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

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)

«СОГЛАСОВАНО»
Руководитель ОП
_____ Боршевников А.Е.

«УТВЕРЖДАЮ»
И.о. директора департамента
_____ Боршевников А.Е.
«25» марта 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Защита информационных процессов в компьютерных системах
Направление 10.03.01 Информационная безопасность
Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)
Форма подготовки очная

курс 4 семестр 7
лекции 32 час.
практические занятия 34 час.
лабораторные работы 34 час.
В том числе с использованием МАО лек. 0 / пр. 0 / лаб. 0 час.
всего часов аудиторной нагрузки 100 час.
в том числе с использованием МАО 32 час.
самостоятельная работа 80 час.
в том числе на подготовку к экзамену 36 час.
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 науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427.

Рабочая программа обсуждена на заседании департамента информационной безопасности протокол № 5а от «15» февраля 2022 г.

И.о. директора департамента информационной безопасности Боршевников А.Е.

Составитель доц. Дзенскевич Е.А.

Владивосток

2022

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании департамента:

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

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании департамента:

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

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании департамента:

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

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании департамента:

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

Заведующий кафедрой _____ _____
(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).

Код и наименование профессиональной компетенции (результат освоения)	**Код и наименование индикатора достижения компетенции**
ПК-1 Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1.1 Определяет состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	ПК-1.2 Администрирует работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	ПК-1.3 Применяет средства контроля работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-2 Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2.1 Определяет состав программных средств системного, прикладного и специального назначения
	ПК-2.2 Осуществляет проверки работоспособности программных средств системного, прикладного и специального назначения
	ПК-2.3 Применяет программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы

	программирования для решения профессиональных задач

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения)
ПК-1.1 Определяет состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает программные интерфейсы настроек политик управления доступом в операционных системах Умеет использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации Владеет навыками настройки антивирусной защиты в соответствии с действующими требованиями
ПК-1.2 Администрирует работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает архитектуру и принципы построения и защиты операционных систем Умеет использовать криптографические протоколы, применяемые в компьютерных сетях Владеет настройкой программных и аппаратных средств построения компьютерных сетей, в том числе использующих криптографическую защиту информации
ПК-1.3 Применяет средства контроля работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает принципы функционирования сетевых протоколов, включающих криптографические алгоритмы Умеет настраивать правила обработки пакетов в компьютерных сетях Владеет навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации
ПК-2.1 Определяет состав программных средств системного, прикладного и специального назначения	Знает классификацию современных компьютерных средств системного, прикладного и специального назначения Умеет применять принципы функционирования программных средств криптографической защиты информации Владеет навыками обеспечения безопасности в базах данных
ПК-2.2 Осуществляет проверки работоспособности программных средств системного, прикладного и специального назначения	Знает критерии оценки эффективности и надежности средств защиты программного обеспечения Умеет применять аналитические и компьютерные модели систем защиты информации Владеет навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации
ПК-2.3 Применяет программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знает основные угрозы безопасности информации и модели нарушителя Умеет оценивать информационные риски Владеет навыками расчета показателей эффективности защиты информации

Для формирования вышеуказанных компетенций в рамках дисциплины 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 являются:

Обозначение	Виды учебных занятий и работы обучающегося
Лек	Лекции
Лаб	Лабораторные работы
Пр	Практические занятия
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	7	16	34	16		44	36	экзамен
2	Виды моделей разграничения доступа	7	16		18				
	Итого:		32	34	34		44	36	

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел 1. Классификация угроз, понятия. (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.

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

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

Практические занятия (34ч)

Раздел 1.

Занятие 1.

Основные элементы теории компьютерной безопасности.

Основная аксиома.

Проблема построения защищенной КС.

Модели ценности информации.

Занятие 2.

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.

Раздел 2.

Занятие 3.

Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ).

Анализ безопасности систем ХРУ.

Монооперационные системы ХРУ.

Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ.

Занятие 4.

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 дос-тупа в произвольном графе доступов при отсутствии ограничений на кооперацию субъектов.

Элементы расширенной модели Take-Grant.

Де-факто правила преобразования графов доступов и информационных потоков.

Занятие 5.

Субъектно-ориентированная модель изолированной программной среды (ИПС).

Объекты, функционально ассоциированные с субъектами.

Мониторы безопасности обращений и порождения субъектов.

Базовая теорема ИПС.

Лабораторные занятия (34ч)

Тема 1. Основные угрозы информации в компьютерных системах

Тема 2. Специфика возникновения угроз в открытых сетях

Тема 3. Особенности защиты информации на узлах компьютерной сети с использованием криптографических методов

Тема 4. Администрирование серверных систем и приложений

Тема 5. Использование межсетевых экранов для защиты информационных процессов

Тема 6. Требования к защите автоматизированных систем от НСД

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Защита информационных процессов в компьютерных системах» 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	Раздел 1. Классификация угроз, понятия.	ПК-1 ПК-2	Знает	ПР-7, ПР-6	Вопросы к экзамену 1-28
			Умеет	ПР-6	Вопросы к экзамену 1-28
			Владеет	ПР-6	Вопросы к экзамену 1-28
2	Раздел 2. Виды моделей разграничения доступа	ПК-1 ПК-2	Знает	ПР-7, ПР-6	Вопросы к экзамену 29-39
			Умеет	ПР-6	Вопросы к экзамену 29-39
			Владеет	ПР-6	Вопросы к экзамену 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 ФОС.

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

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

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

В рамках указанной дисциплины итоговой формой аттестации является экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов.

Методические указания для подготовки к лабораторным занятиям

Структура отчета по лабораторной работе

Отчеты по лабораторным работам представляются в электронной форме, подготовленные как текстовые документы в редакторе MSWord.

Отчет должен быть обобщающим документом, включать всю информацию по выполнению заданий, в том числе таблицы список литературы необходимыми пояснениями и иллюстрациями.

Структурно отчет по лабораторной работе, как текстовый документ, комплектуется по следующей схеме:

✓ *Титульный лист – обязательная* компонента отчета, первая страница отчета, по принятой для лабораторных работ форме (титульный лист отчета должен размещаться в общем файле, где представлен текст отчета);

✓ *Исходные данные к выполнению заданий* – обязательная компонента отчета, с новой страницы, содержат указание варианта, темы и т.д.);

✓ *Основная часть* – материалы выполнения заданий, разбивается по рубрикам, соответствующих заданиям работы, с иерархической структурой: разделы – подразделы – пункты – подпункты и т. д.

Рекомендуется в основной части отчета заголовки рубрик (подрубрик) давать исходя из формулировок заданий, в форме отглагольных существительных;

✓ *Выводы* – обязательная компонента отчета, содержит обобщающие выводы по работе (какие задачи решены, оценка результатов, что освоено при выполнении работы);

✓ *Список литературы* – обязательная компонента отчета, с новой страницы, содержит список источников, использованных при выполнении работы, включая электронные источники (список нумерованный, в соответствии с правилами описания библиографии);

✓ *Приложения* – необязательная компонента отчета, с новой страницы, содержит дополнительные материалы к основной части отчета.

Оформление отчета по лабораторной работе

Необходимо обратить внимание на следующие аспекты в оформлении отчетов работ:

- набор текста;
- структурирование работы;
- оформление заголовков всех видов (рубрик-подрубрик-пунктов-подпунктов, рисунков, таблиц, приложений);
- оформление перечислений (списков с нумерацией или маркировкой);
- оформление таблиц;
- оформление иллюстраций (графики, рисунки, фотографии, схемы, «скриншоты»);
- набор и оформление математических выражений (формул);
- оформление списков литературы (библиографических описаний) и ссылок на источники, цитирования.

Набор текста

Набор текста осуществляется на компьютере, в соответствии со следующими требованиями:

✓ печать – на одной стороне листа белой бумаги формата А4 (размер 210 на 297 мм.);

✓ интервал межстрочный – полуторный;

✓ шрифт – TimesNewRoman;

✓ размер шрифта – 14 пт., в том числе в заголовках (в таблицах допускается 10-12 пт.);

✓ выравнивание текста – «по ширине»;

✓ поля страницы – левое - 30 мм., правое - 10 мм., верхнее и нижнее - 20 мм.;

✓ нумерация страниц – в правом нижнем углу страницы (для страниц с книжной ориентацией), сквозная, от титульного листа до последней страницы, арабскими цифрами (первой страницей считается титульный лист, на котором номер не ставиться, на следующей странице проставляется цифра «2» и т. д.).

✓ режим автоматического переноса слов, за исключением титульного листа и заголовков всех уровней (перенос слов для отдельного абзаца блокируется средствами MSWord с помощью команды «Формат» – абзац при выборе опции «запретить автоматический перенос слов»).

Если рисунок или таблица размещены на листе формата больше А4, их следует учитывать, как одну страницу. Номер страницы в этих случаях допускается не проставлять.

Список литературы и все *приложения* включаются в общую сквозную нумерацию страниц работы.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус D, ауд. D 733,733а. Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 13) Оборудование: ЖК-панель 47", Full HD, LG M4716 CCBA – 1 шт. Доска аудиторная, Моноблок Lenovo C360G-i34164G500UDK с лицензионными программами Microsoft Office 2013(13 шт.) и аудиовизуальными средствами проектор Panasonic DLPProjectorPT-D2110XE	1С Предприяти8 (8.2), 7-Zip, ABBYY Lingvo12,Alice 3, Anaconda3,Autodesk,CodeBlocks,CorelDRAW X7,Dia,Directum4.8,DosBox-0.74,Farmanager,Firebird 2.5,FlameRobin,Foxit Reader,Free Pascal,Geany,Ghostscript,Git,Greenfoot,gsview,Inscape0.91,Java,Java development Kit,Kaspersky,Lazarus,LibreOffice4.4,MatLab R2017b,Maxima 5.37.2,Microsoft Expression,Microsoft Office 2013,Microsoft Silverlight,Microsoft Silverlight 5SDK-русский,MicrosoftSistem Center,Microsoft Visial Studio 2012,MikTeX2.9,MySQL,NetBeans,Notepad++,Oracle VM VirtualBox,PascalABC.NET,PostgreSQL 9.4,PTC Mathcad,Putty,PyQt GPL v5.4.1 for Pythonv 3.4,Pyton2.7(3.4,3.6),QGIS Brighton,RStudio,SAM CoDeC Pack,SharePoint,Strawberry Perl,Tecnomatix,TeXnicCenter,TortoiseSVN,Unity2017.3.1f1, Veusz,Vim8.1,Visual Paradigm CE,Visual Studio2013,Windows Kits,Windows Phone SDK8.1,Xilinx

		Design ToolsAcrobat ReaderDC,AdobeBridge CS3,AdobeDeviceCentralCS3,Adobe ExtendScript Toolkit 2,Adobe Photoshope CS3,DVD-студия Windows,GoogleChrome,Internet Explorer,ITMOproctor,Mozilla Firefox, Visual Studio Installer,Windows Media Center, WinSCP,
690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус А, ауд. А1042 Аудитория для самостоятельной работы студентов	Моноблок Lenovo C360G-i34164G500UDK – 115 шт.; Интегрированный сенсорный дисплей Polymedia FlipBox; Копир-принтер-цветной сканер в e-mail с 4 лотками Xerox WorkCentre 5330 (WC5330C; Полноцветный копир-принтер-сканер Xerox WorkCentre 7530 (WC7530CPS Оборудование для инвалидов и лиц с ограниченными возможностями здоровья: Дисплей Брайля Focus-40 Blue – 3 шт.; Дисплей Брайля Focus-80 Blue; Рабочая станция Lenovo ThinkCentre E73z – 3 шт.; Видео увеличитель ONYX Swing-Arm PC edition; Маркер-диктофон Touch Memo цифровой; Устройство портативное для чтения плоскопечатных текстов PEarl; Сканирующая и читающая машина для незрячих и слабовидящих пользователей SARA; Принтер Брайля Emprint SpotDot - 2 шт.; Принтер Брайля Everest - D V4; Видео увеличитель ONYX Swing-Arm PC edition; Видео увеличитель Topaz 24” XL стационарный электронный; Обучающая система для детей тактильно-речевая, либо для людей с ограниченными возможностями здоровья; Увеличитель ручной видео RUBY портативный – 2 шт.; Экран Samsung S23C200B; Маркер-диктофон Touch Memo цифровой.	Microsoft Windows 7 Pro MAGic 12.0 Pro, Jaws for Windows 15.0 Pro, Open book 9.0, Duxbury BrailleTranslator, Dolphin Guide (контракт № А238-14/2); Неисключительные права на использование ПО Microsoft рабочих станций пользователей (контракт ЭА-261-18 от 02.08.2018): - лицензия на клиентскую операционную систему; - лицензия на пакет офисных продуктов для работы с документами включая формат.docx , .xlsx , .vsd , .ptt.; - лицензия па право подключения пользователя к серверным операционным системам , используемым в ДВФУ : Microsoft Windows Server 2008/2012; - лицензия на право подключения к серверу Microsoft Exchange Server Enterprise; - лицензия па право подключения к внутренней информационной системе документооборота и порталу с возможностью поиска информации во множестве удаленных и локальных хранилищах, ресурсах, библиотеках информации, включая портальные хранилища, используемой в ДВФУ: Microsoft SharePoint; - лицензия на право подключения к системе централизованного управления рабочими станциями, используемой в ДВФУ: Microsoft System Center.

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	Работа с литературой. Подготовка к практическим и лабораторным занятиям.	44	Отчет о выполнении
2	Сессия	Подготовка к экзамену	36	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.

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.

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения)
ПК-1.1 Определяет состав работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает программные интерфейсы настроек политик управления доступом в операционных системах Умеет использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации Владеет навыками настройки антивирусной защиты в соответствии с действующими требованиями
ПК-1.2 Администрирует работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает архитектуру и принципы построения и защиты операционных систем Умеет использовать криптографические протоколы, применяемые в компьютерных сетях Владеет настройкой программных и аппаратных средств построения компьютерных сетей, в том числе использующих криптографическую защиту информации
ПК-1.3 Применяет средства контроля работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает принципы функционирования сетевых протоколов, включающих криптографические алгоритмы Умеет настраивать правила обработки пакетов в компьютерных сетях Владеет навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации
ПК-2.1 Определяет состав программных средств системного, прикладного и специального назначения	Знает классификацию современных компьютерных средств системного, прикладного и специального назначения Умеет применять принципы функционирования программных средств криптографической защиты информации Владеет навыками обеспечения безопасности в базах данных
ПК-2.2 Осуществляет проверки работоспособности программных средств системного, прикладного и специального назначения	Знает критерии оценки эффективности и надежности средств защиты программного обеспечения Умеет применять аналитические и компьютерные модели систем защиты информации Владеет навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации
ПК-2.3 Применяет программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знает основные угрозы безопасности информации и модели нарушителя Умеет оценивать информационные риски Владеет навыками расчета показателей эффективности защиты информации

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Раздел 1. Классификация угроз, понятия.	ПК-1 ПК-2	Знает	ПР-7, ПР-6	Вопросы к экзамену 1-28
			Умеет	ПР-6	Вопросы к экзамену 1-28
			Владеет	ПР-6	Вопросы к экзамену 1-28
2	Раздел 2. Виды моделей разграничения доступа	ПК-1 ПК-2	Знает	ПР-7, ПР-6	Вопросы к экзамену 29-39
			Умеет	ПР-6	Вопросы к экзамену 29-39
			Владеет	ПР-6	Вопросы к экзамену 29-39

Текущая аттестация

ПР-7 Конспект - продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции.

Цели конспектирования состоят в:

- развитии умений систематизировать знания и выделять причинно-следственные связи, выявлять закономерности;

- развитии умений перерабатывать любую информацию, придавая ей иной вид, тип, форму;

- развитии навыков осмысленной переработки текста, структурирования информации, использования основных категорий анализа, работы с большими объемами информации;

- создании модели проблемы (понятийную или структурную).

Требования к представлению и оцениванию материалов (результатов):

В связи с объективным характером конспектирования не предлагается единых и обязательных параметров конспектируемого текста (степень сокращения информации). Объем законспектированного текста определяется самим студентом. Конспект должен быть подготовлен каждым студентом самостоятельно и отражать основные идеи изученной темы.

Перечень вопросов, необходимых для конспектирования определяется темой лекционного занятия. Конспекты выполняются во время лекционных занятий, и проверяются преподавателем в конце семестра.

Критерии оценки:

Уровень освоения	Критерии оценки результатов обучения	Количество баллов / оценка
Повышенный	Конспекты лекций в наличии. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Логически корректное изложение материала.	100-86 Зачтено
Базовый	Конспекты лекций в наличии. Студент показывает умение пользоваться концептуально-понятийным аппаратом. В целом логически корректное, но не всегда точное изложение материала.	85-76 Зачтено
Пороговый	Конспекты лекций в наличии. Студент показывает затруднение с использованием научно-понятийного аппарата; частичные затруднения с выполнением конспекта.	75-61 Зачтено
Уровень не достигнут	Конспекты лекций отсутствуют или студент показывает отрывочное представление о теме.	60-0 Не зачтено

Лабораторная работа (ПР-6) – средство для закрепления и практического освоения материала по определенной теме.

Цель лабораторных работ – выработка у учащихся профессиональных умений применять полученные знания для решения практических задач, умений и навыков пользоваться подходами и методами информационной безопасности для осуществления профессиональной деятельности.

Во всех лабораториях существуют особые правила поведения студентов, которые необходимо неукоснительно соблюдать – правила техники безопасности. За знание правил техники безопасности и обязательство их выполнять каждый студент должен расписаться в соответствующем журнале.

Обработка результатов и оформление отчета проводится в течение недели после выполнения работы. Студент, не сдавший отчета в срок, к следующей работе не допускается.

Требования к представлению и оцениванию материалов (результатов):

Выполнение лабораторной работы осуществляется студентом самостоятельно в часы лабораторных занятий.

При оценке работы студента преподаватель учитывает все этапы работы студента над отчетом. Если отчет не был принят преподавателем и возвращен для доработки, то все исправления вносятся в тот же экземпляр отчета.

При оценке учитывается правильность выполнения отчета. Выставляется дифференцированный зачет.

Критерии оценки:

Уровень освоения	Критерии оценки результатов обучения	Количество баллов / оценка
Повышенный	Студент показал прочные знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, знание методов, используемых в работе, методики обработки результатов. Показано хорошее понимание профессиональной значимости изучаемых вопросов. При выполнении экспериментальной части работы и оформлении отчета студент показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в соответствии с требованиями, структурирован, не содержит ошибок; правильно и полно сформулирован вывод по работе.	100 – 86 Зачтено (отлично)
Базовый	Студент показал знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, знание методов, используемых в работе, методики обработки результатов. Показано хорошее понимание профессиональной значимости изучаемых вопросов. При выполнении экспериментальной части работы и оформлении отчета студент показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в основном – в соответствии с	85-76 Зачтено (хорошо)

	требованиями, структурирован; правильно и полно сформулирован вывод по работе. Допускаются не более 2-х недочетов в оформлении отчета.	
Пороговый	Студент показал базовые знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, демонстрирует, в целом, знание методов, используемых в работе, методики обработки результатов. При выполнении экспериментальной части работы и оформлении отчета студент в целом показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в основном в соответствии с требованиями, не содержит грубых ошибок, вывод по работе сформулирован.	75-61 Зачтено (удовлетворительно)
Уровень не достигнут	Студент не выполнил лабораторную работу, либо показал незнание основных понятий, сущности процессов, рассматриваемых в работе, демонстрирует плохое знание или незнание методов, методики обработки результатов. Слабо сформировано или не сформировано умение работать с данными, отсутствуют выводы по результатам работы. Отчет не соответствует требованиям, не сделан или сделан с грубыми ошибками.	60-0 Не зачтено (неудовлетворительно)

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).

Критерии выставления оценки студенту на экзамене:

Баллы (рейтинговой оценки)	Оценка (стандартная)	Требования к сформированным компетенциям
86-100	«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
76-85	«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
61-75	«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно

		правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
0-60	«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения по дисциплине				
Оценка / виды оценочных средств	2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
Знания *(виды оценочных средств: конспект, лабораторная работа)*	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения *(виды оценочных средств: лабораторная работа)*	Отсутствие умений	В целом успешное, но не систематическое умение	В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера)	Успешное и систематическое умение
Навыки (владения, опыт деятельности)	Отсутствие навыков (владений, опыта)	Наличие отдельных навыков (наличие фрагментарного опыта)	В целом, сформированные навыки (владения), но используемые не в активной форме	Сформированные навыки (владения), применяемые при решении задач