению и использованию моделей безопасности компьютерных систем.

4.3. Требования к выполнению и представлению результатов курсовой работы

Работа выполняется на языке высокого уровня с использованием технологии ООП, то есть программа представляет собой пакет реализующих модель классов и тестирующих классов.

Результаты представляются в виде отчета, содержащего следующие обязательные элементы:

- титульный лист;
- задание на курсовую работу;
- описание модели безопасности и способов проверки безопасности с помощью нее;
- UML-диаграммы и листинг пакета классов, реализующих модель;
- UML-диаграммы и листинг пакета тестирующих классов;
- результаты тестирования;
- выводы по курсовой работе.

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	Опрос	5	2				
4, 5,6	Опрос	6	3				

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	4				
	6	30				
Подготовка к практическим (семинарским) и лабораторным занятиям	5	4				
	6	29				
Выполнение курсовой работы	5	30				
Подготовка к зачетам	5	2				
Подготовка к экзаменам	6	36				
	ВСЕГО:		135			

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

7.1. Характеристика видов и используемых инновационных форм учебных занятий

Наименование видов учебных занятий	Используемые инновационные формы	Объем занятий в инновационных формах (часы)		
		очное обучение	очно-заочное обучение	заочное обучение
Лекции	Лекция-беседа	10		

Наименование видов учебных занятий	Используемые инновационные формы	Объем занятий в инновационных формах (часы)		
		очное обучение	очно-заочное обучение	заочное обучение
Практические и семинарские занятия	Занятия в группах, анализ проблемных ситуаций	10		
Лабораторные занятия	Занятия в группах	10		
ВСЕГО:		30		

7.2. Балльно-рейтинговая система оценивания успеваемости и достижений обучающихся

Перечень и параметры оценивания видов деятельности обучающегося (1 семестр)

№ п/п	Вид деятельности обучающегося	Весовой коэффициент значимости, %	Критерии (условия) начисления баллов
1	Аудиторная активность: посещение лекций и практических (семинарских) занятий	5	68 часов занятий, по 1,47 балла за посещение каждого часа, максимум 100 баллов
2	Текущий контроль	10	2 опроса по 2 вопроса в каждом, за каждый вопрос максимум по 25 баллов.
3	Выполнение лабораторных работ	15	5 лабораторных работ, по 20 баллов за успешную сдачу каждой работы, максимум 100 баллов. 20 баллов за защиту работы можно получить при полном и правильном выполнении задания, предоставлении отчета с корректным оформлением и правильных ответах на вопросы по лабораторной. За недочеты и ошибки баллы снижаются
4	Защита курсовой работы	30	100 баллов за защиту курсовой работы ставится, если обучающийся: <ul style="list-style-type: none"> • предоставил правильно оформленный отчет; • защитил работу в срок; • выполнил работу в полном объеме; • не допустил ошибок в работе; • правильно и исчерпывающе ответил на вопросы преподавателя на тему работы. За нарушения условий в списке баллы снижаются пропорционально тяжести нарушения.
5	Сдача зачета	40	Ответы на теоретические вопросы (полнота, владение терминологией, затраченное время) – максимум 30 баллов за каждый вопрос (всего 2 вопроса); Решение практической задачи – до 40 баллов.
Итого (%):		100	

Перечень и параметры оценивания видов деятельности обучающегося (2 семестр)

№ п/п	Вид деятельности обучающегося	Весовой коэффициент значимости, %	Критерии (условия) начисления баллов
1	Аудиторная активность: посещение лекций и практических (семинарских) занятий	10	85 часов занятий, по 1,18 балла за посещение каждого часа, максимум 100 баллов
2	Текущий контроль	20	2 опроса по 2 вопроса в каждом, за каждый вопрос максимум по 25 баллов.
2	Выполнение лабораторных работ	30	5 лабораторных работ, по 20 баллов за успешную сдачу каждой работы, максимум 100 баллов.

			20 баллов за защиту работы можно получить при полном и правильном выполнении задания, предоставлении отчета с корректным оформлением и правильных ответах на вопросы по лабораторной. За недочеты и ошибки баллы снижаются
4	Сдача зачета	40	Ответы на теоретические вопросы (полнота, владение терминологией, затраченное время) – максимум 30 баллов за каждый вопрос (всего 2 вопроса); Решение практической задачи – до 40 баллов.
Итого (%):		100	

Перевод балльной шкалы в традиционную систему оценивания

Баллы	Оценка по нормативной шкале	
86 - 100	5 (отлично)	Зачтено
75 – 85	4 (хорошо)	
61 – 74		
51 - 60		
40 – 50	3 (удовлетворительно)	Не зачтено
17 – 39	2 (неудовлетворительно)	
1 – 16		
0		

8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Учебная литература

а) основная учебная литература

1. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ А.В. Артемов— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: <http://www.iprbookshop.ru/33430.html>.— ЭБС «IPRbooks»
2. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ О.В. Прохорова— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: <http://www.iprbookshop.ru/43183.html>.— ЭБС «IPRbooks»

б) дополнительная учебная литература

1. Аллан Расселл Информационная революция [Электронный ресурс]: путь к корпоративному разуму/ Расселл Аллан, Миллер Глория, Дэвис Джим— Электрон. текстовые данные.— М.: Альпина Паблишер, Альпина Бизнес Букс, 2016.— 261 с.— Режим доступа: <http://www.iprbookshop.ru/43618.html>.— ЭБС «IPRbooks»
2. Афанасьев М.Я. Встроенные компьютерные системы [Электронный ресурс]: методические рекомендации по выполнению лабораторных работ/ М.Я. Афанасьев, Ю.В. Федосов— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2016.— 52 с.— Режим доступа: <http://www.iprbookshop.ru/65831.html>.— ЭБС «IPRbooks»
3. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: <http://www.iprbookshop.ru/63594.html>.— ЭБС «IPRbooks»

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

1. Бусыгин К. Н. Защита информационных процессов в компьютерных системах. Групповые политики Microsoft Windows [Электронный ресурс]: учебное пособие / Бусыгин К. Н. — СПб.: СПГУТД, 2014.— 127 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=1846, по паролю.
2. Спицкий, С. В. Эффективная аудиторная и самостоятельная работа обучающихся: методические указания / С. В. Спицкий. – СПб.: СПбГУПТД, 2015. – Режим доступа: http://publish.sutd.ru/tp_get_file.php?id=2015811, по паролю.
3. Караулова, И. Б. Организация самостоятельной работы обучающихся / И. Б. Караулова, Г. И. Мелешкова, Г. А. Новоселов. – СПб.: СПГУТД, 2014. – 26 с. – Режим доступа http://publish.sutd.ru/tp_get_file.php?id=2014550, по паролю.

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

1. Java™ Platform, Standard Edition 8 API Specification [Электронный ресурс]. – Режим доступа: <https://docs.oracle.com/javase/8/docs/api/>
2. Электронно-библиотечная система IPRbooks. (<http://www.iprbookshop.ru>)
3. Электронная библиотека учебных изданий СПбГУПТД (<http://publish.sutd.ru>)

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

1. Среда разработки программных продуктов Java
2. JDK 1.8
3. Microsoft Office Standart 2016 Russian Open No Level Academic)
4. Microsoft Windows 10 Home Russian Open No Level Academic Legalization Get Genuine (GGK) + Microsoft Windows 10 Professional (Pro – профессиональная) Russian Upgrade Open No Level Academic

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

1. Компьютерный класс с возможностью выхода в Интернет
2. Проектор

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 лекциях излагается основное содержание курса, иллюстрируемое конкретными примерами, широко используется зарубежный и отечественный опыт по соответствующей тематике.</p> <p>Освоение лекционного материала обучающимся предполагает следующие виды работ:</p> <ul style="list-style-type: none">• проработка рабочей программы в соответствии с целями и задачами, структурой и содержанием дисциплины;• конспект лекций: кратко, схематично, последовательно фиксировать основные положения, выводы и формулировки; пометать важные мысли, выделять ключевые слова, термины. <p>Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации или на практическом занятии</p>
Практические занятия	<p>На практических занятиях (семинарах) 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.</p>
Лабораторные занятия	<p>В процессе выполнения лабораторных работ обучающийся учится применять положения теоретического курса при реализации программного обеспечения. Следует предварительно изучить методические указания по выполнению лабораторных работ.</p>
Самостоятельная работа	<p>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; выполнения рефератов; подготовку к экзамену. Самостоятельная работа выполняется индивидуально, а также может проводиться под руководством (при участии) преподавателя.</p> <p>При подготовке к экзамену необходимо ознакомиться с демонстрационным вариантом задания (перечнем вопросов), проработать конспекты лекций и практических занятий, рекомендуемую литературу, получить консультацию у преподавателя.</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-7	<p>Раскрывает основные характеристики информационного ресурса как объекта защиты</p> <p>Перечисляет и исследует случайные и преднамеренные угрозы</p> <p>Составляет организационно-методологические рекомендации для проведения аудита уязвимостей</p>	<p>Вопросы для устного собеседования</p> <p>Практическое задание</p>	<p>Перечень вопросов для устного собеседования (58 вопросов)</p> <p>Перечень практических заданий (10 заданий)</p>
ПК-3	<p>Раскрывает значение необходимости проведения защитных мероприятий в сфере информационной безопасности</p> <p>Систематизирует данные об управлении сетями и системами</p> <p>Предлагает решение проблем защиты информации в системах с применением программно-аппаратных средств</p>	<p>Вопросы для устного собеседования</p> <p>Практическое задание</p>	<p>Перечень вопросов для устного собеседования (58 вопросов)</p> <p>Перечень практических заданий (10 заданий)</p>
ПК-10	<p>Описывает методы и средства обеспечения информационной безопасности в компьютерных системах.</p> <p>Составляет перечень средств и методов защиты информации.</p> <p>Осуществляет поиск материалов по вопросам обеспечения информационной безопасности в базах данных и Интернет-ресурсах.</p>	<p>Вопросы для устного собеседования</p> <p>Практическое задание</p>	<p>Перечень вопросов для устного собеседования (40 вопросов)</p> <p>Перечень практических заданий (10 заданий)</p>
ПК-12	<p>Описывает основные положения концепции защиты информации в компьютерных системах</p> <p>выполняет настройку защитных механизмов сетевых программно- аппаратных средств</p> <p>Производит оценку эффективности работы основных средств защиты информации в различных системах</p>	<p>Вопросы для устного собеседования</p> <p>Практическое задание</p>	<p>Перечень вопросов для устного собеседования (58 вопросов)</p> <p>Перечень практических заданий (10 заданий)</p>

10.1.2. Описание шкал и критериев оценивания сформированности компетенций

Критерии оценивания сформированности компетенций

Баллы	Оценка по традиционной шкале	Критерии оценивания сформированности компетенций	
		Устное собеседование	Курсовая работа
86 - 100	5 (отлично)	<p>Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу.</p> <p>Учитываются баллы, накопленные в течение семестра.</p>	<p>Критическое и разностороннее рассмотрение вопросов, свидетельствующее о значительной самостоятельной работе с источниками. Качество исполнения всех элементов задания полностью соответствует всем требованиям.</p> <p>Учитываются баллы, накопленные в течение семестра.</p>
75 – 85	4 (хорошо)	<p>Ответ полный, основанный на проработке всех обязательных источников информации. Подход к материалу ответственный, но стандартный.</p> <p>Учитываются баллы, накопленные в течение семестра.</p>	<p>Все заданные вопросы освещены в необходимой полноте и с требуемым качеством. Ошибки отсутствуют. Самостоятельная работа проведена в достаточном объеме, но ограничивается только основными рекомендованными источниками информации.</p>

			Учитываются баллы, накопленные в течение семестра.
61 – 74		Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки. Учитываются баллы, накопленные в течение семестра.	Работа выполнена в соответствии с заданием. Имеются отдельные несущественные ошибки или отступления от правил оформления работы. Учитываются баллы, накопленные в течение семестра.
51 - 60	3 (удовлетворительно)	Ответ воспроизводит в основном только лекционные материалы, без самостоятельной работы с рекомендованной литературой. Демонстрирует понимание предмета в целом, без углубления в детали. Присутствуют существенные ошибки или пробелы в знаниях по некоторым темам. Учитываются баллы, накопленные в течение семестра.	Задание выполнено полностью, но в работе есть отдельные существенные ошибки, либо качество представления работы низкое, либо работа представлена с опозданием. Учитываются баллы, накопленные в течение семестра.
40 – 50		Ответ неполный, основанный только на лекционных материалах. При понимании сущности предмета в целом – существенные ошибки или пробелы в знаниях сразу по нескольким темам, незнание (путаница) важных терминов. Учитываются баллы, накопленные в течение семестра.	Задание выполнено полностью, но с многочисленными существенными ошибками. При этом нарушены правила оформления или сроки представления работы. Учитываются баллы, накопленные в течение семестра.
17 – 39	2 (неудовлетворительно)	Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки. Не учитываются баллы, накопленные в течение семестра.	Отсутствие одного или нескольких обязательных элементов задания, либо многочисленные грубые ошибки в работе, либо грубое нарушение правил оформления или сроков представления работы. Не учитываются баллы, накопленные в течение семестра.
1 – 16		Непонимание заданного вопроса. Неспособность сформулировать хотя бы отдельные концепции дисциплины. Не учитываются баллы, накопленные в течение семестра.	Содержание работы полностью не соответствует заданию. Не учитываются баллы, накопленные в течение семестра.
0		Попытка списывания, использования неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки). Не учитываются баллы, накопленные в течение семестра.	Представление чужой работы, плагиат, либо отказ от представления работы. Не учитываются баллы, накопленные в течение семестра.
40 – 100	Зачтено	Обучающийся своевременно выполнил лабораторные работы; в соответствии с требованиями выполнил и защитил курсовую работу по дисциплине, возможно допуская несущественные ошибки в ответе на вопросы преподавателя. Учитываются баллы, накопленные в течение семестра.	
0 – 39	Не зачтено	Обучающийся не выполнил (выполнил частично) лабораторные работы; не смог изложить содержание и выводы своей курсовой работы, допустил существенные ошибки в ответе на вопросы преподавателя. Не учитываются баллы, накопленные в течение семестра.	

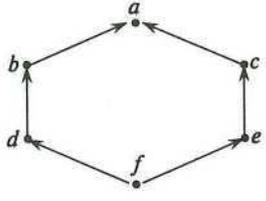
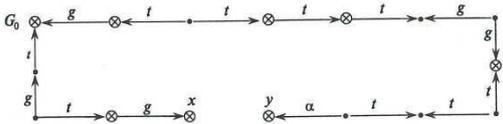
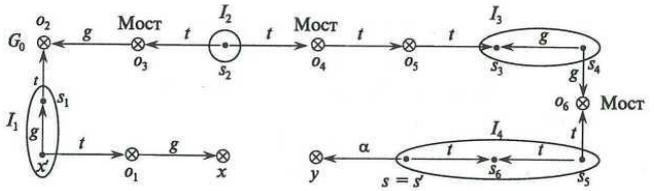
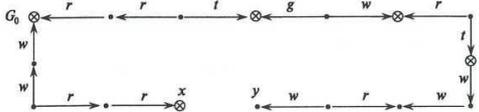
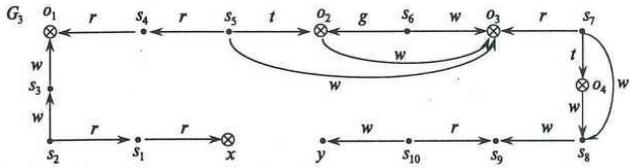
10.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

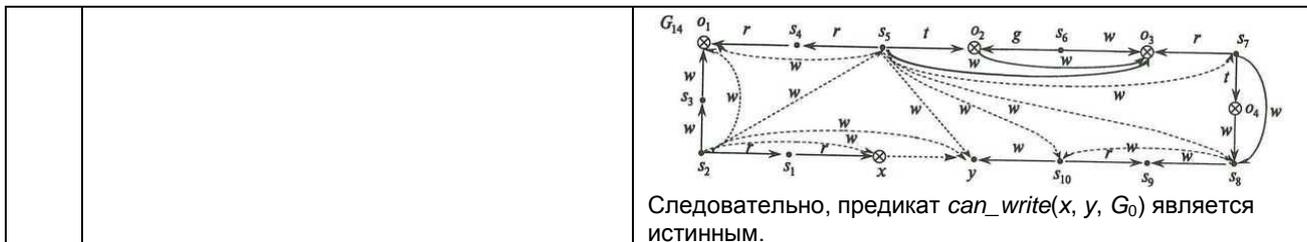
10.2.1. Перечень вопросов (тестовых заданий), разработанный в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировка вопросов	№ темы
1	Виды политик управления доступом и информационными потоками	1
2	Основные определения и классическая классификация угроз безопасности информации	1

3	Диаграмма основных видов формальных моделей безопасности	1
4	Описание модели ХРУ	2
5	Анализ безопасности истем ХРУ	2
6	Описание модели ТМД	3
7	Анализ безопасности систем ТМД	3
8	Описание классической модели Take-Grant	4
9	Анализ безопасности классической модели Take-Grant	4
10	Описание расширенной модели Take-Grant	5
11	Анализ безопасности расширенной модели Take-Grant	5
12	Описание субъектно-ориентированной модели ИПС	6
13	Определение классической модели Белла-ЛаПадулы	7
14	Политика low-watermark в модели Белла-ЛаПадулы	7
15	Безопасность переходов в модели Белла-ЛаПадулы	7
16	Модель мандатной политики целостности информации Биба	7
17	Описание модели СВС	8
18	Автоматная и программная модели безопасности информационных потоков	9
19	Вероятностная модель безопасности информационных потоков	9
20	Описание базовой модели ролевого управления доступом	10
21	Основные положения и администрирование множеств авторизованных ролей пользователей в ролевом управлении доступом	11
22	Администрирование множеств прав доступа и иерархии ролей в ролевом управлении доступом	11
23	Защита от угрозы конфиденциальности информации в модели мандатного ролевого управления доступом	12
24	Защита от угроз конфиденциальности и целостности информации в модели мандатного ролевого управления доступом	12
25	Определение базовой ДП-модели	13
26	Условия передачи прав доступа в базовой ДП-модели	13
27	Условия реализации информационного потока по памяти в базовой ДП-модели	13
28	Условия реализации информационного потока по времени в базовой ДП-модели	13
29	Условия передачи прав доступа в базовой ДП-модели без кооперации доверенных и недоверенных субъектов	14
30	Условия реализации запрещенных информационных потоков по памяти и по времени в базовой ДП-модели без кооперации доверенных и недоверенных субъектов	14
31	Определение ФАС ДП-модели и условия истинности предикатов	15
32	Корректные субъекты в ФАС ДП-модели	15
33	Определение ПБА ДП-модели	16
34	Условия реализации политики безопасного администрирования в ПБА ДП-модели	16
35	Определение ПАР ДП-модели	16
36	Определение ФПАС ДП-модели	17
37	Использование ФАС-модели для анализа веб-системы	18
38	Метод предотвращения возможности получения права доступа владения недоверенным субъектом к доверенному субъекту	19
39	Метод реализации ПБА	19
40	Метод реализации ПАР	19
41	Определения и предположения в мандатной ДП-модели	20
42	Правила преобразования состояний мандатной ДП-модели	20
43	Безопасность в смысле Белла-ЛаПадулы для мандатной ДП-модели	21
44	Условия повышения субъектом уровня доступа в мандатной ДП-модели	21
45	Определение ДП-модели с блокирующими доступами доверенных субъектов	22
46	Условия истинности предиката <i>can_write_time_block</i> в ДП-модели с блокирующими доступами доверенных субъектов	22
47	Определение мандатной ДП-модели с блокирующими доступами доверенных субъектов	23
48	Условия истинности предиката <i>can_write_time_down_block</i> в ДП-модели с блокирующими доступами доверенных субъектов	23
49	Мандатная ДП-модель с отождествлением порожденных субъектов	23
50	Определение мандатной ДП-модели КС, реализующих политику строгого мандатного управления доступом	24
51	Предикат <i>can_write_time_down_block</i> в мандатной ДП-модели КС, реализующих политику строгого мандатного управления доступом	24
52	Определение состояния системы МРОСЛ	25
53	Функционально или параметрически ассоциированные сущности в системе МРОСЛ	26
54	Доступы и права доступа в системе МРОСЛ	26
55	Задание мандатного управления доступом для состояний системы МРОСЛ	27
56	Задание мандатного контроля целостности для состояний системы МРОСЛ	27
57	Де-юре правила преобразования состояний МРОСЛ	28
58	Де-факто правила преобразования состояний МРОСЛ	28

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

№ п/п	Условия типовых задач (задач, кейсов)	Ответ
1	<p>Задание. Задаёт ли решетку представленный граф:</p> 	<p>В соответствии с определением выполнены все свойства отношения частичного порядка «\leq» на множестве $\{a, b, c, d, e, f\}$. Для каждой пары вершин, соединенных в графе путем, существует наименьшая верхняя и наибольшая нижняя границы. Например, справедливы равенства $f \oplus b = f$ и $f \otimes b = b$. Для каждой пары, не соединенных в графе путем, приведем значения наименьших верхних и наибольших нижних границ:</p> <p>$d \oplus e = a, d \otimes e = f;$ $b \oplus e = a, b \otimes e = f;$ $d \oplus c = a, d \otimes c = f;$ $b \oplus c = a, b \otimes c = f.$</p> <p>Следовательно, по определению граф задаёт решетку.</p>
2	<p>Проверьте, истинен ли предикат $can_share(\alpha, x, y, G_0)$ для графа доступов G_0 на рисунке:</p> 	<p>Введем обозначения для объектов и субъектов графа доступов $G_0 = (S_0, O_0, E_0)$. Существует субъект $s = s' \in S_0$ такой, что верно условие $(S_i, y, a) \in E_0$, следовательно, условие 1 теоремы выполнено. Так как s является субъектом, и существует субъект $x' \in S_0$ такой, что он соединен с объектом x начальным пролетом моста, то условие 2 теоремы выполнено.</p> <p>Выделим в графе G_0 острова $I_1 = \{x', s_1\}$, $I_2 = \{s_2\}$, $I_3 = \{s_3, s_4\}$, $I_4 = \{s_5, s_6, s\}$. Каждая пара соседних островов соединена мостом: I_1 и I_2 соединены мостом, проходящим через вершины s_1, o_2, o_3, s_2; I_2 и I_3 соединены мостом, проходящим через вершины s_2, o_4, o_5, s_3; I_3 и I_4 соединены мостом, проходящим через вершины s_4, o_6, s_5. Следовательно, условие 3 теоремы выполнено.</p>  <p>Таким образом, выполнены все условия теоремы, и предикат $can_share(\alpha, x, y, G_0)$ является истинным.</p>
3	<p>Задание. Проверьте, истинен ли предикат $can_write(x, y, G_0)$ для графа доступов G_0 на рисунке ниже. Решение задачи должно быть получено путем непосредственного применения де-юре и де-факто правил.</p> 	<p>Введем обозначения для объектов и субъектов графа доступов G_0. Применим к графу G_0 следующие де-юре правила:</p> <p>$op_1 = grant(w, s_6, o_2, o_3);$ $op_2 = take(w, s_5, o_2, o_3);$ $op_3 = take(w, s_7, o_4, o_8).$</p> <p>Получим граф G_3 такой, что выполняется условие $G_0 \vdash_{op1} G_1 \vdash_{op2} G_2 \vdash_{op3} G_3$.</p>  <p>Применим к графу G_3 следующие де-факто правила:</p> <p>$op_4 = spy(s_2, s_1, x);$ $op_5 = find(s_2, s_3, o_1);$ $op_6 = spy(s_5, s_4, o_1);$ $op_7 = post(s_5, s_2, o_1);$ $op_8 = post(s_7, s_5, o_3);$ $op_9 = find(s_5, s_7, s_8);$ $op_{10} = post(s_{10}, s_8, s_9);$ $op_{11} = find(s_5, s_8, s_{10});$ $op_{12} = find(s_5, s_{10}, y);$ $op_{13} = find(s_2, s_5, y);$ $op_{14} = pass(s_2, y, x).$</p> <p>Получим граф G_{14} такой, что выполняются условия $G_0 \vdash_{op1} G_1 \vdash_{op2} \dots \vdash_{op14} G_{14} = (S_{14}, O_{14}, E_{14} \cup F_{14})$ И $(x, y, w) \in F_{14}$.</p>



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 экзамена и порядок ликвидации академической задолженности

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся (принято на заседании Ученого совета 31.08.2013г., протокол № 1)

10.3.2. Форма проведения промежуточной аттестации по дисциплине

устная письменная компьютерное тестирование иная*

*В случае указания формы «Иная» требуется дать подробное пояснение

10.3.3. Особенности проведения зачета и экзамена

Обучающийся тянет билет, в котором два теоретических вопроса и задача. После этого готовится в течении как минимум 15 минут с использованием конспекта лекций и других материалов. Обучающийся в устной форме доводит до преподавателя ответ на вопрос, при необходимости прямо во время ответа составляет необходимые схемы или диаграммы. Отвечает на сопутствующие вопросы преподавателя, которые могут выходить за рамки билетов, но в рамках изучаемого материала дисциплины (за этот и прошлый семестры).

После ответа на теоретический вопрос обучающийся приступает к решению задачи, гарантированно на решение задачи времени дается 30 минут, решение формулируется с использованием конспекта лекций и иных материалов, при правильном решении задачи преподаватель задает вопросы по методам или технологиям решения, вопросы могут касаться всего материала изучаемой дисциплины (за прошлые семестры включительно).