ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

Институт приоритетных технологий

Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины (модуля): **Методы и средства криптографической защиты информации**

Уровень ОПОП: Специалитет

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)

Форма обучения: Очная

Срок обучения: 2024 - 2030 уч. г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.01 Компьютерная безопасность (приказ № 1459 от 26.11.2020 г.) и учебного плана, утвержденного Ученым советом (от 26.05.2023 г., протокол № 9)

Разработчики:
Никишова А. В., кандидат технических наук, доцент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 08 от 30.08.2023 года

Зав. кафедрой Какорина О. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - Целью освоения дисциплины является теоретическая и практическая подготовка выпускника в области защиты информации с помощью криптографических методов

Задачи дисциплины:

- изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике
- изучение системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов
- изучение принципов разработки шифров, математических методов, используемых в криптографии

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Методы и средства криптографической защиты информации» относится к обязательной части учебного плана.

Дисциплина изучается на 4 курсе.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций, определенных учебным планом в соответствии с ФГОС ВО.

Выпускник должен обладать следующими общепрофессиональными компетенциями (ОПК):

- ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Знания, умения, навыки, формируемые по компетенции в рамках дисциплины

Студент должен знать:

основные принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

Студент должен уметь:

использовать средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

Студент должен владеть навыками:

навыками и методиками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Седьмой семестр	Восьмой семестр
Контактная работа (всего)	**168**	**84**	**84**
Лабораторные	68	34	34
Лекции	68	34	34
Практические	32	16	16
Самостоятельная работа (всего)	**84**	**60**	**24**
Виды промежуточной аттестации	**36**		**36**
Зачет с оценкой		+	
Экзамен	36		36
Общая трудоемкость часы	**288**	**144**	**144**
Общая трудоемкость зачетные единицы	**8**	**4**	**4**

5. Содержание дисциплины

5.1. Содержание дисциплины: Лекции (68 ч.)

Седьмой семестр. (34 ч.)

Тема 1. Основные понятия и определения (2 ч.)

Основные определения. История криптографии. Операция перестановки. Операция подстановки. Роторные машины.

Тема 2. Частотные характеристики открытых текстов (2 ч.)

Использование для дешифрования частотных характеристик открытого текста.

Тема 3. k-граммная модель открытого текста (2 ч.)

Основания для использования k-граммной модели открытого текста. Неоходимость использования математических моделей открытого текста.

Тема 4. Классификация шифров (2 ч.)

Схема классификации шифров. Симметричные, ассиметричные, шифры замены, шифры перестановки, аддитивные шифры, композиционные шифры, детерминированные шифры, вероятностные шифры, многозначные шифры, однозначные шифры, блочные шифры, поточные шифры.

Тема 5. Модели шифров (2 ч.)

Алгебраическая и вероятностная модели шифров.

Тема 6. Простейшие криптографические протоколы (2 ч.)

Простейшие протоколы односторонней аутентификации. Протоколы аутентификации с использованием паролей.

Тема 7. Шифры перестановки (2 ч.)

Шифры перестановки и шифры замены. Шифр простой замены Юлия Цезаря.

Тема 8. Шифры подстановки (2 ч.)

Одноалфавитный шифр подстановки (шифр простой замены). Однозвучный шифр подстановки. Полиграммный шифр подстановки.

Тема 9. Шифры гаммирования (2 ч.)

Определение гаммирования. Процесс зашифрования сообщения шифром гаммирования. Шифр Виженера.

Тема 10. Алгоритмы формирования гаммы (2 ч.)

Режимы работы алгоритма: простая замена; гаммирование; гаммирование с обратной связью; выработка имитовставки.

Тема 11. Подходы к построению симметричных криптосистем (2 ч.)

Этапы шифрования и дешифрования простой перестановкой. Способы проведения процедуры наложения гаммы на открытый текст.

Тема 12. Подходы к построению симметричных криптосистем (2 ч.)

Характеристики методов построения симметричных криптосистем.

Тема 13. Криптографическая стойкость шифров (2 ч.)

Определение стойкости шифра. Вычислительная стойкость. Информацийно-теоретическая стойкость. Доказуемая стойкость.

Тема 14. Теоретически стойкие шифры (2 ч.)

Абсолютно стойкие (теоретически стойкие) криптографические системы. Требования.

Тема 15. Имитостойкость шифров (2 ч.)

Определение имитостойкости. Способы обеспечения имитостойкости.

Тема 16. Линейный криптоанализ (2 ч.)

Метод линейного криптоанализа. Определение линейных приближений.

Тема 17. Дифференциальный криптоанализ (2 ч.)

Определение дифференциального криптоанализа. Вероятностные отношения. Дифференциальный профайл. Характеристики.

Восьмой семестр. (34 ч.)

Тема 18. Системы шифрования с открытым ключом (2 ч.)

Использование необратимых или односторонних функций. Виды односторонних функций. Алгоритм RSA.

Тема 19. Системы шифрования с открытым ключом (2 ч.)

Последовательность шагов алгоримта RSA. Шаги для шифрования и дешифрования сообщения. Система Эль-Гамаля. Криптосистема Мак-Элиса.

Тема 20. Односторонние функции (2 ч.)

Определение односторонней функции. Односторонние функции с люком.

Тема 21. Односторонние функции (2 ч.)

Свойства односторонней функции. Односторонней функцией с секретом K. Применение функций с секретом.

Тема 22. Ассиметричная криптосистема RSA (2 ч.)

Общая идея. Основные принципы асимметричной криптосистемы RSA. Генерация ключей RSA

Тема 23. Ассиметричная криптосистема RSA (2 ч.)

Шифрование и дешифрование сообщений с помощью RSA. Преимущества и недостатки RSA. Применение RSA в современных системах безопасности.

Тема 24. Шифросистема Эль-Гамаля (2 ч.)

Безопасность схемы Эль-Гамаля. Принцип работы шифрсистемы.

Тема 25. Шифросистема Мак-Элиса (2 ч.)

Параметры шифросистемы Мак-Элиса. Последовательность действий для получения открытого и соответствующего секретного ключа каждому из абонентов системы.

Тема 26. Криптосистемы над группой точек эллиптической кривой (2 ч.)

Определение группы точек эллиптической кривой. Эллиптические кривые в вещественных числах.

Тема 27. Криптосистемы над группой точек эллиптической кривой (2 ч.)

Шифрование/дешифрование с использованием эллиптических кривых. Безопасность криптографии с использованием эллиптических кривых.

Тема 28. Схема открытого распределения ключей Диффи-Хеллмана над группой точек эллиптической кривой (2 ч.)

Описание алгоритма. Протоколы управления криптоключами SKIP (Simple Key management for Internet Protocols) и IKE (Internet Key Exchange).

Тема 29. Практические аспекты использования шифросистем с открытым ключом (2 ч.)

Применение. Преимущества.

Тема 30. Алгоритмы цифровых подписей (2 ч.)

Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля (EGSA).

Тема 31. Алгоритмы цифровых подписей (2 ч.)

Алгоритм цифровой подписи DSA. Компоненты электронной цифровой подписи. Надежность практических реализаций схем создания и проверки ЭЦП

Тема 32. Стандарты цифровой подписи (2 ч.)

Отечественный стандарт цифровой подписи. ГОСТ Р 34.10-2012.

Тема 33. Хэш-функции (2 ч.)

Определение хэш-функции. Классификация. Общая модель хэш-функции.

Тема 34. Хэш-функции (2 ч.)

Требования к хэш-функциям. Свойства, которые должны быть присущи криптографическим хэш-функциям. Применение хэш-функций для проверки истинности сообщений

5.2. Содержание дисциплины: Практические (32 ч.)

Седьмой семестр. (16 ч.)

Тема 1. Основные понятия и определения (2 ч.)

Основные определения. История криптографии. Операция перестановки. Операция

подстановки. Роторные машины.

Тема 2. Частотные характеристики открытых текстов (2 ч.)

Использование для дешифрования частотных характеристик открытого текста.

Тема 3. k-граммная модель открытого текста (2 ч.)

Основания для использования k-граммной модели открытого текста. Неоходимость использования математических моделей открытого текста.

Тема 4. Классификация шифров (2 ч.)

Схема классификации шифров. Симметричные, ассиметричные, шифры замены, шифры перестановки, аддитивные шифры, композиционные шифры, детерминированные шифры, вероятностные шифры, многозначные шифры, однозначные шифры, блочные шифры, поточные шифры.

Тема 5. Модели шифров (2 ч.)

Алгебраическая и вероятностная модели шифров.

Тема 6. Простейшие криптографические протоколы (2 ч.)

Простейшие протоколы односторонней аутентификации. Протоколы аутентификации с использованием паролей.

Тема 7. Шифры перестановки (2 ч.)

Шифры перестановки и шифры замены. Шифр простой замены Юлия Цезаря.

Тема 8. Шифры подстановки (2 ч.)

Одноалфавитный шифр подстановки (шифр простой замены). Однозвучный шифр подстановки. Полиграммный шифр подстановки.

Восьмой семестр. (16 ч.)

Тема 9. Шифры гаммирования (2 ч.)

Определение гаммирования. Процесс зашифрования сообщения шифром гаммирования. Шифр Виженера.

Тема 10. Алгоритмы формирования гаммы (2 ч.)

Режимы работы алгоритма: простая замена; гаммирование; гаммирование с обратной связью; выработка имитовставки.

Тема 11. Подходы к построению симметричных криптосистем (2 ч.)

Этапы шифрования и дешифрования простой перестановкой. Способы проведения процедуры наложения гаммы на открытый текст.

Тема 12. Подходы к построению симметричных криптосистем (2 ч.)

Характеристики методов построения симметричных криптосистем.

Тема 13. Криптографическая стойкость шифров (2 ч.)

Определение стойкости шифра. Вычислительная стойкость. Информацийно-теоретическая стойкость. Доказуемая стойкость.

Тема 14. Теоретически стойкие шифры (2 ч.)

Абсолютно стойкие (теоретически стойкие) криптографические системы. Требования.

Тема 15. Имитостойкость шифров (2 ч.)

Определение имитостойкости. Способы обеспечения имитостойкости.

Тема 16. Системы шифрования с открытым ключом (2 ч.)

Использование необратимых или односторонних функций. Виды односторонних функций. Алгоритм RSA.

5.3. Содержание дисциплины: Лабораторные (68 ч.)

Седьмой семестр. (34 ч.)

Тема 1. Шифр Цезаря. (2 ч.)

Цель работы: изучить основные понятия криптографии, классификацию криптографических систем, подстановочный шифр Цезаря.

Тема 2. Шифр Цезаря. (2 ч.)

Цель работы: ознакомиться с одноалфавитными шифрами подстановки. Получить

практические навыки шифрования и дешифрования текста шифром одноалфавитной подстановки.

Тема 3. Частотный криптоанализ. (2 ч.)

Цель работы: ознакомиться с основными подходами к риптоанализу. Получить практические навыки проведения криптоанализа для одноалфавитных шифров подстановки.

Тема 4. Частотный криптоанализ. (2 ч.)

Цель работы: используя частотный анализ дешифровать криптограмму, зашифрованную методом моноалфавитных подстановок.

Тема 5. Шифр Playfair (2 ч.)

Цель работы: ознакомиться с полиграммным шифром подстановки.

Тема 6. Шифр Playfair (2 ч.)

Цель работы: составить программу, кодирующую и декодирующую текст шифром Плейфера.

Тема 7. Шифр табличной маршрутной перестановки. (2 ч.)

Цель работы: ознакомиться с шифрами простой перестановки. Получить практические навыки шифрования данных с помощью шифра табличной маршрутной перестановки.

Тема 8. Шифр перестановки (2 ч.)

Цель работы: изучение принципов построения шифров перестановки. Исследование свойств перестановочных шифров.

Тема 9. Шифр перестановки (2 ч.)

Цель работы: научиться раасшифровывать фразу, зашифрованную методом двойной перестановкой.

Тема 10. Шифрование методом гаммирования. (2 ч.)

Цель работы: освоить на практике применение шифрования методом гаммирования.

Тема 11. Генерация псевдослучайных чисел. (2 ч.)

Цель работы: изучить методы генерации псевдослучайных чисел. Линейный конгруэнтный генератор.

Тема 12. Методы построения блочных шифров. Сеть Фейстеля. (2 ч.)

Цель работы: ознакомиться с блочными составными шифрами, освоить криптографические преобразования подстановки и перестановки.

Тема 13. Методы построения блочных шифров. Сеть Фейстеля. (2 ч.)

Цель работы: изучить и реализовать шифрование информации при помощи сети Фейстеля.

Тема 14. Алгоритм блочного шифрования (2 ч.)

Цель работы: изучить и реализовать режимы работы блочных шифров и схемы кратного шифрования для симметричных алгоритмов шифрования.

Тема 15. Алгоритм блочного шифрования (2 ч.)

Цель работы: Изучить режимы использования блочных шифров. Изучить способы объединения блочных шифров (многократное шифрование, сеть
Фейстела).

Тема 16. Метод линейного криптоанализа (2 ч.)

Цель работы: знакомство с классическим криптографическим алгоритмом - алгоритмом линейного шифрования данных (шифрования гаммированием).

Тема 17. Метод линейного криптоанализа (2 ч.)

Цель работы: закрепление теоретических знаний и практическое освоение метода линейного криптоанализа блочных симметричных криптосистем на примере криптосистемы S-DES.

Восьмой семестр. (34 ч.)

Тема 18. Средство криптографической защиты информации КриптоПро CSP (2 ч.)

Цель работы: ознакомиться с основными функциями СКЗИ КриптоПро CSP.

Тема 19. Средство криптографической защиты информации КриптоПро CSP (2 ч.)

Цель работы: изучить сновные характеристики СКЗИ КриптоПро CSP. Структура и состав СКЗИ КриптоПро CSP.

Тема 20. Установка СКЗИ КриптоПро CSP (2 ч.)

Цель работы: выполнить установка и настройку СКЗИ КриптоПро CSP

Тема 21. Работа с контейнерами и сертификатами СКЗИ КриптоПро CSP (2 ч.)

Цель работы: осуществить копирование и удаление закрытого ключа, находящегося в существующем контейнере. Тестирование (проверка работоспособности) и отображение свойств ключа (ключей) и сертификата (сертификатов) в существующем контейнере.

Тема 22. Работа с контейнерами и сертификатами СКЗИ КриптоПро CSP (2 ч.)

Цель работы: просмотр и установка сертификата, находящегося в существующем контейнере закрытого ключа на носителе. Осуществление связки между существующим сертификатом из файла и существующим контейнером закрытого ключа на носителе.

Тема 23. Работа с контейнерами и сертификатами СКЗИ КриптоПро CSP (2 ч.)

Цель работы: изменение и удаление сохраненных паролей (PIN-кодов) доступа к носителям закрытых ключей. Очистка информации о ранее использованных съёмных носителях, на которых располагались контейнеры закрытых ключей.

Тема 24. Настройка СКЗИ КриптоПро CSP (2 ч.)

Цель работы: выполнить настройку СКЗИ КриптоПро CSP в соответствии с документацией.

Тема 25. Генерация ключей и получение сертификата при помощи УЦ (2 ч.)

Цель работы: изучить принципы управления ключами на основе электронных сертификатов и архитектуру инфраструктуры открытых ключей.

Тема 26. Генерация ключей и получение сертификата при помощи УЦ (2 ч.)

Цель работы: изучить процесс получения цифрового сертификата.

Тема 27. Схемы разделения секрета (2 ч.)

Цель работы: ознакомиться с различными схемами разделения секретных ключей, которые используются в криптографических системах.

Тема 28. Схемы разделения секретного ключа (2 ч.)

Цель работы: ознакомиться со схемой разделения секрета Шамира.

Тема 29. Схемы разделения секретного ключа (2 ч.)

Цель работы: ознакомиться с векторной схемой разделения секрета.

Тема 30. Удостоверяющий центр КриптоПро УЦ (2 ч.)

Цель работы: выполнить установку Удостоверяющего Центра "КриптоПро УЦ".

Тема 31. Удостоверяющий центр КриптоПро УЦ (2 ч.)

Цель работы: настроить Удостоверяющий центр КриптоПро УЦ в соответствии с документацией.

Тема 32. Электронная цифровая подпись (2 ч.)

Цель работы: ознакомиться с основными схемами цифровой подписи и получить навыки создания и проверки подлинности ЦП.

Тема 33. Электронная цифровая подпись (2 ч.)

Цель работы: программно реализовать алгоритм формирования электронной цифровой подписи и проверки ее подлинности.

Тема 34. Электронная цифровая подпись (2 ч.)

Цель работы: выполнить вычисление и проверку электронной подписи сообщения по алгоритму Эль-Гамаля.

6. Виды самостоятельной работы студентов по дисциплине

Седьмой семестр (60 ч.)

Вид СРС: Ознакомление с нормативными документами (30 ч.)

Тематика заданий СРС:

Стандарты криптографической защиты:

1. ГОСТ 28147-89. Системы обработки информации. Защита крипто-графическая. Алгоритм криптографического преобразования.

2. ГОСТ Р 34.10-2012. Информационная технология. Криптографиче-ская защита информации. Процессы формирования и проверки электроннойцифровой подписи.
3. ГОСТ Р 34.11-2012. Информационная технология. Криптографиче-ская защита информации. Функция хэширования
4. ГОСТ Р 34.12-2015. Информационная технология. Криптографиче-ская защита информации. Блочные шифры.
5. ГОСТ Р 34.13-2015. Информационная технология. Криптографиче-ская защита информации. Режимы работы блочных шифров.
6. ГОСТ 34.10-2018 Информационная технология (ИТ). Криптографи-ческая защита информации. Процессы формирования и проверки электрон-ной цифровой подписи.
7. ГОСТ 34.11-2018 Информационная технология (ИТ). Криптографи-ческая защита информации. Функция хэширования.
8. ГОСТ 34.12-2018 Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры.
9. ГОСТ 34.13-2018. Информационная технология (ИТ). Криптографи-ческая защита информации. Режимы работы блочных шифров

Вид СРС: Подготовка рефератов (30 ч.)

Тематика заданий СРС:

Тематика рефератов:
1. История развития криптографии.
2. Шифры гаммирования.
3. Криптосистема RSA.
4. Функции хэширования.
5. Электронные цифровые подписи.
6. Нормативно-правовые основы криптографическойзащиты информации.
7. Программные СКЗИ. Особенности и примеры.
8. Аппаратные и программно-аппартные СКЗИ.Особенности и примеры.
9. СКЗИ от несанкционированного доступа.
10. СКЗИ для передачи данных в локальных сетях.
11. Криптографическая защита удаленного доступа клокальной сети.
12. Персональные криптографические средства аутентификации.
13. Средства шифрования, встроенные в операционнуюсистему Windows.

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы.
Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора.
Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и целей.
Требования к языку реферата. Должен отличаться точностью, краткостью, ясностью и простотой.
Структура реферата.
1. Титульный лист.
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо

неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных.
При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.

Восьмой семестр (24 ч.)

Вид СРС: Ознакомление с нормативными документами (24 ч.)

Тематика заданий СРС:

Нормативные документы:
1. Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи»
2. Федеральный закон Российской Федерации от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»
3. Указ Президента Российской Федерации от 03.04.1995 № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»
4. Постановление Правительства РФ от 16.04.2012 N 313 "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)"
5. Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005)
6.. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Фонд оценочных средств. Оценочные материалы

8.1. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий

Базовый уровень:

обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий

Пороговый уровень:

обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне

Уровень ниже порогового:

система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Экзамен, зачет с оценкой	
Повышенный	5 (отлично)	91 и более
Базовый	4 (хорошо)	71 – 90
Пороговый	3 (удовлетворительно)	60 – 70
Ниже порогового	2 (неудовлетворительно)	Ниже 60

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Отлично	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины, а также по основным вопросам, выходящим за ее пределы; точное использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач; выраженную способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации; полное и глубокое усвоение основной, и дополнительной литературы, по изучаемой учебной дисциплине; умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин; творческую самостоятельную работу на учебных занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Хорошо	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины; использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения; владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач; способность решать сложные проблемы в рамках учебной дисциплины; свободное владение типовыми решениями; усвоение основной и дополнительной литературы, рекомендованной рабочей программой по учебной дисциплине; умение ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку; активную самостоятельную работу на учебных занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.
Удов-летвори-тельно	Обучающийся демонстрирует: достаточные знания в объеме рабочей программы по учебной дисциплине; использование научной терминологии, грамотное, логически правильно изложение ответа на вопросы, умение делать выводы без существенных ошибок; владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач; способность самостоятельно применять типовые решения в рамках изучаемой дисциплины; усвоение основной литературы, рекомендованной рабочей программой по дисциплине; умение ориентироваться в базовых теориях, концепциях и направлениях по дисциплине; работу на учебных занятиях под руководством преподавателя, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.
Неудов-летвори-тельно	Обучающийся демонстрирует: фрагментарные знания в рамках изучаемой дисциплины; знания отдельных литературных источников, рекомендованных рабочей программой по учебной дисциплине; неумение использовать научную терминологию учебной дисциплины, наличие в ответе грубых, логических ошибок; пассивность на занятиях или отказ от ответа, низкий уровень культуры исполнения заданий.

8.2. Вопросы, задания текущего контроля

В целях освоения компетенций, указанных в рабочей программе дисциплины, предусмотрены следующие вопросы, задания текущего контроля:

- ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Студент должен знать:

основные принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

Вопросы, задания:

1. Типовые схемы построения СКЗИ.
2. Требования к средствам криптографической защиты информации.

3. Как реализовано шифрование: аппаратное и программное?

Студент должен уметь:

использовать средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

Задания:

1. Установить и настроить СКЗИ.
2. Методы, средства анализа и контроля защищенности СКЗИ.
3. Правила введения в эксплуатацию СКЗИ.

Студент должен владеть навыками:

навыками и методиками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

Задания:

1. Просмотреть сертификаты в контейнере.
2. Выбрать СКЗИ с учётом заданных требований.
3. Создать электронную подпись.

8.3. Вопросы промежуточной аттестации

Седьмой семестр (Зачет с оценкой)

1. История криптографии
2. Основные понятия криптографии
3. Шифры перестановки
4. Шифры замены
5. Криптоанализ шифров перестановки
6. Вопросы криптоанализа простейших шифров замены

Восьмой семестр (Экзамен)

1. Понятие односторонней функции и односторонней функции с "лазейкой"
2. Криптосистема на базе эллиптических кривых
3. Системы шифрования с открытыми ключами
4. Криптосистемы RSA и Эль-Гамаля
5. Криптографические хэш-функции
6. Электронная цифровая подпись

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

Промежуточная аттестация обучающихся ведется непрерывно и включает в себя:

для дисциплин, завершающихся (согласно учебному плану) зачетом/зачетом с оценкой (дифференцированным зачетом), – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и оценивание окончательных результатов обучения по дисциплине;

для дисциплин, завершающихся (согласно учебному плану) экзаменом, – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и семестровую аттестацию (экзамен) – оценивание окончательных результатов обучения по дисциплине.

По дисциплинам, завершающимся зачетом/зачетом с оценкой, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 100 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля.

По дисциплинам, завершающимся экзаменом, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 60 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля и количества баллов, набранных на семестровой аттестации (экзамене).

Система оценивания.

В соответствии с Положением о балльно-рейтинговой системе оценки успеваемости обучающихся Волгоградского государственного университета предусмотрена возможность предоставления студентам выполнения дополнительных заданий повышенной сложности (не включаемых в перечень обязательных и, соответственно, в перечень обязательного текущего контроля успеваемости) и получения за выполнение таких заданий «премиальных» баллов, - для поощрения обучающихся, демонстрирующих выдающие способности.

Оценка качества освоения образовательной программы включает текущий контроль успеваемости, промежуточную аттестацию обучающихся и государственную итоговую аттестацию выпускников.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля можно отнести:

Форма текущего контроля: Контрольная работа

контрольные работы применяются для оценки знаний, умений, навыков по дисциплине или ее части. Контрольная работа, как правило, состоит из небольшого количества средних по трудности вопросов, задач или заданий, требующих поиска обоснованного ответа. Может занимать часть или полное учебное занятие с разбором правильных решений на следующем занятии.

Форма текущего контроля: Устный опрос, собеседование

устный опрос, собеседование являются формой оценки знаний и предполагают специальную беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной. Процедуры направлены на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.

Форма текущего контроля: Письменные задания или лабораторные работы

письменные задания являются формой оценки знаний и предполагают подготовка письменного ответа, решение специализированной задачи, выполнение теста. являются формами контроля и средствами применения и реализации полученных обучающимися знаний, умений и навыков в ходе выполнения учебно-практической задачи, связанной с получением значимого результата с помощью реальных средств деятельности. Рекомендуются для проведения в рамках тем (разделов), наиболее значимых в формировании компетенций. Тест является простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест состоит из небольшого количества элементарных задач; может предоставлять возможность выбора из перечня ответов; занимает часть учебного занятия (10–30 минут); правильные решения разбираются на том же или следующем занятии; частота тестирования определяется преподавателем.

Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов) /модуля (модулей). Промежуточная аттестация помогает оценить более крупные совокупности знаний, умений и навыков, в некоторых случаях – даже формирование определенных компетенций.

К формам промежуточного контроля можно отнести:

Форма промежуточной аттестации: Зачет с оценкой

зачет с оценкой служит формой проверки усвоения учебного материала по дисциплине (модулю), практики, готовности к практической деятельности.

Форма промежуточной аттестации: Экзамен

экзамен по дисциплине или ее части имеет цель оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач. Форма проведения, как правило, предусматривает ответы на вопросы экзаменационного билета, выполнение которых направленно на проверку сформированности компетенций по соответствующей учебной дисциплине.

Методика формирования результирующей оценки:

Седьмой семестр

1. Контрольная работа - от 0 до 35 баллов
2. Устный опрос, собеседование - от 0 до 30 баллов
3. Письменные задания или лабораторные работы - от 0 до 35 баллов
4. Зачет с оценкой - Аттестация по дисциплине в форме зачета (зачета с оценкой) проводится по сумме результатов модульных контрольных работ и текущей успеваемости обучающегося.

Восьмой семестр

1. Контрольная работа - от 0 до 35 баллов
2. Устный опрос, собеседование - от 0 до 30 баллов
3. Письменные задания или лабораторные работы - от 0 до 35 баллов
4. Экзамен - от 0 до 40 баллов

9. Перечень основной и дополнительной учебной литературы

9.1 Основная литература

1. Бабаш Александр Владимирович Криптографические методы защиты информации [Электронный ресурс]: учебное - Издание 2 - РИОР, 2014. - 216 с. - Режим доступа: http://new.znanium.com/go.php?id=432654

2. Лапонина, О. Р. Криптографические основы безопасности [Электронный ресурс]: учебное - Интуит НОУ, 2016. - 243 с. - Режим доступа: http://www.book.ru/book/917744

9.2 Дополнительная литература

1. Баранова, Е. К. Криптографические методы защиты информации. Лабораторный практикум +CD [Электронный ресурс]: учебное - КноРус, 2017. - Режим доступа: http://www.book.ru/book/920017

В качестве учебно-методического обеспечения могут быть использованы другие учебные, учебно-методические и научные источники по профилю дисциплины, содержащиеся в электронно-библиотечных системах, указанных в п. 11.2 «Электронно-библиотечные системы».

9.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://www.edu.ru. - Федеральный портал «Российское образование»
2. http://fstec.ru - Официальный сайт Федеральной службы по техническому и экспортному контролю
3. http://www.garant.ru/ - Гарант

10.Методические указания по освоению дисциплины для лиц с ОВЗ и инвалидов

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального учебного плана (при необходимости), изучение данной дисциплины базируется на следующих возможностях:
- индивидуальные консультации преподавателя;
- максимально полная презентация содержания дисциплины в ЭИОС (в частности, полнотекстовые лекции, презентации, аудиоматериалы, тексты для перевода и анализа и т.п.).

11. Перечень информационных технологий

В учебном процессе активно используются информационные технологии с применением современных средств телекоммуникации; электронные учебники и обучающие компьютерные программы. Каждый обучающийся обеспечен неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) университета. ЭИОС предоставляет открытый доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к электронным библиотечным системам и электронным образовательным ресурсам.

11.1 Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

Программное обеспечение:
1. Microsoft Windows 7 Professional, 11 лицензий, номер 60357707
2. Microsoft Windows 7 Home Premium, 1 лицензия, OEM-лицензия
3. Microsoft Windows 8.1 Home, 1 лицензия OEM-лицензия
4. Microsoft Office 2007 Standart, 1 лицензия, номер 43847745
5. Microsoft Office 2016, 1 лицензия, Сублицензионный договор No 31604241628 от 21.11.16
6. LibreOffice 12 лицензий (свободно-распространяемое программное обеспечение)
7. FreeBSD, 1 лицензия FreeBSD license свободное программное обеспечение
8. Oracle VM VirtualBox, 14 лицензий GNU GPL свободное программное обеспечение
9. Mozila FireFox, 13 лицензий Mozilla Public License 2.0 (MPL) свободное программное обеспечение
10. Visual Studio Community 2017, 13 лицензий, учебное программное обеспечение
11. Python 2.7, 13 лицензий PSFL (свободно-распространяемое программное обеспечение)

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, лабораторного типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего
контроля и промежуточной аттестации.
Программное обеспечение:
1. Windows 10 Профессиональная, 13 лицензий, номер 65946188.
2. Microsoft Windows 8.1 Home, 1 лицензия OEM-лицензия
3. Microsoft Office 2016, 14 лицензий, сублицензионный договор No31604241628 от 21.11.2016.
4. Oracle VM VirtualBox 15 лицензий GNU GPL свободное программное обеспечение
5. Microsoft Windows 7 Home Premium, 1 лицензия, OEM-лицензия
6. Microsoft Office 2007 Standart, 1 лицензия, номер 43847745

11.2 Современные профессиональные базы данных и информационно-справочные системы, в т.ч. электронно-библиотечные системы
(обновление выполняется еженедельно)

Название	Краткое описание	URL-ссылка

Научная электронная библиотека	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.	http://elibrary.ru/
ЭБС "Лань"	Электронно-библиотечная система	https://e.lanbook.com/
ЭБС Znanium.com	Электронно-библиотечная система	https://znanium.com/
ЭБС BOOK.ru	Электронно-библиотечная система	https://www.book.ru/
ЭБС Юрайт	Электронно-библиотечная система	https://www.biblio-online.ru/
Scopus	Scopus – крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. В базе содержится 23700 изданий от 5000 международных издателей, в области естественных, общественных и гуманитарных наук, техники, медицины и искусства.	http://www.scopus.com/
Web of Science	Наукометрическая реферативная база данных журналов и конференций. С платформой Web of Science вы можете получить доступ к непревзойденному объему исследовательской литературы мирового класса, связанной с тщательно отобранным списком журналов, и открыть для себя новую информацию при помощи скрупулезно записанных метаданных и ссылок.	https://apps.webofknowledge.com/
КонсультантПлюс	Информационно-справочная система	http://www.consultant.ru/
Гарант	Информационно-справочная система по законодательству Российской Федерации	http://www.garant.ru/
Научная библиотека ВолГУ им О.В. Иншакова		http://library.volsu.ru/

12. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения занятий лекционного и семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
Специализированная мебель:
1. парта со скамьей- 60 шт.
2. учебные места - 120 шт.
3. рабочее место преподавателя (стол и стул) – 1 шт.
4. доска аудиторная-1 шт.
Демонстрационное оборудование:
1. Доска (меловая)
2. Мультимедийное оборудование

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, лабораторного типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
Специализированная мебель:
1. Столы – 8 шт.
2. стулья – 16 шт.
3. парта со скамьей – 8 шт.

4. рабочее место преподавателя (стол и стул) – 1 шт.
Демонстрационное оборудование:
1. Проектор BenQ MX 505
2. Экран проекционный
3. Доска (магнитная, маркерная)
Рабочие места на базе вычислительной техники (18 шт):
1.Моноблок VPS 5000 (16 шт.);
2. Ноутбук Acer AS5738G;
3. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
Сетевое оборудование:
1. Wi-Fi роутер ASUS RT-N10
2. Концентратор.
3. Комплекс "Сетевое оборудование "Cisco" часть 1

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, лабораторного типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.)
Специализированная мебель:
1. компьютерные столы – 13 шт.
2. стулья – 29 шт.
3. парта – 8 шт.
4. рабочее место преподавателя (стол и стул) – 1 шт.
Средства вычислительной техники (15 шт):
1. Компьютерный комплекс Option в составе: Системный блок клавиатура, мышь, монитор (13 шт);
2. Ноутбук Acer AS5738G;
3. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
Сетевое оборудование:
1. Маршрутизатор ASUS WL-520GU.
2. Концентратор.
Демонстрационное оборудование:
1. Доска (магнитная, маркерная)
2. Проектор projector DLP ColorBoost II
3. Экран для проектора Digis

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС ВолГУ.