ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЕГИОНАЛЬНЫЙ ИНСТИТУТ БИЗНЕСА И УПРАВЛЕНИЯ»

Рассмотрено и одобрено на заседании Учебно-Методического совета
Протокол № 1 от 23 августа 2024 г.

УТВЕРДЖЕНО
Проректор по учебной работе
_____ Ю.И. Паничкин
Личная подпись инициалы, фамилия
«23» августа 2024 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ к рабочей программе

дисциплины «Криптография»

Направление подготовки	**09.03.03 Прикладная информатика**
Направленность подготовки (профиль)	**Прикладная информатика**
Уровень программы	**бакалавриат**
Форма обучения	**очно-заочная**

Рязань 2024 г.

Фонд оценочных средств текущей и промежуточной аттестации по дисциплине «Криптография»

Фонд оценочных средств является неотъемлемой частью рабочей программы дисциплины и основной образовательной программы.

Фонд оценочных средств представляет собой комплекс учебных заданий, предназначенных для измерения уровня достижений обучающимся установленных результатов обучения, и используется при проведении текущей и промежуточной аттестации (в период зачетно-экзаменационной сессии).

Цель ФОС – установление соответствия уровня подготовки обучающихся на данном этапе обучения требованиям рабочей программы дисциплины.

Основными задачами ФОС по учебной дисциплине являются:

- контроль достижений целей реализации ОП – формирование компетенций;
- контроль процесса приобретения обучающимся необходимых знаний, умений, навыков(владения/опыта деятельности) и уровня сформированности компетенций;
- оценка достижений обучающегося;
- обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование методов обучения в образовательном процессе.

1. Планируемые результаты обучения по дисциплине в рамках планируемых результатов освоения основной образовательной программы. Перечень компетенций в процессе освоения образовательной программы.

Дисциплина «Криптография» обеспечивает освоение следующих компетенций с учетом этапа освоения:

2. -1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

3. Соответствие уровня освоения компетенции планируемым результатам обучения и критериям их оценивания

Код компетенции	Наименование компетенции
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

Показатель оценивания	**Критерии оценивания**				
	1	2	3	4	5
Знает особенности системного и критического мышления и готовность к нему	Студент продемонстрировал отсутствие знаний.	Студент демонстрирует небольшое понимание заданий. У студента нет ответа.	Студент демонстрирует частичное понимание заданий. Большинство требований, предъявляемых к заданию выполнены.	Студент демонстрирует значительное знание заданий. Все требования, предъявляемые к заданию выполнены.	Студент демонстрирует полное знание заданий. Все требования, предъявляемые к заданию выполнены.

Умеет анализировать источник информации с точки зрения временных и пространственных условий его возникновения. Анализирует ранее сложившиеся в науке оценки информации.	Студент продемонстрировал отсутствие умений.	Студент демонстрирует неумения выполнять задания.	Студент демонстрирует частичное умение выполнений заданий. Большинство требований, предъявляемых к заданию выполнены.	Студент демонстрирует значительное знание заданий. Все требования, предъявляемые к заданию выполнены.	Студент демонстрирует полное умение выполнений заданий. Все требования, предъявляемые к заданию выполнены.
Владеет и формирует собственное суждение и оценку информации, принимает обоснованное решение. Определяет практические последствия предложенного решения задачи.	Проявляет ся полное или практически полное отсутствие навыков.	У студента не сформирован ы дисциплинарные компетенции, проявляется недостаточность навыков.	В целом успешное, но не систематическое применение навыков	В целом успешное, но содержащее отдельные пробелы применение навыков	Успешное и систематическое применение навыков

4. Фонд оценочных средств и материалы текущего контроля успеваемости обучающихся и промежуточной аттестации по дисциплине

4.1. В ходе реализации дисциплины «Криптография» используются следующие формы текущего контроля успеваемости обучающихся:
опрос, реферат, контрольная работа.
4.2. Преподаватель при текущем контроле успеваемости, оценивает уровень подготовленности обучающихся к занятию по следующим показателям:

- устные (письменные)ответы на вопросы преподавателя по теме занятия;
- по сформированности собственных суждений основанных на значимых фактах и практических результатах отраженных в реферате, эссе;
- аргументированности, актуальности, новизне содержания доклада;
- по точному выполнению целей и задач контрольной работы.

Детализация баллов и критерии оценки текущего контроля успеваемости утверждается на заседании кафедры.

3.2.1. Вопросы для подготовки к опросу по всем изучаемым тема дисциплины:

1. Важные моменты в истории развития теории защиты информации. «Наивная» криптография: шифр Цезаря, шифр Пиблса; Формальная криптография: шифр Вижинера, роторные криптосистемы; математическая криптография: доказуемо криптостойкие системы; компьютерная криптография: криптосистемы с открытым ключом, автоматизированный криптоанализ.
2. Модель передачи сообщения в криптосистеме с открытым ключом. Основы теории чисел: функция Эйлера, обобщенный алгоритм Евклида, быстрый алгоритм возведения в степень справа налево и слева направо. Понятие односторонней функции. Примеры односторонних функций. Система защищенной передачи ключей Диффии Хеллмана. Шифр Шамира. Шифр

Эль-Гамаля. Шифр RSA. Электронная подпись на базе RSA

3. Понятие риптографического протокола. Протокол «Ментальный покер». Протокол «Доказательство с нулевым знанием»: задача о раскраске, задача о гамильтоновом цикле. Электронные деньги. Задача о взаимной верификации.

4. Первый шифр с секретным ключом: шифр Цезаря. Понятие блокового шифра. Шифр ГОСТ 28147- 89. Шифр RC-5. Шифр RC-6. Шифр AES (Rijndael). Режимы функционирования блоковых шифров: режим электронной кодовой книги (ECB),режим цепных блоков (CBC). Понятие идеального шифра. Первый идеальный шифр – шифр Вернама. Потоковые шифры. Генераторы псеводослучайных чисел. Режим OFB блокового шифра. Режим CTR блокового шифра. Шифр RC-4. Криптографические хеш-функции. Понятие хеш-функции. Требования к криптографическим хеш-функциям. Примеры криптографических хеш-функций

5. Краткая информация об эллиптических кривых. Математические основы теории эллиптических кривых. Общий вид уравнения эллиптической кривой. Свойства эллиптических кривых. Арифметические операции на эллиптических кривых. Оценки количества точек на эллиптической кривой. Построение криптосистем на основе арифметики на эллиптических кривых.

6. Физические генераторы случайных чисел. Генераторы псевдослучайных чисел: конгруэнтные генераторы, сдвиговые регистры, сдвиговый регистр с линейной обратной связью, сдвиговые регистры с нелинейной обратной связью.

7. Цели и задачи криптоанализа. Криптографическая устойчивость информационных систем. Линейный криптоанализ. Дифференциальный криптоанализ. Градиентная статистическая атака.

8. История стеганографии. Задачи стеганографии. Модель передачи скрытых сообщений. Первые стеганографические системы. Современная стеганография. Защита авторского права. Цифровые водяные знаки. Цифровые отпечатки пальцев. Обнаружение факта передачи скрытого сообщения. Понятие идеальной стеганографической системы.

9. Основные определения теории сжимающего кодирования. Сжимающие коды: Код Фано, Код Хаффмана, Код Шенона, Адаптивный код Хаффмана, Арифметический код, Стопка книг, Код LZ77, Код LZ78.

10. Задачи теории кодирования. Примеры ошибок при передаче сообщений. Модель передачи данных в зашумленном канале. Типы ошибок в канале связи. Основные определения теории кодирования. Основные понятия теории групп. Группа автоморфизмов. Расстояние Хэмминга. Вес Хэмминга.Линейные коды. Проверочная и порождающая матрицы. Связь проверочной и порождающей матрицы. Границы объемов кодов: граница Хэмминга, граница Синглтона. Циклические коды. Теорема о столбцах проверочной матрицы. Код Хэмминга и его свойства. Примеры кода Хэмминга. Декодирование кода Хэмминга. Теорема Шеннона

Устный(письменный) опрос проводится в течение установленного времени преподавателем. Опрашиваются все обучающиеся группы. За опрос выставляется оценка до 10 баллов. Набранные баллы являются рейтинг-баллами.

Рейтинг-баллы	**Аттестационная оценка обучающегося по дисциплине учебного плана в национальной системе оценивания**
8-10	отлично
6-7	хорошо

4-5	удовлетворительно
0-3	неудовлетворительно

При оценивании учитывается:
1. Целостность, правильность и полнота ответов
2. В ответе приводятся примеры из практики, даты, Ф.И.О. авторов
3. Применяются профессиональные термины и определения

Процедура оценки опроса:
1. Если ответ удовлетворяет 3-м условиям – 8-10 баллов.
2. Если ответ удовлетворяет 2-м условиям – 6-7 баллов.
3. Если ответ удовлетворяет 1-муусловию – 4-5 баллов.
4. Если ответ не удовлетворяет ни одному условию – 0-3

3.2.2. Темы рефератов:

Реферат – форма научно-исследовательской деятельности, направленная на развитие научного мышления, на формирование познавательной деятельности по дисциплине через комплекс взаимосвязанных методов исследования, на самообразование и творческую деятельность. Используя ЭИОС ММА, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, базы данных, ЭБС, выделять значимые и актуальные положения, противоположные мнения с обоснованием собственной точки зрения.

Общий список тем рефератов
1. История и основные направления развития современной защитой информации
2. Криптография с открытым ключом
3. Криптографические протоколы
4. Шифры с секретным ключом
5. Криптосистемы на эллиптических кривых
6. Случайные числа в криптографии
7. Основы криптоанализа
8. Стеганография
9. Сжимающее кодирование
10. Теория кодирования

Критерии оценки:
1. Выполнение задания в срок. Сформулированы предмет анализа или исходные тезисы.
2. Отражены суждения и оценки, основанные на значимых фактах и практических результатах.
3. Использованы электронные информационные ресурсы, базы данных, ЭБС

Процедура оценки реферата, эссе:
1. Если ответ удовлетворяет 3-м условиям – 18-20 баллов.
2. Если ответ удовлетворяет 2-м условиям – 15-17 баллов.
3. Если ответ удовлетворяет 1-му условию – 10-14 баллов.
4. Если ответ не удовлетворяет ни одному условию – 1-9

Рейтинг- баллы	**Аттестационная оценка обучающегося по дисциплине учебного плана в национальной системе оценивания**
18-20	Отлично

15-17	Хорошо
10-14	Удовлетворительно
1-9	Неудовлетворительно

5. 2.4. Тематика контрольных работ

Контрольная работа предполагает выработку умений обучающимся показать глубокое знание теории предмета; на основе материала, установить и проанализировать следственно-логические связи и продемонстрировать навыки практического применения теоретической информации изучаемой дисциплины. Написание контрольной работы требует формулирование цели и задачи всей работы, заключение или выводы следуют из поставленных целей и задач.

Примерная тематика контрольных работ:

1. Важные моменты в истории развития теории защиты информации
2. Модель передачи сообщения в криптосистеме с открытым ключом
3. Понятие криптографического протокола
4. Первый шифр с секретным ключом: шифр Цезаря. Понятие блокового шифра.
5. Краткая информация об эллиптических кривых. Математические основы теории эллиптических кривых
6. Физические генераторы случайных чисел.
7. Цели и задачи криптоанализа
8. История стеганографии. Задачи стеганографии
9. Основные определения теории сжимающего кодирования
10. Задачи теории кодирования. Примеры ошибок при передаче сообщений.

За контрольную работу выставляется оценка до 20 баллов. Набранные баллы являются рейтинг-баллами.

Критерии оценки контрольной работы:

1. Выполнение задания в срок. Соответствие содержания заявленной теме;
2. Самостоятельность в выполнении работы, точность и полнота изложенного материала.
3. Логическое изложение материала. Соблюдение требований к оформлению работы.

Процедура оценки контрольной работы:

1. Если ответ удовлетворяет 3-м условиям – 18-20 баллов.
2. Если ответ удовлетворяет 2-м условиям – 15-17 баллов.
3. Если ответ удовлетворяет 1-му условию – 10-14 баллов.
4. Если ответ не удовлетворяет ни одному условию – 1-9

Рейтинг-баллы	**Аттестационная оценка студента по дисциплине учебного плана в национальной системе оценивания**
18-20	Отлично
15-17	Хорошо
10-14	Удовлетворительно
1-9	Неудовлетворительно

4. Форма и средства (методы) проведения промежуточной аттестации

4.1. Промежуточный контроль: экзамен(рейтинговая система)

Экзамен с оценкой проводится в устной форме. Время, отведенное на подготовку вопросов Экзамена, составляет 15 мин. По рейтинговой системе оценки, формы контроля оцениваются отдельно. Экзамен составляет от 0 до 20 баллов. Допуск к экзамену составляет 45 баллов.

Типовые оценочные средства.

Примерный перечень вопросов к экзамену

1. Основные этапы развития теории защиты информации.
2. Наивная криптография. Шифр Цезаря.
3. Идеальная криптосистема. Шифр Вернама.
4. Система обмена ключами Диффи и Хеллмана.
5. Шифр Шамира.
6. Шифр Эль-Гамаля.
7. Шифр RSA.
8. Электронная цифровая подпись. Схема протокола. Пример построения
9. на основе шифра RSA.
10. Криптосистемы на эллиптических кривых. Основы арифметики на
11. эллиптических кривых. Принцип построения криптосистем на
12. эллиптических кривых.
13. Генераторы псевдо случайных чисел
14. Потоковые шифры. Примеры потоковых шифров.
15. Шифр RC4.
16. Блоковые шифры. Примеры блоковых шифров. Режимы функционирования блоковых шифров.
17. Схема построения потокового шифра на основе блокового шифра.
18. Теорема Шеннона.
19. Расстояние Хемминга. Вес Хэмминга. Код Хэмминнга.
20. Линейные коды. Проверочная матрица. Порождающая матрица.
21. Теорема и связи проверочной и порождающей матриц.
22. Циклические коды.
23. Границы объемов кодов. Граница Хэмминга. Граница Синглтона.

Градация перевода рейтинговых баллов обучающихся в пятибалльную систему аттестационных оценок и систему аттестационных оценок ECTS.

Академический рейтинг обучающегося	**Аттестационная оценка обучающегося по дисциплине учебного плана в национальной системе оценивания**	**Аттестационная оценка обучающегося по дисциплине учебного плана в системе ECTS**
95-100	Отлично	+ A (excellent)
80-94		A (excellent)
75-79	Хорошо	+B (good)
70-74		B (good)
55-69	Удовлетворительно	C (satisfactory)

50-54		D (satisfactory)
45-49	Неудовлетворительно	E (satisfactory failed)
1-44		F (not rated)
0		N/A (not rated)

5. Практическая работа(практическая подготовка): проверка выполнения заданий по практической подготовке в профессиональной деятельности и самостоятельной работы на практических занятиях.

Практическое задание – это частично регламентированное задание по практической подготовке в профессиональной деятельности, имеющее алгоритмическое или нестандартное решение, позволяющее диагностировать умения, интегрировать знания различных научных областей в практическую подготовку связанную с профессиональной деятельности. Может выполняться в индивидуальном порядке или группой обучающихся.

Работа во время проведения практического занятия состоит из следующих элементов:

- консультирование обучающихся преподавателем с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем практических заданий и задач;
- самостоятельное выполнение практических заданий согласно обозначенной учебной программой тематики;
- ознакомление с инструктивными материалами с целью осознания задач практического занятия, техники безопасности при работе в аудитории.

Обработка, обобщение полученных результатов практической подготовки проводиться обучающимися самостоятельно или под руководством преподавателя (в зависимости от степени сложности поставленных задач).

6 . Примерные темы к курсовым работам(проектам)

Курсовая работа/проект– предусмотрена/не предусмотрена

7 .Оценка компетенций (в целом)

Оценка компетенций (в целом) осуществляется по итогам суммирования текущих результатов обучающегося и промежуточной аттестации.

В оценке освоения компетенций (в целом)учитывают: полноту знания учебного материала по теме, степень активности обучающегося на занятиях в семестре; логичность изложения

материала; аргументированность ответа; уровень самостоятельного мышления, практической подготовки; умение связывать теоретические положения с практикой, в том числе и с будущей профессиональной деятельностью с промежуточной аттестации.