МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета информационных технологий и компьютерной безопасности
_____ Гусев П.Ю.
«21» декабря 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Специальные методы информационной безопасности»

Направление подготовки 09.04.01 Информатика и вычислительная техника

Профиль Искусственный интеллект

Квалификация выпускника магистр

Нормативный период обучения 2 года / 2 года и 5 м.

Форма обучения очная / заочная

Год начала подготовки 2022

Автор программы _____ /Паринов М.В./

Заведующий кафедрой
Компьютерных
интеллектуальных
технологий проектирования _____ /М.И. Чижов/

Руководитель ОПОП _____ /М.И. Чижов/

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

- понимание моделей и стандартов информационной безопасности;
- усвоение методов защиты информационных систем;
- приобретение теоретических знаний и практических навыков по использованию современных программных средств для обеспечения информационной безопасности и защиты информации от несанкционированного использования.
- формирование у студентов мотивации к самообразованию за счет активизации самостоятельной познавательной деятельности.

1.2. Задачи освоения дисциплины

- изучение и классификация причин нарушений безопасности;
- проектирование мониторов безопасности субъектов и объектов;
- приобретение практических навыков работы с современными сетевыми фильтрами и средствами криптографического преобразования информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Специальные методы информационной безопасности» относится к дисциплинам части, формируемой участниками образовательных отношений (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Специальные методы информационной безопасности» направлен на формирование следующих компетенций:

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

ПК-2 - Способен участвовать в решении профессиональных проектных задач, выбирать и реализовывать командную роль в работе над проектом в соответствии с приоритетами собственной деятельности

Компетенция	Результаты обучения, характеризующие сформированность компетенции
УК-1	Знать классификацию причин нарушений безопасности;
	Уметь сравнительный анализ параметров систем защиты информации
	Владеть навыками выбора корректных средств защиты информации

ПК-2	Знать современное состояние и тенденции развития методов информационной безопасности;
	Уметь разрабатывать, выбирать и тестировать программные средства защиты информации
	Владеть навыками разработки ПО для защиты информации

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Специальные методы информационной безопасности» составляет 4 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		3
Аудиторные занятия (всего)	36	36
В том числе:		
Лекции	16	16
Лабораторные работы (ЛР)	20	20
Самостоятельная работа	108	108
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: час	144	144
зач.ед.	4	4

заочная форма обучения

Виды учебной работы	Всего часов	Семестры
		3
Аудиторные занятия (всего)	12	12
В том числе:		
Лекции	4	4
Лабораторные работы (ЛР)	8	8
Самостоятельная работа	128	128
Часы на контроль	4	4
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: час	144	144
зач.ед.	4	4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Основы информационной безопасности	Концептуальная модель информационной безопасности. Понятие политики безопасности. Основные информационные угрозы	4	4	18	26
2	Причины нарушения безопасности	Исследование причин нарушений безопасности. Анализ опасности. Методики противодействия. Реализация и гарантирование политики безопасности.	4	4	18	26
3	Защищенные сети	Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей. Создание механизмов безопасности в распределенной компьютерной системе.	2	4	18	24
4	Методы криптографии	Анализ существующий подходов. Типы шифрования. Симметричные и несимметричные шифры. Анализ криптостойкости. Цифровая электронная подпись.	2	4	18	24
5	Разработка криптографических систем	Разработка программных продуктов, использующих основные алгоритмы шифрования. Использование типовых библиотек. Алгоритмизация. Протоколы шифрования	2	2	18	22
6	Реализация защищенных информационных систем	Модели безопасного субъектного взаимодействия в компьютерной системе. Аутентификация пользователей. Сопряжение защитных механизмов. Использование программных средств собственной разработки для защиты информации	2	2	18	22

Итого	**16**	**20**	**108**	**144**

заочная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Основы информационной безопасности	Концептуальная модель информационной безопасности. Понятие политики безопасности. Основные информационные угрозы	2	2	20	24
2	Причины нарушения безопасности	Исследование причин нарушений безопасности. Анализ опасности. Методики противодействия. Реализация и гарантирование политики безопасности.	2	2	20	24
3	Защищенные сети	Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей. Создание механизмов безопасности в распределенной компьютерной системе.	-	2	22	24
4	Методы криптографии	Анализ существующий подходов. Типы шифрования. Симметричные и несимметричные шифры. Анализ криптостойкости. Цифровая электронная подпись.	-	2	22	24
5	Разработка криптографических систем	Разработка программных продуктов, использующих основные алгоритмы шифрования. Использование типовых библиотек. Алгоритмизация. Протоколы шифрования	-	-	22	22
6	Реализация защищенных информационных систем	Модели безопасного субъектного взаимодействия в компьютерной системе. Аутентификация пользователей. Сопряжение защитных механизмов. Использование программных средств собственной разработки для защиты информации	-	-	22	22
Итого			**4**	**8**	**128**	**140**

5.2 Перечень лабораторных работ

Исследование и изучение структуры средств безопасности операционных систем и использование их для конфиденциального доступа к информации.

Разработка и реализация алгоритма функционирования системы безопасности объектов.

Разработка и реализация алгоритма функционирования системы безопасности субъектов.

Разработка и реализация алгоритма сетевого фильтра.

Разработка и реализация алгоритма криптографического преобразования.

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
УК-1	Знать классификацию причин нарушений безопасности;	Тестирование, защита лабораторных работ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь сравнительный анализ параметров систем защиты информации	Тестирование, защита лабораторных работ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками выбора корректных средств защиты информации	Тестирование, защита лабораторных работ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-2	Знать современное состояние и тенденции развития методов информационной безопасности;	Тестирование, защита лабораторных работ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	Уметь разрабатывать, выбирать и тестировать программные средства защиты информации	Тестирование, защита лабораторных работ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками разработки ПО для защиты информации	Тестирование, защита лабораторных работ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 3 семестре для очной формы обучения, 3 семестре для заочной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
УК-1	Знать классификацию причин нарушений безопасности;	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь сравнительный анализ параметров систем защиты информации	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть навыками выбора корректных средств защиты информации	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПК-2	Знать современное состояние и тенденции развития методов информационной безопасности;	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь разрабатывать, выбирать и тестировать программные средства защиты информации	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть навыками разработки ПО для защиты информации	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1.	Шифрование-это: ❖ процесс создания алгоритмов шифрования ❖ процесс сжатия информации ❖ **процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется**
2.	В каком случае построение цифровой подписи не требует наличия в системе третьего лица – арбитра, занимающегося аутентификацией? ❖ **при шифровании с помощью ассимметричного алгоритма** ❖ при шифровании с помощью симметричного алгоритма ❖ арбитр необходим всегда
3.	Можно ли отнести слабую аутентификацию к проблемам безопасности? ❖ нет ❖ **да** ❖ в редких случаях
4.	1. Возможно ли расшифровывать информацию без знания ключа? ❖ нет ❖ **да** ❖ в редких случаях
5.	Возможно ли вычислить закрытый ключ ассиметричного алгоритма, зная открытый? ❖ **нет** ❖ да ❖ в редких случаях
6.	Характерная черта алгоритма Эль-Гамаля состоит в : ❖ **протоколе передачи подписанного сообщения, позволяющего подтверждать подлинность отправителя** ❖ в точной своевременной передаче сообщения ❖ алгоритм не имеет особенностей и идентичен RSA
7.	Аутентификацией называют: ❖ процесс регистрации в системе ❖ способ защиты системы ❖ **процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов**
8.	Аутентификация бывает: ❖ статическая ❖ устойчивая ❖ постоянная ❖ **все варианты правильные** ❖ правильного варианта нет
9.	Стойкость ключа характеризуется ❖ длинной ❖ непредсказуемостью

	❖ **все варианты правильные** ❖ правильного варианта нет
10	Условие, при котором в распоряжении аналитика находиться возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера n используется в анализе: ❖ **на основе произвольно выбранного шифротекста** ❖ **на основе произвольно выбранного открытого текста** ❖ на основе только шифротекста

7.2.2 Примерный перечень заданий для решения стандартных задач

1.	Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи возникает: ❖ **со стороны злоумышленника** ❖ со стороны законного отправителя сообщения ❖ со стороны законного получателя сообщения
2.	Какие алгоритмы используют один и тот же ключ для шифрования и дешифровки? ❖ асимметричный ❖ **симметричный** ❖ правильного ответа нет
3.	Процесс нахождения открытого сообщения соответственно заданному закрытому при неизвестном криптографическом преобразовании называется: ❖ шифрование ❖ дешифровка ❖ расшифровка
4.	В каких основных форматах существует симметричный алгоритм? ❖ блока и строки; ❖ **потока и блока;** ❖ потока и данных
5.	Открытым текстом в криптографии называют: ❖ расшифрованный текст ❖ любое послание ❖ **исходное послание**
6.	Какой ключ известен только приемнику? ❖ открытый ❖ **закрытый** основании какой информации создается сетевой маршрут?
7.	Наука, занимающаяся защитой информации, путем преобразования этой информации это: ❖ криптография ❖ **криптология** ❖ криптоанализ

8.	В каких **шифрах результат шифрования очередного блока зависит только от** него самого и не зависит от других блоков шифруемого массива данных? ❖ в потоковых ❖ **в блочных**
9.	Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это: ❖ шифр функциональных преобразований ❖ шифр замен ❖ **шифр перестановок**
10	Функция, предназначенная для выработки блока данных, используемого для модификации шифруемого блока, из инварианта и ключевого элемента называется: ❖ **функция шифрования шага преобразования** ❖ **инвариант стандартного шага шифрования**

7.2.3 Примерный перечень заданий для решения прикладных задач

1	**Условие,** при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им *массива открытых данных* размера n используется в анализе: ❖ **на основе произвольно выбранного шифротекста** ❖ **на основе произвольно выбранного открытого текста** ❖ правильного ответа нет
2	Как называется модификация DESa ❖ Triple Des+ ❖ M-506 ❖ Deh
3	Какие перестановки существуют в стандарте DES ❖ простые+ ❖ расширенные+ ❖ сокращенные+
4	Сколько существует перестановок в стандарте DES ❖ 3+ ❖ 4 ❖ 2
5	Зашифрованный файл, хранящийся на логическом диске, который подключается к системе как еще один логический диск – это… ❖ виртуальный контейнер+ ❖ файл ❖ программа
6	Устройство, дающее статически случайный шум – это… ❖ генератор случайных чисел+ ❖ контроль ввода на компьютер ❖ УКЗД

7	УКЗД – это… ❖ устройство криптографической защиты данных+ ❖ устройство криптографической заданности данных ❖ нет правильного ответа
8	Какой ключ используется в шифре ГОСТ ❖ 256-битовый+ ❖ 246-битовый ❖ 356-битовый
9	Чем отличается блок-схема алгоритма ГОСТ от блок-схемы DES-алгоритма ❖ отсутствием начальной перестановки и числом циклов шифрования+ ❖ длиной ключа ❖ методом шифрования
10	Электронной подписью называется… ❖ присоединяемое к тексту его криптографическое преобразование+ ❖ текст ❖ зашифрованный текст

7.2.4 Примерный перечень вопросов для подготовки к зачету

1.	Исторический подход к защите информации в КС.
2.	Информация – предмет защиты.
3.	Информация – объект защиты.
4.	Случайные угрозы информации в КС.
5.	Преднамеренные угрозы информации в КС.
6.	Защита информации в КС от случайных угроз.
7.	Способы повышения надежности и отказоустойчивости КС.
8.	Защита информации в КС от преднамеренных угроз.
9.	Основные способы НСД.
10.	Физическая защита ПЭВМ от НСД.
11.	Как настроить безопасное соединение
12.	Как настроить защиту беспроводной сети
13.	Как настроить защиту SSH
14.	Как настроить парольную защиту
15.	Как настроить VPN
16.	Как настроить HTTPS
17.	Как настроить FTPS
18.	Как настроить коммутатор с защитой информации
19.	Как настроить динамическую маршрутизацию с шифрованием
20.	Как настроить защиту портов устройства
21.	Основные принципы шифрования DES
22.	Основные принципы шифрования AES
23.	Основные принципы шифрования RSA
24.	Основные принципы шифрования DSA

25.	Основные принципы шифрования на основе шифра Цезаря
26.	Основные принципы шифрования на основе оригинального шифра подстановки
27.	Основные принципы шифрования на основе оригинального шифра перестановки
28.	Отличие обычных и безопасных соединений
29.	Анализ влияния длины ключа на криптостойкость
30.	Анализ современных алгоритмов шифрования

7.2.5 Примерный перечень заданий для подготовки к экзамену

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет выставляется при ответе не менее 70% от полного содержимого вопросов. Допускается мелкие неточности. Основной материал должен быть усвоен полностью.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основы информационной безопасности	УК-1, ПК-5	Тест, защита лабораторных работ
2	Причины нарушения безопасности	УК-1, ПК-5	Тест, защита лабораторных работ
3	Защищенные сети	УК-1, ПК-5	Тест, защита лабораторных работ
4	Методы криптографии	УК-1, ПК-5	Тест, защита лабораторных работ
5	Разработка криптографических систем	УК-1, ПК-5	Тест, защита лабораторных работ
6	Реализация защищенных информационных систем	УК-1, ПК-5	Тест, защита лабораторных работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем

осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Защита информации техническими средствами [Электронный ресурс] : учебное пособие / А.И. Спивак; А.В. Разумовский; Ю.Ф. Каторин; ред. Ю.Ф. Каторин. - Санкт-Петербург : Университет ИТМО, 2012. - 417 с.URL: http://www.iprbookshop.ru/66445.html

Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 284 с. URL: http://biblioclub.ru/index.php?page=book&id=480637

Защита информации : лабораторный практикум / В.И. Смирнов. - Йошкар-Ола : ПГТУ, 2017. - 67 с. - ISBN 978-5-8158-1866-8. URL: http://biblioclub.ru/index.php?page=book&id=476512

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Лицензионное программное обеспечение:

- MS Visual Studio
- Калькулятор
- Блокнот
- Yandex browser

Ресурсы информационно-телекоммуникационной сети «Интернет»:

- Образовательный портал ВГТУ
- docs.microsoft.com

Современные профессиональные базы данных:

- eLIBRARY.RU
- База ГОСТ docplan.ru

Информационные справочные системы:

- wiki.cchgeu.ru
- window.edu.ru

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

- Учебная лаборатория с доступом к локальной сети и сети Интернет (лаборатории 213/2, 202/2, расположенные по адресу г. Воронеж, ул. Плехановская, д. 11)
- Проекционная аппаратура

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Специальные методы информационной безопасности» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие:

	- работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.