МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

СОГЛАСОВАНО
Руководитель ОП

_____ Варлатая С.К.
(подпись) (Ф.И.О. рук. ОП)

УТВЕРЖДАЮ
И.о. заведующего кафедрой

_____ Нефедев К.В.
(подпись) (Ф.И.О. рук. ОП)

«_____»_____20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Защита информационных процессов в компьютерных системах
Направление 10.03.01 Информационная безопасность
Организация и технологии защиты информации
Форма подготовки очная

курс 4 семестр 7
лекции 32 час.
практические занятия 32 час.
лабораторные работы 34 час.
В том числе с использованием МАО лек. 0 / пр. 0 / лаб. 0 час.
всего часов аудиторной нагрузки 98 час.
в том числе с использованием МАО 32 час.
самостоятельная работа 46 час.
в том числе на подготовку к экзамену не предусмотрено
контрольные работы (количество) не предусмотрено
курсовая работа / курсовой проект не предусмотрено
зачет не предусмотрено
экзамен 7 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17.11.2020 № 1427.

Рабочая программа обсуждена на заседании кафедры Информационная безопасность протокол № 4 от «27» января 2021 г.

И.о. заведующего кафедрой Информационная безопасность, д.ф.-м.н., профессор Нефедев К.В.

Составитель доц. Дзенскевич Е.А.

Владивосток

2021

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры/департамента:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой/Директор департамента _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры/департамента:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой/Директор департамента _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры/департамента:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой/Директор департамента _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры/департамента:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой/Директор департамента _____ _____
(подпись) (И.О. Фамилия)

Цели и задачи освоения дисциплины:

Цель: изучить основные виды политик управления доступом и информационными потоками в КС в том числе и основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков;

Задачи:

- изучение основных формальных моделей политик безопасности, моделей дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков;
- приобретение навыков использования математических моделей безопасности при осуществлении анализа защищенности КС.

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные/ общепрофессиональные/ профессиональные компетенции (элементы компетенций).

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1	ОПК-1.1 Использует основы информации, информационных технологий и информационной безопасности
		ОПК-1.2 Решает профессиональные задачи информационной безопасности с применением естественнонаучных и общеинженерных знаний
		ОПК-1.3 Осуществляет теоретическое и экспериментальное исследования объективных потребностей личности, общества и государства в контексте защиты информации
Способен применять информационно-коммуникационные	ОПК-2	ОПК-2.1 Определяет современные информационные технологии

технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности		и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности
		ОПК-2.2 Выбирает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности
		ОПК-2.3 Применяет современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности

Код и наименование индикатора достижения компетенции	**Наименование показателя оценивания (результата обучения по дисциплине)**
ОПК-1.1 Использует основы информации, информационных технологий и информационной безопасности	Знает: цели, задачи и принципы построения комплексной системы защиты информации
	Умеет: оценивать эффективность комплексной системы защиты информации
	Владеет: современными методами и технологиями по формированию требований по защите информации
ОПК-1.2 Решает профессиональные задачи информационной безопасности с применением естественнонаучных и общеинженерных знаний	Знает: программные средства системного, прикладного и специального назначения для защиты информации, а так же современные инструментальные средства, языки и системы программирования
	Умеет: применять для различных целей программные средства системного, прикладного и специального назначения
	Владеет: современными и широко используемыми языками и системами программирования для решения профессиональных задач
ОПК-1.3 Осуществляет теоретическое и экспериментальное исследования объективных	Знает: принципы и методы организационной защиты информации
	Умеет: применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем

потребностей личности, общества и государства в контексте защиты информации	Владеет: методами технической защиты информации
ОПК-2.1 Определяет современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	Знает: основные определения, понятия и символику математики, связи между различными понятиями, приемы и методы решения практических задач, возникающих в профессиональной деятельности
	Умеет: использовать базовые знания, математический аппарат, выбирать эффективный метод и использовать его для решения профессиональных задач, самостоятельно работать с учебной, учебно- методической и справочной литературой, другими источниками, воспринимать, осмысливать информацию
	Владеет: основными знаниями и понятиями математики, математическим аппаратом, способами и формами представления результата, приемами выбора и применения эффективных методов для решения профессиональных с использованием математического аппарата
ОПК-2.2 Выбирает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	Знает: основные дискретные структуры: конечные автоматы, грамматики, графы; комбинаторные структуры
	Умеет: применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач
	Владеет: приемами использования в профессиональной деятельности базовых знаний в области дискретной математики
ОПК-2.3 Применяет современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	Знает: методы перечисления для основных дискретных структур
	Умеет: пользоваться законами комбинаторики для решения прикладных задач
	Владеет: приемами использования в профессиональной деятельности базовых знаний в области дискретной математики

Для формирования вышеуказанных компетенций в рамках дисциплины «Электроника и схемотехника» применяются следующие методы активного/ интерактивного обучения: лекция – беседа, лекция – пресс-конференция.

Трудоёмкость дисциплины и видов учебных занятий по дисциплине

Общая трудоемкость дисциплины составляет 5 зачётных единиц (180 академических часов). (1 зачетная единица соответствует 36 академическим часам)

Видами учебных занятий и работы обучающегося по дисциплине могут являться:

Обозначение	Виды учебных занятий и работы обучающегося
Лек	Лекции
Лаб	Лабораторные работы
Пр	Практические занятия
ОК	Онлайн курс
СР	Самостоятельная работа обучающегося в период теоретического обучения
Контроль	Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации

Структура дисциплины:

Форма обучения – очная.

№	Наименование раздела дисциплины	Семестр	Количество часов по видам учебных занятий и работы обучающегося						Формы промежуточной аттестации, текущего контроля успеваемости
			Лек	Лаб	Пр	ОК	СР	Контроль	
1	Классификация угроз, понятия								
2	Виды моделей разграничения доступа								
	Итого:		32	34	32		46	36	

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Модуль 1. Классификация угроз, понятия. (16 ч)

Раздел 1. Введение. Основные понятия и определения. (16 ч)

Тема 1. Сущность, субъект, доступ, информационный поток (7 ч)

Основные элементы теории компьютерной безопасности (сущность, субъект, доступ, право доступа, информационные потоки по памяти или по времени). Основная аксиома. Проблема построения защищенной КС. Модели ценности информации: аддитивная модель, порядковая шкала, решетка многоуровневой безопасности.

Тема 2. Угрозы безопасности информации. Политика безопасности (9ч) Классификация угроз безопасности информации. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС. Понятие политики безопасности. Модель нарушителя. Основные виды политик управления доступом и информационными потоками. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков.

Модуль 2. Виды моделей разграничения доступа. (16ч)

Раздел 1. Модели компьютерных систем с дискреционным управлением доступом (16 ч)

Тема 1. Модель матрицы доступов Харрисона-Руззо-Ульмана (5 ч)

Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ). Анализ безопасности систем ХРУ. Монооперационные системы ХРУ. Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ.

Тема 2. Классическая и расширенная модели распространения прав доступа Take-Grant (5 ч)

Классическая модель Take-Grant. Де-юре правила преобразования графов доступов. Условия передачи прав доступа в графе доступов, состоящем только из субъектов. Остров, мост, пролеты моста. Условия передачи прав доступа в произвольном графе доступов при отсутствии ограничений на кооперацию субъектов. Элементы расширенной модели Take-Grant. Де-факто правила

преобразования графов доступов и информационных потоков.

Тема 3. Субъектно-ориентированная модель изолированной программной среды (6 ч)

Субъектно-ориентированная модель изолированной программной среды (ИПС). Объекты, функционально ассоциированные с субъектами. Мониторы безопасности обращений и порождения субъектов. Базовая теорема ИПС.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторная работа (34ч)

Тема 1. Основные угрозы информации в компьютерных системах (6ч)

Тема 2. Специфика возникновения угроз в открытых сетях (4ч)

Тема 3. Особенности защиты информации на узлах компьютерной сети с использованием криптографических методов (6ч)

Тема 4. Администрирование серверных систем и приложений (6ч)

Тема 5. Использование межсетевых экранов для защиты информационных процессов (5ч)

Тема 6. Требования к защите автоматизированных систем от НСД (7ч)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Защита информационных процессов в компьютерных системах» представлено в Приложении 1 и включает в себя:

- план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
- характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;
- требования к представлению и оформлению результатов самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Модуль 1. Классификация угроз, понятия.	ОПК-2.1 Определяет современные информационные технологии и и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	Знает: основные определения, понятия и символику математики, связи между различными понятиями, приемы и методы решения практических задач, возникающих в профессиональной деятельности	ПР-1	1-28
			Умеет: использовать базовые знания, математический аппарат, выбирать эффективный метод и использовать его для решения профессиональных задач, самостоятельно работать с учебной, учебно-методической и справочной литературой, другими источниками, воспринимать, осмысливать информацию	ПР-7	1-28
			Владеет: основными знаниями и понятиями математики, математическим аппаратом, способами и	ПР-6	1-28

			формами представления результата, приемами выбора и применения эффективных методов для решения профессиональных с использованием математического аппарата		
2	Модуль 2. Виды моделей разграничения доступа	ОПК-2.2 Выбирает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	Знает: основные дискретные структуры: конечные автоматы, грамматики, графы; комбинаторные структуры	ПР-1	29-39
			Умеет: применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач	ПР-7	29-39
			Владеет: приемами использования в профессиональной деятельности базовых знаний в области дискретной математики	ПР-6	29-39

Методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. С. К. Варлатая, М. В. Шаханова, Защита информационных процессов в компьютерных сетях: учебно-методический комплекс. С. К. Варлатая, М. В. Шаханова; Дальневосточный федеральный университет, 2015. 216 с.
2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. — М.: Горячая линия - Телеком, 2011. 320 с.
3. Васильков, А. В. Безопасность и управление доступом в информационных системах: учеб. пособие для сред. проф. образования / А. В. Васильков, И. А. Васильков. - М.: Форум, 2010. - 367 с.: ил., табл. - (Профессиональное образование). - Библиогр.: с. 356-358. - ISBN 978-5-91134-360-6: 285-89.
4. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учеб. пособие для вузов по направл. "Информатика и вычисл. техника" / В. Ф. Шаньгин. - М.: ФОРУМ [и др.], 2010. - 591 с.: ил. - (Высшее образование). - Библиогр.: с. 568-573

Дополнительная литература

1. В. А. Трайнев, Системный подход к обеспечению информационной безопасности предприятия (фирмы). В. А. Трайнев; Международная академия наук информации, информационных процессов и технологий (МАН ИПТ), Москва: Дашков и КО, 2018. 331 с.
2. Информационная безопасность и защита информации: учебное пособие для вузов / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова, Старый Оскол: ТНТ, 2015. 383 с.

Интернет-ресурсы

1. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=4925 Пушкарев В.В. Пушкарев В.П. Защита информационных процессов в компьютерных системах. 2012г. 131 стр.
2. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=6031 Горенский Б.М.Кирякова О.В.Лапина Л.А.Ченцов С.В. Информационные технологии в управлении технологическими процессами цветной

металлургии: лабораторный практикум. 2012г. 148 стр.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Защита информационных процессов в компьютерных системах», составляет 98 часов. На самостоятельную работу – 46 часов. При этом аудиторная нагрузка состоит из 32 лекционных часов и 32 часов лабораторных работ.

Обучающийся получает теоретические знания на лекциях. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Подготовка к лабораторным работам предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению лабораторных работ. Основной лабораторных работ является выполнение заданий с последующим предоставлением отчета о выполнении.

В рамках указанной дисциплины итоговой формы аттестации является экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов лабораторных работ.

Методические указания для написания реферата

Прежде всего, нужно выбрать тему реферата и подобрать соответствующую литературу. После ознакомления с литературой следует приступить к составлению плана. План реферата должен состоять из названия (темы), введения, основной части, заключения и списка использованной литературы (3-5 работ). Основная часть, как правило, разбивается на дополнительные вопросы (не более 3-4).

Объём реферата должен быть не менее 12 машинописных страниц.

Во введении описывается цель, задачи работы, а также раскрываются смысл и значение основных понятий выбранной темы, область их применения.

В основной части необходимо:

а) ещё раз уточнить тему работы;

б) разбить основную часть работы на дополнительные вопросы;

в) дать ответы на эти вопросы, получив вспомогательные результаты. На их основе дать ответ на основной вопрос. Допускаются ссылки на дополнительную литературу.

В заключении подводятся итоги исследования. Заключение не должно быть большим по объёму.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для обеспечения данной дисциплины необходима аудитория, оснащенная презентационной техникой, компьютерный класс с программным обеспечением и возможностью использования Интернет-ресурсов, учебная лаборатория, оборудованная экспериментальными стендами и соответствующими измерительными приборами, учебные и методические пособия (учебники, программы, сборники упражнений и т.д.), расходные материалы (бумага, картридж).

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-18 неделя обучения	Подготовка самостоятельных и лабораторных работ.		Отчет о выполнении
2	Сессия	Подготовка к экзамену	9	Экзамен

Подготовка отчетов к лабораторным работам предполагает повторение лекционного материала и выполнение практических заданий и лабораторных работ. В результате студент должен представить отчеты о проделанной работе.

Методические рекомендации к работе с литературными источниками

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Критерии оценки выполнения самостоятельной работы

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы

1. Просмотр и проверка выполнения самостоятельной работы преподавателем.
2. Самопроверка, взаимопроверка выполненного задания в группе.
3. Обсуждение результатов выполненной работы на занятии.
4. Текущее тестирование.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентов учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные

возможности, варианты действий;

- умение сформировать свою позицию, оценку и аргументировать ее.

Критерии оценки выполнения контрольных заданий для самостоятельной работы

Процент правильных ответов	**Оценка**
От 95% до 100%	отлично
От 76% до 95%	хорошо
От 61% до 75%	удовлетворительно
Менее 61 %	неудовлетворительно

Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников, материалов по лабораторным работам.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Паспорт фонда оценочных средств

Код и наименование индикатора достижения компетенции	**Наименование показателя оценивания (результата обучения по дисциплине)**
ОПК-1.1 Использует основы информации, информационных технологий и информационной безопасности	Знает: цели, задачи и принципы построения комплексной системы защиты информации
	Умеет: оценивать эффективность комплексной системы защиты информации
	Владеет: современными методами и технологиями по формированию требований по защите информации
ОПК-1.2 Решает профессиональные задачи информационной безопасности с применением естественнонаучных и общеинженерных знаний	Знает: программные средства системного, прикладного и специального назначения для защиты информации, а так же современные инструментальные средства, языки и системы программирования
	Умеет: применять для различных целей программные средства системного, прикладного и специального назначения
	Владеет: современными и широко используемыми языками и системами программирования для решения профессиональных задач
ОПК-1.3 Осуществляет теоретическое и экспериментальное исследования объективных потребностей личности, общества и государства в контексте защиты информации	Знает: принципы и методы организационной защиты информации
	Умеет: применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем
	Владеет: методами технической защиты информации
ОПК-2.1 Определяет современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	Знает: основные определения, понятия и символику математики, связи между различными понятиями, приемы и методы решения практических задач, возникающих в профессиональной деятельности
	Умеет: использовать базовые знания, математический аппарат, выбирать эффективный метод и использовать его для решения профессиональных задач, самостоятельно работать с учебной, учебно- методической и справочной литературой, другими источниками, воспринимать, осмысливать информацию
	Владеет: основными знаниями и понятиями математики, математическим аппаратом, способами и формами представления результата, приемами выбора и применения

	эффективных методов для решения профессиональных с использованием математического аппарата
ОПК-2.2 Выбирает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	Знает: основные дискретные структуры: конечные автоматы, грамматики, графы; комбинаторные структуры
	Умеет: применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач
	Владеет: приемами использования в профессиональной деятельности базовых знаний в области дискретной математики
ОПК-2.3 Применяет современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	Знает: методы перечисления для основных дискретных структур
	Умеет: пользоваться законами комбинаторики для решения прикладных задач
	Владеет: приемами использования в профессиональной деятельности базовых знаний в области дискретной математики

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Модуль 1. Классификация угроз, понятия.	ОПК-2.1 Определяет современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	Знает: основные определения, понятия и символику математики, связи между различными понятиями, приемы и методы решения практических задач, возникающих в профессиональной деятельности	ПР-1	1-28
			Умеет: использовать базовые знания, математический аппарат, выбирать эффективный метод и использовать его для решения профессиональных задач, самостоятельно работать с учебной, учебно-методической и справочной литературой, другими источниками, воспринимать, осмысливать информацию	ПР-7	1-28
			Владеет: основными	ПР-6	1-28

			знаниями и понятиями математики, математическим аппаратом, способами и формами представления результата, приемами выбора и применения эффективных методов для решения профессиональных с использованием математического аппарата		
2	Модуль 2. Виды моделей разграничения доступа	ОПК-2.2 Выбирает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	Знает: основные дискретные структуры: конечные автоматы, грамматики, графы; комбинаторные структуры	ПР-1	29-39
			Умеет: применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач	ПР-7	29-39
			Владеет: приемами использования в профессиональной деятельности базовых знаний в области дискретной математики	ПР-6	29-39

Оценочные средства для промежуточной аттестации
Список вопросов на экзамен

1. Представьте классификацию видов угроз информационной безопасности Российской Федерации. Перечислите угрозы безопасности информационных и телекоммуникационных средств и систем.
2. Какие функциональные блоки включает система разграничения доступа, нарисуйте структурную схему диспетчера доступа.
3. Представьте модель защиты доступа к компьютерной сети. Перечислите службы (функции) защиты компьютерной сети, дайте им определение.
4. Представьте структурно (рисунком) модели многозвенной и многоуровневой защиты информации и поясните их.
5. Представьте модель защиты компьютерной системы, какие составляющие имеет технология защиты информации и какие основные задачи необходимо решить при разработке конкретного средства защиты информации для этой модели.
6. На какие вопросы должна давать ответы политика безопасности предприятия?
7. Перечислите (представьте рисунками) виды нарушений в компьютерных системах и дайте им определение. Представьте классификацию нарушений в терминах пассивных и активных атак.
8. Перечислите (представьте структурно на рисунке) методы обеспечения безопасности процессов переработки информации,

составляющих основу механизмов защиты в компьютерных системах. Какие функции защиты информации включает метод управления доступом.

9. Представьте классификацию методов и средств предотвращения угроз шпионажа и диверсий. Поясните применение системы охраны объекта и противодействие подслушиванию.

10. Перечислите базовые технологии (механизмы) безопасности информации в компьютерных системах. Дайте определение процессам идентификации, аутентификации и авторизации для обеспечения защиты информации.

11. Представьте классификацию методов и средств предотвращения угроз шпионажа и диверсий. Поясните организацию работы с конфиденциальными информационными ресурсами, противодействие наблюдению и защиту от злоумышленных действий обслуживающего персонала и пользователей компьютерной системы.

12. Перечислите базовые технологии (механизмы) безопасности информации в компьютерных системах. Дайте определение технологии защищенного канала.

13. Представьте классификацию методов предотвращения угроз несанкционированного доступа в компьютерных системах.

14. Перечислите (представьте структурно на рисунке) атаки на политику безопасности и процесс административного управления в компьютерной системе.

15. Перечислите формальные и неформальные средства обеспечения безопасности процессов переработки информации, составляющих основу механизмов защиты в компьютерных системах.

16. Каким требованиям должна удовлетворять безопасная информационная система.

17. Представьте классификацию методов и средств предотвращения случайных угроз компьютерных систем.

18. В чем заключается концепция построения виртуальных защищенных сетей VPN. Как формируется сеть VPN, дайте определение ей и ее основным устройствам, приведите пример пакета, подготовленного для туннелирования.

19. Представьте классификацию криптографических методов предотвращения угроз информационной безопасности в компьютерных системах. Каким требованиям должны отвечать современные методы шифрования.

20. Перечислите (представьте структурно на рисунке) атаки на постоянные компоненты системы защиты информации в компьютерной системе.

21. На какие группы подразделяются методы и средства парирования угроз информационной безопасности в компьютерных системах, представьте классификацию методов и средств парирования угроз от электромагнитных излучений и наводок. Поясните активные методы парирования угроз от электромагнитных излучений и наводок.

22. Перечислите (представьте структурно на рисунке) атаки на сменные элементы системы защиты информации в компьютерной системе.

23. На какие группы подразделяются методы и средства парирования угроз информационной безопасности в компьютерных системах, представьте классификацию методов и средств парирования угроз от электромагнитных излучений и наводок. Поясните пассивные методы парирования угроз от электромагнитных излучений и наводок.

24. Перечислите (представьте структурно на рисунке) атаки на протоколы информационного взаимодействия в компьютерной системе.

25. На какие группы подразделяются методы и средства нейтрализации угроз информационной безопасности в компьютерных системах, представьте классификацию методов и средств борьбы с компьютерными вирусами. В чем заключаются методы: сканирования, обнаружения изменений и эвристический анализ для поиска вирусов.

26. Перечислите (представьте структурно на рисунке) нападения на функциональные элементы компьютерных сетей.

27. На какие группы подразделяются методы и средства нейтрализации угроз информационной безопасности в компьютерных системах, представьте классификацию методов и средств борьбы с компьютерными вирусами. В чем заключаются методы использования резидентных сторожей и аппаратно-программной защиты от вирусов.

28. Условия (правила) безопасной работы компьютерных систем и технология обнаружения заражения вирусами.

29. Программно-аппаратные комплексы противодействия несанкционированному межсетевому доступу. Функции, схема подключения и структура межсетевого экрана.

30. Контроль целостности и системные вопросы защиты программ и данных на этапе эксплуатации компьютерных систем.

31. Программно-аппаратные комплексы противодействия несанкционированному межсетевому доступу. Типы межсетевых экранов, поясните действие экранирующего маршрутизатора.

32. Перечислите и поясните этапы построения системы информационно-компьютерной безопасности, недостатки которых могут использоваться для разработки атак.

33. Программно-аппаратные комплексы противодействия несанкционированному межсетевому доступу. Типы межсетевых экранов, поясните действие шлюза сеансового уровня.

34. Перечислите и поясните функции системы защиты информации, которые следует проанализировать при поиске уязвимостей компьютерных систем.

35. Программно-аппаратные комплексы противодействия несанкционированному межсетевому доступу. Типы межсетевых экранов, поясните действие прикладного шлюза.

36. Представьте классификацию VPN сети по уровням модели OSI (эталонной модели взаимодействия открытых систем (ЭМ ВОС)), дайте определение этим группам. Представьте классификацию VPN по архитектуре технического решения и по способу технической реализации.

37. Какие протоколы формирования защищенного канала относятся к канальному уровню модели OSI (эталонной модели взаимодействия открытых систем (ЭМ ВОС)). Представьте архитектуру протоколов PPTP и L2TP, поясните их

38. Перечислите и поясните протоколы формирования защищенного канала на сеансовом уровне модели OSI (эталонной модели взаимодействия открытых систем (ЭМ ВОС)).

39. . Поясните протокол формирования защищенного канала на сетевом уровне модели OSI (эталонной модели взаимодействия открытых систем (ЭМ ВОС)), представьте его архитектуру и поясните (какие протоколы в него входят, поясните их).

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Защита информационных процессов в компьютерных системах», составляет 98 часов. На самостоятельную работу – 46 часов. При этом аудиторная нагрузка состоит из 32 лекционных часов и 32 часов лабораторных работ.

Обучающийся получает теоретические знания на лекциях. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Подготовка к лабораторным работам предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению лабораторных работ. Основной лабораторных работ является выполнение заданий с последующим предоставлением отчета о выполнении.

В рамках указанной дисциплины итоговой формы аттестации является экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов лабораторных работ.

Методические указания для написания реферата

Прежде всего, нужно выбрать тему реферата и подобрать соответствующую литературу. После ознакомления с литературой следует приступить к составлению плана. План реферата должен состоять из названия (темы), введения, основной части, заключения и списка использованной литературы (3-5 работ). Основная часть, как правило, разбивается на дополнительные вопросы (не более 3-4).

Объём реферата должен быть не менее 12 машинописных страниц.

Во введении описывается цель, задачи работы, а также раскрываются смысл и значение основных понятий выбранной темы, область их применения.

В основной части необходимо:

г) ещё раз уточнить тему работы;

д) разбить основную часть работы на дополнительные вопросы;

е) дать ответы на эти вопросы, получив вспомогательные результаты. На их основе дать ответ на основной вопрос. Допускаются ссылки на дополнительную литературу.

В заключении подводятся итоги исследования. Заключение не должно быть большим по объёму.