МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ИГУ»)

Институт математики и информационных технологий

Кафедра алгебраических и информационных систем

«УТВЕРЖДАЮ»
Директор ИМИТ ИГУ
_____ М. В. Фалалеев
«15» мая 2024 г.

Рабочая программа дисциплины (модуля)

Б1.О.27 Информационная безопасность

Направление подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль) подготовки Фундаментальная информатика и информационные технологии

Квалификация выпускника бакалавр

Форма обучения очная

Иркутск 2024 г.

1. Цели и задачи дисциплины

Цель

Цели: ознакомление студентов с теоретическими основами информационной безопасности, основами криптографии и основами обеспечения защиты информации, формирование практических умений и навыков, необходимых для приобретения квалификации бакалавра информационных технологий, формирование ключевых профильных компетенций.

Задачи:

- дать специальные знания по дисциплине;
- достичь достаточного уровня знаний по криптографическим и организационным методам обеспечения информационной безопасности;
- сформировать у студентов практические навыки работы со средствами обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

2.1. Учебная дисциплина (модуль) относится к обязательной части программы и изучается на третьем курсе.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, сформированные Б1.О.21 Вычислительные системы и компьютерные сети.

2.3. Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: Б1.О.31 Стандартизация, сертификация и управление качеством программного обеспечения, Б1.О.28 Архитектура программного обеспечения, Б1.В.15 Администрирование компьютерных сетей.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций (элементов следующих компетенций) в соответствии с ФГОС ВО по соответствующему направлению подготовки.

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ИДК УК2.1 Формулирует цели, задач, значимости, ожидаемых результатов проекта	Знает международные и национальные стандарты в области информационной безопасности; Умеет составлять политики безопасности уровня методов предприятия; Владеет основными навыками защиты информации;
	ИДК УК2.2 В рамках поставленных задач определяет имеющиеся ресурсы и ограничения, действующие правовые нормы	Знает основные нормативные правовые документы в сфере информационной безопасности; Умеет составлять политики безопасности уровня методов предприятия;

		Владеет основными навыками защиты информации;
	ИДК $_{УК2.3}$ Разрабатывает план реализации проекта	Знает основные виды угроз информационной безопасности и способы противодействия этим угрозам; Умеет составлять политики безопасности уровня методов предприятия; Владеет основными навыками защиты информации;
	ИДК $_{УК2.4}$ Осуществляет контроль реализации проекта	Знает основные виды угроз информационной безопасности и способы противодействия этим угрозам; Умеет анализировать и выбирать средства обеспечения информационной безопасности; Владеет приемами анализа и классификации угроз информационной безопасности;
	ИДК $_{УК2.5}$ Проводит оценку эффективности реализации проекта и разработку плана действий по его корректировке	Знает основные виды угроз информационной безопасности и способы противодействия этим угрозам; Умеет анализировать и выбирать средства обеспечения информационной безопасности; Владеет приемами анализа и классификации угроз информационной безопасности;
ОПК-5 Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	ИДК $_{ОПК5.1}$ Знает основы системного администрирования, современные стандарты информационного взаимодействия систем	Знает основные средства обеспечения информационной безопасности; Умеет соблюдать основные требования по противодействию наиболее распространенным угрозам информационной безопасности; Владеет основными навыками использования нормативных документов при организации обеспечения информационной безопасности на предприятии;
	ИДК $_{ОПК5.2}$ Способен инсталлировать программное обеспечение	Знает формальные модели безопасности;

	информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	Умеет соблюдать основные требования по противодействию наиболее распространенным угрозам информационной безопасности; Владеет основными навыками использования нормативных документов при организации обеспечения информационной безопасности на предприятии;
	ИДК $_{ОПК5.3}$ Способен выполнять настройку и сопровождение информационных систем и баз данных с учетом информационной безопасности	Знает формальные модели безопасности; Умеет соблюдать основные требования по противодействию наиболее распространенным угрозам информационной безопасности; Владеет основными навыками использования нормативных документов при организации обеспечения информационной безопасности на предприятии;
ОПК-2 Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение, в том числе отечественного происхождения, для решения задач профессиональной деятельности	ИДК $_{ОПК2.1}$ Понимает базовые принципы и устройство современных информационных технологий и программных средств	Знает основные прикладные алгоритмы криптографии; инфраструктуру открытых ключей; Умеет анализировать алгоритмы взаимодействия на наличие уязвимостей; Владеет навыками реализации прикладных алгоритмов криптографии в языках программирования, работы с криптопровайдерами, использования криптографических примитивов в языках программирования.
	ИДК $_{ОПК2.2}$ Способен применять современное программное обеспечение (в том числе отечественного производства) для решения задач профессиональной деятельности	Знает основные прикладные алгоритмы криптографии; инфраструктуру открытых ключей; Умеет анализировать алгоритмы взаимодействия на наличие уязвимостей; Владеет навыками реализации прикладных алгоритмов криптографии в языках программирования, работы с криптопровайдерами,

		использования криптографических примитивов в языках программирования.
	ИДК $_{ОПК2.3}$ Способен применять суперкомпьютерные методы для решения задач профессиональной деятельности	Знает основные прикладные алгоритмы криптографии; инфраструктуру открытых ключей; Умеет анализировать алгоритмы взаимодействия на наличие уязвимостей; Владеет навыками реализации прикладных алгоритмов криптографии в языках программирования, работы с криптопровайдерами, использования криптографических примитивов в языках программирования.

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 4 зачетных единиц, 144 часа, в том числе 35 часов на контроль, практическая подготовка 144.
Форма промежуточной аттестации: 6 семестр - экзамен.

4.1. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ, С УКАЗАНИЕМ ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ И ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)				Формы текущего контроля успеваемости
			Контактная работа преподавателя с обучающимися			Самостоятельная работа + контроль	
			Лекции	Семинарские (практические занятия)	Контроль обучения		
	Раздел 1. Криптографические основы информационной безопасности	6			5		
	Тема 1.1. Основы криптографии		4	4		8	Опрос, защита отчета о лабораторной работе
	Тема 1.2. Блочное шифрование		4	4		8	Опрос, защита отчета о лабораторной работе
	Тема 1.3. Целостность сообщений		4	4		8	Опрос, защита отчета о лабораторной работе
	Тема 1.4. Цифровая подпись		4	4		8	Опрос, защита отчета о лабораторной работе

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)				Формы текущего контроля успеваемости
			Контактная работа преподавателя с обучающимися			Самостоятельная работа + контроль	
			Лекции	Семинарские (практические занятия)	Контроль обучения		
	Раздел 2. Организационные основы информационной безопасности	6			5		
	Тема 2.1. Нормативные основы информационной безопасности		4	4		10	Опрос, защита отчета о лабораторной работе
	Тема 2.2. Виды и классификация возможных нарушений информационной безопасности		4	4		10	Опрос, защита отчета о лабораторной работе
	Тема 2.3. Политика безопасности		4	4		10	Опрос, защита отчета о лабораторной работе
	Тема 2.4. Безопасность беспроводных сетей		4	4		8	Опрос, защита отчета о лабораторной работе
Итого часов			32	32	10	70	

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
6	**Тема 1.1. Основы криптографии**	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	2 неделя	8	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru
6	**Тема 1.2. Блочное шифрование**	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	4 неделя	8	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
6	**Тема 1.3. Целостность сообщений**	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	6 неделя	8	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru
6	**Тема 1.4. Цифровая подпись**	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	8 неделя	8	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
6	**Тема 2.1. Нормативные основы информационной безопасности**	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	10 неделя	10	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru
6	**Тема 2.2. Виды и классификация возможных нарушений информационной безопасности**	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	12 неделя	10	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
6	**Тема 2.3. Политика безопасности**	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	14 неделя	10	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru
6	**Тема 2.4. Безопасность беспроводных сетей**	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	16 неделя	8	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru
Общая трудоемкость самостоятельной работы по дисциплине (час)				70		
Из них объем самостоятельной работы с использованием электронного обучения и дистанционных образовательных технологий (час)						

4.3. Содержание учебного материала

РАЗДЕЛ 1. КРИПТОГРАФИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ

БЕЗОПАСНОСТИ
ТЕМА 1.1. Основы криптографии
Общие принципы и модели. Защита от несанкционированного доступа. Понятие ключа. Шифрование и кодирование. Криптосистемы. Шифр Вернама. Лемма о теоретически стойком шифре. Потоковые шифры.
ТЕМА 1.2. Блочное шифрование
Принцип итерирования. Понятие псевдослучайной функции и псевдослучайной перестановки. Шифр DES. Описание структуры. Шифр AES. Описание структуры и принципы работы. Переборные атаки на блочные шифры. Переборные атаки на блочные шифры. Проблема Случайное шифрование. Одноразовое шифрование. Режим CBC. Набивка блоков. Режим CTR.
ТЕМА 1.3. Целостность сообщений
Коды аутентификации сообщений. Построение кодов аутентификации больших сообщений. Конструкции CBC-MAC и NMAC. Хеш-функции. Конструкция Меркла-Дамгарда для построения хеш-функций. Понятие целостности шифр-текста. Аутентичное шифрования на примере протокола TLS.
ТЕМА 1.4. Цифровая подпись
Понятие цифровой подписи. Основные принципы и отличия от реальной подписи. Алгоритмы цифровой подписи. DSS. ГОСТ. Закон об ЭЦП в России. Различные виды подписи. Удостоверяющие центры. Понятие ключа подписи. Инфраструктура открытых ключей (PKI).
РАЗДЕЛ 2. ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ТЕМА 2.1. Нормативные основы информационной безопасности
Направления ИБ. Механизмы. Инструментарий. Методы защиты информации. Виды противников и нарушителей информационной безопасности. Международные стандарты информационного обмена. Категории прав на информацию. Служебная, коммерческая и государственная тайны. Сведения, не составляющие коммерческую и государственную тайну. Закон «Об информации, информационных технологиях и о защите информации». Закон «О персональных данных». Закон «Об электронной подписи».
ТЕМА 2.2. Виды и классификация возможных нарушений информационной безопасности
Понятие угрозы и уязвимости. Классификации угроз. Три вида нарушений безопасности. Меры по противодействию угрозам нарушения конфиденциальности, целостности, доступности. Построение модели угроз и методики оценки рисков. Качественные и количественные методики оценки рисков. Классификация компьютерных вирусов. Меры по их профилактике. Методология защиты информационных систем.
ТЕМА 2.3. Политика безопасности
Цели и задачи организации. Взаимодействие между субъектами. Правила безопасности. Уровни формирования политик безопасности.
ТЕМА 2.4. Безопасность компьютерных сетей
Беспроводные сети стандартов 802.11. Особенности защиты информации в беспроводных сетях. Основные угрозы и уязвимости. Режимы функционирования и шифрования данных в беспроводных сетях.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/н	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции (индикаторы)*
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1	1.1	ЛР «Основы криптографии»	4	4	устный опрос, письменные задания	УК-2 (ИДК УК2.1), ОПК-2 (ИДК ОПК2.1)
2	1.2	ЛР «Блочное шифрование»	4	4	устный опрос, письменные задания	УК-2 (ИДК УК2.1), ОПК-2 (ИДК ОПК2.1)
3	1.3	ЛР «Простое хэширование»	4	4	устный опрос, письменные задания	УК-2 (ИДК УК2.1), ОПК-2 (ИДК ОПК2.1)
4	1.4	ЛР «Формирование электронной подписи в VipNet»	4	4	устный опрос, письменные задания	УК-2 (ИДК УК2.1), ОПК-2 (ИДК ОПК2.1), ОПК-5
5	2.1	ЛР «Изучение государственной системы защиты информации»	4	4	устный опрос, письменные задания	УК-2 (ИДК УК2.2), ОПК-2 (ИДК ОПК2.2, ОПК2.3)
6	2.2	ЛР «Определение факторов, воздействующих на информацию», ЛР «Метод экспертных оценок»	4	4	устный опрос, письменные задания	УК-2 (ИДК УК2.2), ОПК-2 (ИДК ОПК2.2, ОПК2.3)
7	2.3	ЛР «Анализ политики безопасности с помощью MSAT»	4	4	устный опрос, письменные задания	УК-2 (ИДК УК2.3 УК2.4), ОПК-2 (ИДК ОПК2.2, ОПК2.3), ОПК-5 (ИДК ОПК5.1)
8	2.4	ЛР «Проектирование системы защиты информации»	4	4	устный опрос, письменные задания	УК-2 (ИДК УК2.3, УК2.4, УК

						2.5), ОПК-2 (ИДК ОПК2.2, ОПК2.3), ОПК-5 (ИДК ОПК5.2, ОПК5.3)
		Всего	32			

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СР)

Тема	Задание	Формируемые компетенции
Тема 2.1 Нормативные основы информационной безопасности	Состав документов на объект информатизации и ИСКИИ. Требования к защите сетей связи общего пользования.	УК-2 (ИДК УК2.2), ОПК-2 (ИДК ОПК2.2, ОПК2.3), ОПК-5 (ИДК ОПК5.1)
Тема 2.2. Виды и классификация возможных нарушений информационной безопасности	Методика определения угроз безопасности	УК-2 (ИДК УК2.2), ОПК-2 (ИДК ОПК2.2, ОПК2.3)
Тема 2.3. Политика безопасности	Рекомендованные приемы разработки правил информационной безопасности	УК-2 (ИДК УК2.3 УК2.4), ОПК-2 (ИДК ОПК2.2, ОПК2.3)
Тема 2.4. Безопасность компьютерных сетей	Инженерно-техническая укрепленность объекта.	УК-2 (ИДК УК2.3, УК2.4, УК 2.5), ОПК-2 (ИДК ОПК2.2, ОПК2.3), ОПК-5 (ИДК ОПК5.2, ОПК5.3)

4.4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Во время изучения дисциплины студент посещает лекции, практические занятия, выполняет лабораторные задания, готовится к тестам, зачетам и экзаменам. Для каждого вида деятельности необходимо правильно организовать самостоятельную работу.

Лекции. В высшем учебном заведении лекция является важной формой учебного процесса. На лекции студенты получают глубокие и разносторонние знания. Лекция способствует развитию творческих способностей, формирует идейную убежденность, позволяет устанавливать связь учебного материала с производством, новейшими научными достижениями. Лекция требует три вида деятельности: подготовку к лекции, работу на лекции и работу после лекции.

После прослушивания лекции студент должен проработать и осмыслить полученный материал. На каждый пример, приведенный на лекции, желательно, (если это возможно) привести свой. Для утверждений, приведенных на лекции, можно попытаться привести другие формулировки, не меняя, конечно же, сути утверждения. Утверждения станут более понятными, если привести примеры, подтверждающие справедливость утверждения и примеры, которые не удовлетворяют условиям, при которых утверждение становится справедливым. Материал, изложенный в лекции, можно просмотреть в других источниках.

В процессе лекционного занятия студент должен выделять важные моменты, выводы, анализировать основные положения. Недостаточно только «слушать» лекцию. Возможности памяти человека не универсальны. Как бы внимательно студент не слушал лекцию,

большая часть информации вскоре после восприятия будет забыта. Чтобы восстановить лекционный материал, его нужно повторить, а для этого лекцию необходимо конспектировать. Конспект лекций должен быть в отдельной тетради, в которой не должно быть ничего, кроме лекции. Не надо стремиться подробно слово в слово записывать всю лекцию. Конспектируйте только самое важное в рассматриваемом параграфе: формулировки определений и теорем, выводы основных уравнений и формул, то, что старается выделить лектор, на чем акцентирует внимание студентов, при этом формулировки определений и утверждений надо постараться записать так, как их формулирует преподаватель.

Тетрадь для конспекта лекций также требует особого внимания. Ее нужно сделать удобной, практичной и полезной, ведь именно она является основным информативным источником при подготовке к различным отчетным занятиям, зачетам, экзаменам. Конечно, оформление лекционной тетради – это дело вкуса. Но целесообразно отделить поля, где студент мог бы изложить свои мысли, вопросы, появившиеся в ходе лекции. Полезно одну из страниц оставлять свободной. Она потребуется потом, при самостоятельной подготовке. Сюда можно будет занести дополнительную информацию по данной теме, полученную из других источников: чертежи и рисунки, схемы и графики, цитаты и биографии выдающихся ученых и т.д.

Практическое занятие. Практические занятия по решению задач существенно дополняют лекции. В процессе анализа и решения задач студенты расширяют и углубляют знания, полученные из лекционного курса и учебников, приобретают умение применять общие закономерности к конкретным случаям. На практических занятиях по дискретной математике используются: 1) задачи-упражнения, помогающие студентам приобрести твёрдые навыки расчёта и вычислений; 2) задачи для закрепления и контроля знаний; 3) познавательные задачи.

Необходимо, чтобы студенты готовили теоретический материал, потому, что именно невыполнение этого требования приводит к неудаче при решении задач.

Несмотря на различие в видах задач, их решение можно проводить по следующему общему плану (некоторые пункты плана могут выпадать в некоторых конкретных случаях): а) прочесть внимательно условие задачи; б) посмотреть, все ли термины в условиях задачи известны и понятны (если что-то неясно, следует обратиться к учебнику, просмотреть решения предыдущих задач, посоветоваться с преподавателем); в) сделать чертёж, если это необходимо; г) произвести анализ задачи, (нужно чётко понимать, в чем будет заключаться решение задачи); д) решить задачу; е) проанализировать полученный ответ.

Если задача не решена или «не решается», то необходимо еще раз вернуться к пунктам а) и б). Сколько раз нужно возвращаться к этим пунктам? Практика показывает, что не более десяти раз. Если и после этого задача «не решается», то можно попытаться найти решение этой или похожей задачи в различных источниках.

Домашнее задание. При выполнении домашнего задания необходимо просмотреть текст лекции, выучить новые определения, формулировки теорем, формулы, посмотреть задания, которые были выполнены на практике и применить полученные знания для выполнения домашней работы.

Тест. В первую очередь постарайтесь узнать чего ждать от теста, какие примерно там будут задания. Если вам доступны образцы теста (как, например, при сдаче ЕГЭ), необходимо этим воспользоваться и ежедневно тренироваться.

Не оставляйте все на самый последний момент. Если будете постоянно готовиться к тесту, вы наверняка улучшите свои знания. Для этого составьте план на каждый день, чтобы правильно распределять свое время.

Делайте небольшие перерывы во время учебы. В промежутках можно дать себе небольшую физическую нагрузку. Мозг лучше всего работает, когда умственный труд сменяется физическим. Прогуляйтесь, побегайте, поиграйте в баскетбол, попинайте мяч - помимо стимуляции умственной деятельности, это снимет стресс.

Отдых и контроль над волнением — одни из главных составляющих успеха при подготовке к тесту. Часто ошибки совершаются только из-за стресса, который мешает сконцентрироваться и собраться. Чтобы быть отдохнувшим и расслабленным, соблюдайте составленный режим и старайтесь высыпаться.

Работа с литературой. Во время лекций студенту предлагается найти ответы на некоторые вопросы в предложенных источниках литературы. Студент должен проработать каждый источник, найти ответ на вопрос во всех источниках, где он есть и сформулировать ответ, систематизировав информацию.

Экзамен. На экзамене оцениваются: 1) понимание и степень усвоения теории; 2) методическая подготовка; 3) знание фактического материала; 4) знакомство с обязательной литературой, может быть, с современными публикациями по данному курсу; 5) умение приложить теорию к практике, решать практические задачи и т. д.; 6) знакомство с историей науки; 7) логика, структура и стиль ответа, умение защищать выдвигаемые положения. Но значение экзаменов не ограничивается проверкой знаний. Являясь естественным завершением работы студента, они способствуют обобщению и закреплению знаний и умений, приведению их в строгую систему, а также устранению возникших в процессе занятий пробелов.

При подготовке к экзаменам не следует также оставлять без вывода утверждения, которые в книге или лекции сопровождаются замечаниями: «Легко доказать, что...», «Легко получить выражение...» и т. п. Все пропущенные в книге или в лекции преобразования студенту нужно проделать самостоятельно.

Студенты готовятся к экзаменам по-разному. Одни из них прорабатывают лишь некоторые вопросы, выбранные наугад, другие стремятся запомнить весь материал подряд, не вникая глубоко в его суть. Работа при этом концентрируется на одном стремлении - сдать экзамен. Недостатки такой системы очевидны. Очевидно также, что подготовка не должна ограничиваться чтением лекционных записей. Первоначальные необработанные конспекты студента содержат факты, определения, выводы, сделанные преподавателем, но в них, как правило, слабо просматривается связующая идея курса, так как студент, записывая каждую лекцию в отдельности, редко способен сразу и достаточно точно уловить общую направляющую мысль. Поэтому конспект требует дополнительной обработки на основе использования учебников и рекомендованной литературы.

Существенные недостатки имеет и такой способ подготовки к экзаменам, как беглый просмотр всего материала. Он эффективен только на некоторых этапах планирования и закрепляющего повторения. Более надежный и целесообразный путь – это тщательная систематизация материала при вдумчивом повторении, запоминании формулировок, установлении внутрипредметных связей, увязке различных тем и разделов, закреплении путем решения задач.

Перед экзаменом назначается консультация. Цель ее – дать ответы на вопросы, возникшие в ходе самостоятельной подготовки. Хотелось бы обратить особое внимание на важность предэкзаменационных консультаций. Здесь студент имеет полную возможность получить ответ на все неясные ему вопросы. А для этого он должен проработать до консультации весь курс. Кроме того, преподаватель будет отвечать на вопросы других студентов, что будет для вас повторением и закреплением знаний. И еще очень важное обстоятельство: лектор на консультации, как правило, обращает внимание на те разделы, по которым на предыдущих экзаменах ответы были неудовлетворительными,

а также фиксирует внимание на наиболее трудных разделах курса. Некоторые студенты не приходят на консультации либо потому, что считают, что у них нет вопросов к лектору, либо полагают, что у них и так мало времени и лучше самому почитать материал по конспекту или в учебнике. Это глубокое заблуждение. Никакая другая работа не сможет принести столь значительного эффекта накануне экзамена, как консультация преподавателя.

Подготовку к экзамену следует начинать с первого дня изучения дисциплины. Как правило, на лекциях подчеркиваются наиболее важные и трудные вопросы или разделы курса, требующие внимательного изучения и обдумывания. Нужно эти вопросы выделить и обязательно постараться разобраться в них, не дожидаясь экзамена, проработать их, готовясь к практическим или лабораторным занятиям, попробовать самостоятельно решить несколько типовых задач. И если, несмотря на это, часть материала осталась неусвоенной, ни в коем случае нельзя успокаиваться, надеясь на то, что это не попадется на экзамене. Факты говорят об обратном: если те или другие вопросы курса не вошли в экзаменационный билет, преподаватель может их задать (и часто задает) в виде дополнительных вопросов. Точно такое же отношение должно быть выработано к вопросам и задачам, перечисленным в экзаменационной программе, выдаваемой студентам еще до экзамена. Обычно эти же вопросы и аналогичные задачи содержатся в экзаменационных билетах. Не следует оставлять без внимания ни одного раздела курса; если не удалось в чем-то разобраться самому, нужно обратиться к товарищам; если и это не помогло выяснить какой-либо вопрос до конца, нужно обязательно задать этот вопрос преподавателю на предэкзаменационной консультации. Чрезвычайно важно приучить себя к умению самостоятельно мыслить, учиться думать, понимать суть дела. Очень полезно после проработки каждого раздела восстановить в памяти содержание изученного материала, кратко записав это на листе бумаги. Если этого не сделать, то большая часть материала останется не понятой, а лишь формально заученной, и при первом же вопросе экзаменатора студент убедится в том, насколько поверхностно он усвоил материал.

4.5. Примерная тематика курсовых работ (проектов)

Не предусмотрено.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) перечень литературы

а) основная литература

1. Введение в криптографию / ред. В. В. Ященко. – М.: Изд-во МЦНМО, 2012. – 347 с. – ISBN: 978-5-4439-0026-1 (26 экз.) +

2. Рябец Л.В. Задачник-практикум по криптографии: учеб. пособие / Л.В. Рябец. – Иркутск : Изд-во Вост-Сиб. гос. акад. образ., 2013. – 76 с. – ISBN: 978-5-85827-864-1 (19 экз.)

3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М.: ДМК-Пресс. – 2010. – 542 с. – ISBN: 978-5-94074-518-1 (25 экз.)

4. Келлеров А. С., Корольков Ю. Д. Основы информационной безопасности : учеб. пособие. – Иркутск: Изд-во ИГУ, 2013. – 113 с. . – ISBN: 978-5-9624-0791-3 (30 экз.)

б) дополнительная литература

5. Герман О.Н. Теоретико-числовые методы в криптографии: учебник для студ. учреждений высш. проф. образования / О.Н. Герман. – М.: Академия. – 2012. – 257 с. – ISBN: 978-5-7695-6786-5. Режим доступа: ЭЧЗ «Библиотех». – Неогранич. доступ.

6. Конеев И. Р. Информационная безопасность предприятия: научное издание / И. Р. Конеев, А. В. Беляев. – СПб.: БХВ-Петербург, 2003. – 733 с. – ISBN 5-94157-280-8 (40 экз).

7. Бабаш А.В. Информационная безопасность. Лабораторный практикум: учеб. пособие / А. В. Бабаш. – М.: КноРус, 2013. – 131 с. – ISBN 978-5-406-02760-8 (50 экз.).

8. Глухов М.М. Введение в теоретико-числовые методы криптографии / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. – СПб.: Лань. – 2011. – 400 с. – ISBN: 978-5-8114-1116-0. Режим доступа: ЭБС «Лань». – Неогранич. доступ.

б) периодические издания

не предусмотрено

в) список авторских методических разработок:

Конспекты лекций по дисциплине, учебное видео в ЭОР дисциплины на EDUCA

г) базы данных, информационно-справочные и поисковые системы

1. Некоммерческая Интернет-версия «Консультант Плюс» www.consultant.ru
2. Банк данных угроз ИБ bdu.fstec.ru
3. Официальный интернет-портал правовой информации pravo.gov.ru
4. Единое окно доступа к образовательным ресурсам window.edu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Компьютерный класс на 25 мест.

Оборудование: Специализированная (учебная) мебель; доска для мела/маркера, оборудование для презентации учебного материала: проектор, экран, персональные компьютеры, доступ в Интернет.

6.2. Программное обеспечение:

Среды программирования:

1. Java
2. Visual C++
3. Lasarus
4. Python

СКЗИ:

5. VipNet

Офисное ПО:

6. LibreOffice

6.3. Технические и электронные средства:

Электронный ресурс дисциплины в EDUCA, презентационное оборудование, персональный компьютер с возможностью демонстрации презентаций в формате pdf.

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для достижения планируемых результатов обучения, в дисциплине «Информационная безопасность», используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими. Используется самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений, обеспечивающих возможность качественно выполнять профессиональную деятельность. Используется анализ поведенческих ошибок, создание образцов документов, поиск оптимальных решений конкретной производственной проблемы методом «brain-storming».

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: коллективная мыслительная деятельность в группах при выполнении индивидуальных групповых заданий, поиск оптимальных решений в рамках предложенной ситуации.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при проведении ролевых игр, при выполнении домашних индивидуальных заданий, на еженедельных консультациях.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Оценочные материалы для входного контроля

Не предусмотрен

8.2. Оценочные материалы текущего контроля

Вид контроля	Контролируемые темы	Контролируемые компетенции (индикаторы компетенций)
Защита отчета о лабораторной работе	1.1 - 2.4	УК-2, ОПК-2, ОПК-5, в составе ИДК согласно разделу 4.3.1 РПД

Оценочные материалы текущего контроля (задания на лабораторную работу, требования к отчёту о выполнении ЛР, контрольные вопросы) размещены на ЭОР дисциплины в ИОС EDUCA.

Примеры оценочных средств текущего контроля

Контрольные вопросы к лабораторной работе «Создание ЭП в ViPNet»

1.Что является единицей разграничения доступа в защищенной сети?
2.Зачем нужны списки рассылки копий?
3.Что нужно сделать в ЦУС, чтобы заново начать генерацию DST файлов?
4.Что должен сделать администратор при смене мастер-ключа?
5.Что содержится в DST файле?
6.Где задаются полномочия (права доступа пользователя)?
7.Для какой программы задаются полномочия?
8.Что происходит при нажатии кнопки «Сформировать все справочники» в «ЦУС»?
9.Что такое сетевой узел?
10.Что такое Главные абоненты?
11.Где хранится мастер-ключ?
12.Что находится на ключевой дискете?
13.Для чего служит ключевой набор?

8.3. Оценочные материалы промежуточного контроля

Список вопросов для промежуточной аттестации:

1. Почему компьютерные вирусы причисляют к особому классу разрушающих программных воздействий. Раскройте основные каналы распространения компьютерных вирусов и других вредоносных программ.
2. 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.
3. Дайте определение основным понятиям процесса разграничения доступа к объектам операционной системы (ОС): «объект доступа»; «метод доступа»; «субъект доступа»; «право доступа». Приведите правила мандатного (полномочного) разграничения доступа и поясните их.
4. Приведите классификацию криптографических алгоритмов и охарактеризуйте их. Раскройте смысл функционирования схемы шифрования в алгоритме DES. Основные режимы работы блочного симметричного алгоритма.
5. Перечислите и поясните возможные типы сетевых атак на компьютерные (информационные) системы, какие существуют технологии построения систем обнаружения атак.
6. Перечислите защитные механизмы, реализуемые программно-аппаратными комплексами (средствами) защиты информации в компьютерных системах (ПЭВМ). Дайте определение понятию - «субъект доступа», какие процедуры реализуются при его обращении к компьютерной системе.
7. Перечислите атрибутивные идентификаторы, используемые для идентификации субъекта доступа в КС, и коротко дайте им определение. Перечислите рекомендации для организации парольной защиты.
8. Какими способами блокируется угроза несанкционированного копирования информации ПЭВМ, в чем они заключаются, раскройте их содержание.
9. Как осуществляемся управление криптоключами, требования к распределению ключей, методы распределения ключей, поясните схему открытого распределения ключей Диффи-Хеллмана
10. Раскройте процедуры алгоритмов цифровой подписи на основе отечественных стандартов ГОСТ Р 34.10.

11. Основные подходы к защите данных от НСД: какие действия выполняются при организации доступа к оборудованию и ПО компьютерных систем (ПЭВМ); оценка эффективности наращивания средств контроля доступа по кривой роста относительного уровня обеспечения безопасности компьютерных систем (ПЭВМ).
12. Приведите классификацию криптографических алгоритмов и охарактеризуйте их. Раскройте смысл функционирования схемы шифрования в алгоритме ГОСТ 28147-89. Основные режимы работы блочного симметричного алгоритма.
13. Какие основные функции выполняет подсистема защиты операционных систем (ОС), дайте коротко им определение. В чем заключается процедура аудита применительно к ОС, чем она обусловлена, каким требованиям она должна удовлетворять?
14. Перечислите базовые технологии (механизмы) безопасности информации в компьютерных системах. Дайте определение процессам идентификации, аутентификации и авторизации для обеспечения защиты информации. Приведите и раскройте типы процессов аутентификации, какие атаки проводятся на протоколы аутентификаций и какие механизмы применяются для их отражения.
15. Дайте определение и поясните технологии построения систем обнаружения сетевых вторжений и выявления признаков атак на информационные системы.
16. Перечислите и раскройте способы строгой аутентификации. Поясните на структурной схеме применение односторонней хэш-функции к сообщению, дополненному секретным ключом.
17. Поясните на структурных схемах простую аутентификацию пользователя ресурсов компьютерной системы с использованием пароля и аутентификацию, основанную на использовании односторонней хэш-функции для проверки пароля.
18. Дайте определение основным понятиям процесса разграничения доступа к объектам операционной системы (ОС): «объект доступа»; «метод доступа»; «субъект доступа»; «право доступа». Приведите правила избирательного разграничения доступа и поясните их реализацию на примере матрицы доступа, дайте определение понятиям: домен доступа; список прав доступа.
19. В чем заключается задача идентификации пользователя, дайте определение понятию протокола идентификации. В чем заключается локальная и удаленная идентификация, что такое идентифицирующая информация.
20. Перечислите и раскройте способы строгой аутентификации. Поясните на структурной схеме применение для аутентификации односторонней хэш-функции с параметром-ключом.
21. Какими способами блокируется угроза несанкционированного копирования информации ПЭВМ, в чем они заключаются, раскройте их содержание.
22. Какие существуют криптосистемы шифрования, раскройте их смысл функционирования.
23. Приведите классификацию криптографических алгоритмов и охарактеризуйте их. Раскройте процедуру хэширования по алгоритму ГОСТ Р 34.11.
24. Приведите классификацию криптографических алгоритмов и охарактеризуйте их.
25. В чем заключается биометрическая аутентификация пользователей, какие у нее достоинства и недостатки.
26. В чем заключается процедура простой аутентификации, какими способами она производится, поясните схематично ее реализацию с использованием пароля.
27. Раскройте основные процедуры формирования электронной цифровой подписи и функции хэширования.
28. Приведите классификацию криптографических алгоритмов и охарактеризуйте их. Раскройте алгоритм шифрования RSA.
29. Перечислите методы противодействия дизассемблированию программ для ЭВМ, охарактеризуйте их.
30. Перечислите методы ограничения доступа к компонентам ЭВМ, какие применяют средства для ограничения доступа к компонентам ЭВМ.
31. Раскройте основные методы аутентификации, использующие пароли и PIN-коды.

Примеры оценочных средств для промежуточной аттестации:

Примеры заданий экзаменационного теста:
№1
Политика безопасности - это
а) документ верхнего уровня, цель которого обеспечение решения вопросов информационной безопасности и вовлечение высшего руководства организации в данный процесс
б) совокупность документов, регламентирующих правила обращения с конфиденциальной информацией в зависимости от фазы ее обработки и категории конфиденциальности
в) совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации предприятия

№2
На федеральном уровне приоритеты обеспечения информационной безопасности определяются
а) Доктриной информационной безопасности РФ
б) Федеральными законами
в) Политикой безопасности

№3
Фактор, воздействующий на информацию - это...
а) явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней
б) совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее
в) субъект, случайно или преднамеренно совершивший действие, следствием которого является возникновение и/или реализация угроз нарушения безопасности информации

№4
Обязательными к использованию при оценке угроз безопасности информации, обрабатываемой в информационных системах персональных данных и государственных информационных являются сведения из:

а) Банка данных угроз информационной безопасности ФСТЭК России
б) Государственного стандарта «Факторы, воздействующие на информацию»
в) Kaspersky Threat Landscape

№5
Если полномочия субъекта представляются списком ресурсов, доступных пользователю, и правами по доступу к каждому ресурсу из списка, то такой метод называется...

а) дискреционным
б) мандатным
в) ролевым

№6
Угрозу перехвата данных можно отнести к угрозам...
а) конфиденциальности
б) целостности
в) доступности

№7
Можно ли обеспечить 100% защиту от всех видов ущерба?
а) нет, и целью защиты информации становится уменьшение размеров ущерба до допустимых значений.
б) да, но сделать это невозможно экономически целесообразным способом
в) иногда, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба

№8
Дискреционное управление доступом - это...
а) разграничение доступа между поименованными субъектами и поименованными объектами
б) разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и допуска субъектов к информации соответствующего уровня конфиденциальности
в) организация прав доступа субъектов к объектам сгруппированных с учетом специфики их применения

№9
Метод защиты программы от исследования путем обфускации заключается в:
а) различной сложности преобразовании кода в процессе его выполнения
б) автоматической генерации участков исполняемого кода в процессе выполнения
в) создании избыточности указателей перехода, и внедрении взаимоувязанных нефункциональных участков кода, затрудняющих анализ декомпилированного текста

№10
Сертификация средств криптографической защиты информации осуществляется при участии:
а) ФСБ России
б) ФСТЭК России
в) Роскомнадзора

№11
Обычный способ идентификации - это...
а) ввод имени пользователя при входе в систему
б) пароль
в) изучение физиологических и поведенческих характеристик субъекта

№12
К достоинству моделей дискреционного доступа можно отнести...
а) их гибкость

б) возможность наложения ограничений на передачу информации от одного пользователя другому
в) контроль информационных потоков

Разработчики:

(подпись) старший преподаватель (занимаемая должность) Муценек В.Е. (Ф.И.О.)

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.03 «Прикладная информатика» (уровень бакалавриата), утвержденный приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 г. № 922, зарегистрированный в Минюсте России «12» октября 2017 г. № 48531 с изменениями и дополнениями от 26.11.2020, 8.02.2021.

Программа рассмотрена на заседании кафедры Алгебраических и информационных систем ИМИТ ИГУ «04» апреля 2023 г.

Протокол № 9 Зав. кафедрой_____ Пантелеев В. И.