Компонент ОПОП 11.05.01 Радиоэлектронные системы и комплексы
Направленность (профиль) Инфокоммуникационные технологии и радиотехнические системы
наименование ОПОП

Б1.О.38
шифр дисциплины

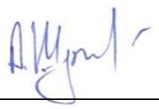
ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Дисциплины (модуля) **Основы защиты информационных систем**

Разработчик:
Шульженко А.Е.
ФИО
старший преподаватель
должность

Утверждено на заседании кафедры
радиотехники и связи
наименование кафедры
протокол №_7_ от _04.03.2025 года_

И.о. заведующего кафедрой РТиС



А.Е. Шульженко

1. Критерии и средства оценивания компетенций и индикаторов их достижения, формируемых дисциплиной (модулем)

Код и наименование компетенции	Код и наименование индикатора(ов) достижения компетенции	Результаты обучения по дисциплине (модулю)			Оценочные средства текущего контроля	Оценочные средства промежуточной аттестации
		Знать	***Уметь***	***Владеть***		
ОПК-7 Способен решать стандартные задачи профессиональной деятельности с применением современных методов исследования и информационно-коммуникационных технологий	ИД-1 $_{ОПК-7}$ знает современные принципы поиска, хранения, обработки, анализа и представления в требуемом формате информации ИД-2 $_{ОПК-7}$ решает задачи обработки данных с помощью современных средств автоматизации ИД-3 $_{ОПК-7}$ проводит анализ защищенности информационно-коммуникационных технологий используемых в стандартной деятельности	современные принципы поиска, хранения, обработки, анализа и представления в требуемом формате информации	решать задачи обработки данных с помощью современных средств автоматизации	навыками обеспечения информационной безопасности	- комплект заданий для выполнения лабораторных работ; практических работ; - тестовые задания; - типовые задания по вариантам для выполнения расчетно-графической работы;	Экзаменационные билеты

2. Оценка уровня сформированности компетенций (индикаторов их достижения)

Показатели оценивания компетенций (индикаторов их достижения)	**Шкала и критерии оценки уровня сформированности компетенций(индикаторов их достижения)**			
	Ниже порогового *(«неудовлетворительно»)*	**Пороговый** *(«удовлетворительно»)*	**Продвинутый** *(«хорошо»)*	**Высокий** *(«отлично»)*
Полнота знаний	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущены не грубые ошибки.	Уровень знаний в объёме, соответствующем программе подготовки. Допущены некоторые погрешности.	Уровень знаний в объёме, соответствующем программе подготовки.
Наличие умений	При выполнении стандартных заданий не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Выполнены типовые задания с не грубыми ошибками. Выполнены все задания, но не в полном объеме (отсутствуют пояснения, неполные выводы)	Продемонстрированы все основные умения. Выполнены все основные задания с некоторыми погрешностями. Выполнены все задания в полном объёме, но некоторые с недочетами.	Продемонстрированы все основные умения. Выполнены все основные и дополнительные задания без ошибок и погрешностей. Задания выполнены в полном объеме без недочетов.
Наличие навыков (владение опытом)	При выполнении стандартных заданий не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для выполнения стандартных заданий с некоторыми недочетами.	Продемонстрированы базовые навыки при выполнении стандартных заданий с некоторыми недочетами.	Продемонстрированы все основные умения. Выполнены все основные и дополнительные задания без ошибок и погрешностей. Продемонстрирован творческий подход к решению нестандартных задач.
Характеристика сформированности компетенции	Компетенции фактически не сформированы. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. ИЛИ Зачетное количество баллов не набрано согласно установленному диапазону	Сформированность компетенций соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач. ИЛИ Набрано зачетное количество баллов согласно установленному диапазону	Сформированность компетенций в целом соответствует требованиям. Имеющихся знаний, умений, навыков достаточно для решения стандартных профессиональных задач. ИЛИ Набрано зачетное количество баллов согласно установленному диапазону	Сформированность компетенций полностью соответствует требованиям. Имеющихся знаний, умений, навыков в полной мере достаточно для решения сложных, в том числе нестандартных, профессиональных задач. ИЛИ Набрано зачетное количество баллов согласно установленному диапазону

3. Критерии и шкала оценивания заданий текущего контроля

3.1 Критерии и шкала оценивания практических работ

Перечень лабораторных и практических работ, описание порядка выполнения и защиты работы, требования к результатам работы, структуре и содержанию отчета и т.п. представлены в методических материалах по освоению дисциплины (модуля) и в электронном курсе в ЭИОС МАУ.

Оценка/баллы	Критерии оценивания
Отлично	Задание выполнено полностью и правильно. Отчет по лабораторной/практической работе подготовлен качественно в соответствии с требованиями. Полнота ответов на вопросы преподавателя при защите работы.
Хорошо	Задание выполнено полностью, но нет достаточного обоснования или при верном решении допущена незначительная ошибка, не влияющая на правильную последовательность рассуждений. Все требования, предъявляемые к работе, выполнены.
Удовлетворительно	Задания выполнены частично с ошибками. Демонстрирует средний уровень выполнения задания на лабораторную/практическую работу. Большинство требований, предъявляемых к заданию, выполнены.
Неудовлетворительно	Задание выполнено со значительным количеством ошибок на низком уровне. Многие требования, предъявляемые к заданию, не выполнены. ИЛИ Задание не выполнено.

3.2 Критерии и шкала оценивания контрольной работы

Перечень контрольных заданий, рекомендации по выполнению представлены в методических материалах по освоению дисциплины (модуля) и в электронном курсе в ЭИОС МАУ.

В ФОС включен типовой вариант контрольного задания.

1. Отличительной особенностью современности является переход от индустриального общества к информационному, в котором главным ресурсом становится информация. Перечислите основные источники информации в настоящее время.
2. Совокупность объекта разведки, технического средства разведки, и физической среды, в которой распространяется информационный сигнал, называется техническим каналом утечки информации. Приведите схему технического канала утечки информации.
3. Под безопасностью информации понимаются условия хранения, обработки и передачи информации, при которых обеспечивается ее защита от угроз уничтожения, изменения, хищения и утечки. Опишите возможные угрозы информационной безопасности.
4. Особенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды распространения сигналов конфиденциальной информации. Опишите причины возникновения электромагнитного канала утечки и информации.
5. Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» утвержденный Гостехкомиссей РФ 30.03.92 определяет комплекс мероприятий при постановке задачи защиты информации, один из которых защита информации от несанкционированного доступа (НСД). Перечислите основные способы НСД к информации согласно приведенного РД.

6. Руководящий документ "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" устанавливает 9 классов защищенности автоматизированных систем от НСД к информации. Определите класс системы если в ней работают несколько пользователей с одинаковыми правами доступа к хранящейся информации.

7. Одним из элементов защиты информации является использование криптографических систем. Их можно разделить на 2 больших класса симметричные и ассиметричные системы. Приведите 4 базовых класса симметричных криптосистем.

8. В криптографической системе с открытым ключом открытый (не секретный) ключ передаётся по открытому каналу и используется для шифрования сообщения. Для расшифровки сообщения используется закрытый ключ (секретный). На каком принципе основано симметричное шифрование?

9. Согласно руководящему документу "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации". Межсетевой экран представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС. Приведите 4 основные вида МЭ по принципу действия.

10. Антивирус – программное средство, предназначенное для борьбы с вирусами, основными задачами которой является препятствование проникновению вирусов в ОС; обнаружение наличия вирусов в ОС; устранение вирусов из ОС без нанесения повреждений другим объектам системы; минимизация ущерба от действий вирусов. Приведите основные технологии обнаружения вирусов.

11. Согласно ФЗ № 63 от 06.04.2011 Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и используется для определения подписывающего информацию. Для подписи используются хэш-функции. Объясните принцип использования хэш-функций в ЭЦП.

12. Одной из проблем использования беспроводных сетей стандарта 802.11 был низкий уровень криптографической системы защиты информации. Приведите протоколы шифрования и количество бит данных используемых для пароля в стандарте 802.11.

13. Самым простым и одним из самых эффективных алгоритмов шифрования является так называемое XOR-шифрование. Ниже приведена таблица истинности для XOR:

Таблица 1 - Таблица истинности для XOR

x	y	$z = x \oplus y$
0	0	0
1	0	1
0	1	1
1	1	0

Восстановить одно из слагаемых можно при помощи второго: или $y = z \oplus x$

Используя следующий алфавит

Таблица 2 - Алфавит

а	б	в	г
1	2	3	4

Для создания алфавита каждой букве ставится ее порядковый номер в соответствии с русским алфавитом, затем цифра переводится в десятичную систему счисления (возможно использование калькулятора ОС Windows в режиме "Программист")

Используя ключ (номер варианта соответствует последней цифре в зачетной книжке студента) зашифровать свою фамилию, представить исходный текст и зашифрованный.

Таблица 3 - Список ключей

Номер варианта									
0	1	2	3	4	5	6	7	8	9
ключ									
10	11	12	13	14	15	16	17	18	19

Пример:

Исходное сообщение "РСК", ключ 20

Р	С	К
18	19	12
Ключ 20		
Шифрование методом XOR		
6	7	24
Зашифрованное сообщение		
Е	Ё	Ц

14. Процесс криптографического закрытия данных может осуществляться программными и аппаратными средствами, при этом к криптографической системе предъявляется ряд требований. Сформулируйте основные требования к криптосистемам.

15. Одним из наиболее уязвимых мест в защите информации при платежах банковскими картами в терминалах является процесс аутентификации платежной карты. Опишите преимущества информационной защиты EMV-карт над картами с магнитной полосой.

Оценка/баллы	**Критерии оценивания**
Отлично	Работа выполнена полностью, без ошибок (возможна одна неточность, описка, не являющаяся следствием непонимания материала).
Хорошо	Работа выполнена полностью, но обоснования шагов решения недостаточны, допущена одна негрубая ошибка или два-три недочета, не влияющих на правильную последовательность рассуждений.

Удовлетворительно	В работе допущено более одной грубой ошибки или более двух-трех недочетов, но обучающийся владеет обязательными умениями по проверяемой теме.
Неудовлетворительно	В работе есть грубые ошибки и недочеты ИЛИ Контрольная работа не выполнена.

4. Критерии и шкала оценивания результатов обучения по дисциплине (модулю) при проведении промежуточной аттестации

Критерии и шкала оценивания результатов освоения дисциплины (модуля) с экзаменом

Для дисциплин (модулей), заканчивающихся экзаменом, результат промежуточной аттестации складывается из баллов, набранных в ходе текущего контроля и при проведении экзамена:

В ФОС включен список вопросов и заданий к экзамену и типовой вариант экзаменационного билета:

1. Информационная безопасность как часть национальной безопасности страны.
2. Объекты информационной безопасности. Источники угроз информационной безопасности РФ.
3. Законодательная база защиты информации в РФ. Перечень сведений относящихся к государственной тайне.
4. Источники информации. Технические каналы утечки информации, причины их образования.
5. Угрозы безопасности информации. Возможности перехвата информации.
6. Построение защиты информации на предприятии. Принципы построения защиты информации в автоматизированных системах.
7. Несанкционированный доступ к информации, хранящейся на СВТ. Основные способы НСД к информации
8. Основные направления обеспечения защиты от НСД. Классификация нарушителя. Требования к показателям защищенности.
9. Классы защищенности АС. Дискреционная и мандатная защита в АС.
10. Системы защиты АС от НСД. Компоненты. Возможности.
11. Защита информации в электронных платежных системах. Защита данных при транзакции в различных типах платежных карт.
12. Криптографические системы. Требования к криптографическим системам. Ключ (открытый и закрытый), алфавит. Криптоатаки.
13. Симметричные и ассиметричные криптографические системы.
14. Политика сетевой безопасности предприятия.
15. Защита информации в беспроводных сетях
16. Межсетевые экраны, классификация, принцип работы.
17. Антивирусная защита информационных систем. Классификация вирусов. Режимы работы антивирусов.
18. Антивирусная защита информационных систем. Антивирусы. Технологии обнаружения вирусов.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МУРМАНСКИЙ АРКТИЧЕСКИЙ УНИВЕРСИТЕТ»

Морская академия
Наименование структурного подразделения

Кафедра радиотехники и связи
Наименование кафедры

Специальность 11.05.01 Радиоэлектронные системы и комплексы
Специализация Радиоэлектронные системы управления и передачи информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №____

по дисциплине «Основы защиты информационных систем»

Вопрос 1. Информационная безопасность как часть национальной безопасности страны

Вопрос 2. Антивирусная защита информационных систем. Антивирусы. Технологии обнаружения вирусов

Оценка	Критерии оценки ответа на экзамене
Отлично	Обучающийся глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, не затрудняется с ответом при видоизменении вопроса. Владеет специальной терминологией, демонстрирует общую эрудицию в предметной области, использует при ответе ссылки на материал специализированных источников, в том числе на Интернет-ресурсы.
Хорошо	Обучающийся твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, владеет специальной терминологией на достаточном уровне; могут возникнуть затруднения при ответе на уточняющие вопросы по рассматриваемой теме; в целом демонстрирует общую эрудицию в предметной области.
Удовлетворительно	Обучающийся имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, плохо владеет специальной терминологией, допускает существенные ошибки при ответе, недостаточно ориентируется в источниках специализированных знаний.
Неудовлетворительно	Обучающийся не знает значительной части программного материала, допускает существенные ошибки, нарушения логической последовательности в изложении программного материала, не владеет специальной терминологией, не ориентируется в источниках специализированных знаний. Нет ответа на поставленный вопрос.

Оценка, полученная на экзамене, переводится в баллы («5» - 20 баллов, «4» - 15 баллов, «3» - 10 баллов) и суммируется с баллами, набранными в ходе текущего контроля.

Итоговая оценка по дисциплине (модулю)	Суммарные баллы по дисциплине (модулю), в том числе	Критерии оценивания
Отлично	91 - 100	Выполнены все контрольные точки текущего контроля на высоком уровне. Экзамен сдан
Хорошо	81-90	Выполнены все контрольные точки текущего контроля. Экзамен сдан
Удовлетворительно	70- 80	Контрольные точки выполнены в неполном объеме. Экзамен сдан
Неудовлетворительно	69 и менее	Контрольные точки не выполнены или не сдан экзамен

5. Задания диагностической работы для оценки результатов обучения

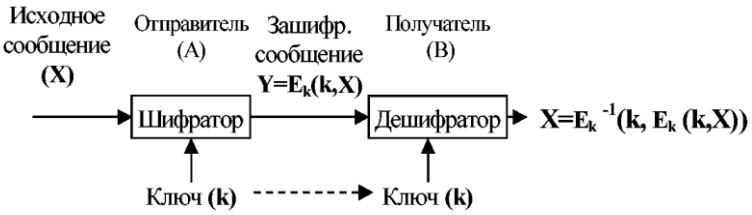
по дисциплине (модулю) в рамках внутренней независимой оценки качества образования

ФОС содержит задания для оценивания знаний, умений и навыков, демонстрирующих уровень сформированности компетенций и индикаторов их достижения в процессе освоения дисциплины (модуля).

Комплект заданий разработан таким образом, чтобы осуществить процедуру оценки каждой компетенции, формируемых дисциплиной (модулем), у обучающегося в письменной форме.

Содержание комплекта заданий включает: тестовые задания и расчетные задачи,

Комплект заданий диагностической работы

Компетенция ОПК-7 Способен решать стандартные задачи профессиональной деятельности с применением современных методов исследования и информационно-коммуникационных технологий	
1.	Какой протокол обеспечивает безопасное подключение в сети Internet: a) ftp b) https c) http d) нет правильного ответа
2.	Какие требования к паролю необходимо соблюдать для сохранения данных: a) Длина и спец. символы b) Наличие подсказки c) Нет правильного ответа
3.	 На рисунке представлена система шифрования a) Симметричная b) Асимметрична
4.	В сетевых протоколах безопасности TLS и SSLприменяется a) Симметричный алгоритм шифрования b) Асимметричный алгоритм шифрования
5.	Если в автоматизированной системе работают 2 пользователя с равными правами доступа ко всей информации, то такой системы присваивают группу безопасности a) 1а/б b) 1а/б c) 2а/б
6.	Основной задаче компьютерного вируса является a) Распространение

	b) Уничтожение данных c) Блокировка компьютера d) Вовлечение в DDoS атаки
7.	Одним их методов работы антивируса является a) Сигнатурный анализ b) Блокировка входящих пакетов c) Отслеживание состояния соединения
8.	Повторение опытов позволяет: a) Исключить ошибку оператора b) Набрать статистические данные о ходе эксперимента c) Оценить ошибку и одновременно приводит к ее уменьшению d) нет правильного ответа
9.	Фишинговая атака представляет собой a) Выдачу фейковых сайтов, имитирующих интернет-страницы популярных компаний за настоящие с целью заражения ПК вирусом b) Подмену исходящих пакетов пользователя c) Атаку «человек посередине»
10.	Причины образования технических каналов утечки информации a) Несовершенство элементной базы b) Несовершенство схемных решений c) Злоумышленные действия d) Все выше перечисленные