**Примерные оценочные материалы, применяемые при проведении**

**промежуточной аттестации по дисциплине (модулю)**

**«Основы информационной безопасности».**

При проведении промежуточной аттестации обучающемуся предлагается дать ответы на 3 вопроса из нижеприведенного списка..

**Ответ** студента оценивается одной из следующих оценок**: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».**

Оценка **«удовлетворительно»** - правильные и конкретные, без грубых ошибок ответы на основные вопросы. Наличие отдельных неточностей в ответах. В целом правильные ответы с небольшими неточностями на дополнительные вопросы. Некоторое использование в ответах на вопросы материалов рекомендованной литературы.

Оценка **«хорошо»** - твердые и достаточно полные знания программного материала, понимание сущности рассматриваемых процессов и явлений. Последовательные и правильные, но недостаточно развернутые ответы на основные вопросы. Правильные ответы на дополнительные вопросы. Ссылки в ответах на вопросы на отдельные материалы рекомендованной литературы.

Оценка **«отлично»** - глубокие исчерпывающие знания всего программного материала, понимание сущности и взаимосвязи рассматриваемых процессов и явлений. Логически последовательные, полные, правильные и конкретные ответы на все основные вопросы. Правильные и конкретные ответы дополнительные вопросы. Использование в необходимой мере в ответах на вопросы материалов всей рекомендованной литературы.

Оценка **«неудовлетворительно»** выставляется в случае, когда количество неправильных ответов превышает количество допустимых для положительной оценки.

Примерный перечень вопросов:

1. Информационная безопасность человека и общества.
2. Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений.
3. Расскажите про классификацию атак
4. Дайте описание журналу аудита. Для чего он нужен
5. Какие криптосистемы вы знаете
6. Что такое аутентификация и идентификация пользователей
7. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна
8. Основные каналы утечки информации. Защита от утечки информации по техническим каналам
9. Методы и средства защиты информации
10. Какие вирусы вы знаете, опишите их классификацию
11. Реализация методов и средств защиты информации.
12. Средства опознания и разграничения доступа к информации.
13. Какие устройства идентификации и аутентификации вы знаете?
14. Отличие защиты информации в локальных сетях от глобальных сетей?
15. Криптография. Симметричные криптосистемы.
16. Аутентификация пользователей как системы защиты информации.
17. Криптография. Асимметричные криптосистемы
18. Информационная безопасность человека и общества
19. Какие криптосистемы вы знаете?
20. Основные каналы утечки информации.
21. Чем отличается симметричная и ассиметричная криптосистема
22. Электронно-цифровая подпись
23. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей»
24. Основные алгоритмы шифрования данных: DES.
25. Аутентификация пользователей как защита информации
26. Криптосистемы и их классификация.
27. Что такое информация
28. Классы вирусов.
29. Несанкционированный доступ к системе и информации?
30. Опишите классификацию атак на систему
31. Опишите классификацию атак на систему
32. Опишите ассиметричную систему шифрования
33. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».
34. Основные алгоритмы шифрования данных: DES
35. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна
36. Что такое открытый ключ в криптографии?
37. Опишите ассиметричные системы криптографии
38. Опишите логическую бомбу и для чего она внедряется в вирусы?
39. Методы и средства защиты информации. Содержание способов и средств обеспечения безопасности информации.
40. Электронно-цифровая подпись.

**Выполнение и защита курсового проекта**

Студентам на 6-й неделе семестра обучения выдается задание по курсовому проекту.

Защита курсового проекта проводится в конце семестра. Защита демонстрирует понимание методов научного исследования, знание понятийного аппарата, умение правильно и четко формулировать свои мысли, отстаивать обоснованную позицию с применением научного стиля мышления.

Для защиты необходим оформленный отчет по курсовому проекту, презентация с результатами работы.

Защита проекта проводится в форме публичного доклада и является открытой. После защиты преподавателем выдается практическое задание, после которого озвучивается оценка за работу.

Примерный перечень практических заданий:

1. Криптограмма ЩНТШНЬ получена из открытого текста циклическим
2. сдвигом букв русского алфавита (А...ДЕЖ...ЩЬ...Я) на k знаков вправо. Найдите
3. ключ k, восстановите исходное сообщение.
	1. Методом Цезаря зашифруйте слово “Защита”. К=3.
4. Зашифруйте методом Цезаря слово “Компьютер” Ключ= 5
5. Зашифруйте текст “Системы криптографии” по шифру цезаря, где K=6
6. Зашифруйте текст “Средства защиты” по шифру цезаря, где K=2
7. Зашифруйте текст “Всемирная паутина” по шифру цезаря, где K=3
8. Зашифруйте текст “Системы Обработки данных” по шифру цезаря, где K=2
9. Зашифруйте текст “Ассиметричные криптосистемы” по шифру цезаря, где K=5
10. Зашифруйте текст “Информационные системы и технологии” по шифру цезаря, где K=2
11. Зашифруйте текст “Алгоритм криптосистемы” по шифру цезаря, где K=4
12. Зашифруйте текст “Новые технологии” по шифру цезаря, где K=5
13. С помощью ключа УСТРОЙСТВО зашифруйте словосочетание «информация, как средство познания мира»
14. Зашифруйте текст “Аутентификация и идентификация” по шифру цезаря, где K=4
15. Зашифруйте текст “Аутентификация и идентификация” по шифру цезаря, где K=4
16. Зашифруйте текст “Шифр и расшифровка” по шифру цезаря, где K=3
17. Зашифруйте текст “Криптографическая система “по шифру цезаря, где K=6
18. Зашифруйте текст “Журнал аудита” по шифру цезаря, где K=5
19. Зашифруйте текст “Биометрические устройства” по шифру цезаря, где K=4.
20. Зашифруйте текст “Аутентификация и идентификация” по шифру цезаря, где K=2
21. Зашифруйте текст “Технические данные” по шифру цезаря, где K=4.