Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 11.03.01 Радиотехника

Наименование образовательной программы: Беспроводные технологии и интернет вещей

Уровень образования: высшее образование - бакалавриат

Форма обучения: Заочная

Оценочные материалы
по дисциплине
Защита информации

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Шалимова Е.В. Идентификатор: Rf4bb1f0c-ShalimovaYV-f267ebd6	Е.В. Шалимова
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Шиндина Т.А. Идентификатор: Rd0ad64b2-ShindinaTA-e12224c9	Т.А. Шиндина
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ПК-1 Способен осуществлять сбор научно-технической информации для проведения оценочных расчетов отдельных блоков радиоэлектронных устройств (РЭУ), осуществлять разработку функциональных схем РЭУ и компьютерное моделирование отдельных блоков РЭУ

ИД-1 Умеет проводить сбор и анализ научно-технической информации для проведения оценочных расчетов параметров элементов радиоэлектронных устройств, составлять научно-технические отчеты по результатам работы

ИД-2 Знает методы построения функциональных схем радиоэлектронного устройства и умеет выполнять компьютерное моделирование элементов радиоэлектронных устройств по типовым методикам с использованием пакетов прикладных программ

и включает:

для текущего контроля успеваемости:

Форма реализации: Выполнение задания

1. "Проведение анализа защищенности объекта защиты информации" (Решение задач)
2. "Средства защиты базы данных" (Решение задач)

Форма реализации: Компьютерное задание

1. "Защита информации" (Тестирование)
2. "Правовое обеспечение информационной безопасности" (Тестирование)

БРС дисциплины

8 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	3	6	9	12
1. Введение в информационную безопасность					
Концепция инженерно-технической защиты информации				+	
Правовое обеспечение информационной безопасности		+			
Организационное обеспечение информационной безопасности					
Характеристика угроз безопасности информации			+		+
Технические средства обеспечения информационной безопасности					+

Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах				
Структура и принципы функционирования современных вычислительных систем			+	
Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств			+	
Защита от компьютерных вирусов	+		+	
Уничтожение остаточных данных			+	
Защита от потери информации				
Защита от потери информации и отказов программно-аппаратных средств		+		+
Защита информационно-программного обеспечения на уровне операционных систем		+		+
Защита информации на уровне систем управления базами данных		+		+
Специфические особенности защиты информации в локальных и глобальных компьютерных сетях		+		+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-1	ИД-1$_{ПК-1}$ Умеет проводить сбор и анализ научно-технической информации для проведения оценочных расчетов параметров элементов радиоэлектронных устройств, составлять научно-технические отчеты по результатам работы	Знать: основные руководящие и нормативные документы в сфере инженерно-технической защите информации методику организации инженерно-технической защиты информации основные принципы организации и методы реализации технической защиты информации Уметь: использовать основные принципы и методы инженерно-технической защиты информации различать виды защищаемой информации, идентифицировать её источники и носители	"Правовое обеспечение информационной безопасности" (Тестирование) "Проведение анализа защищенности объекта защиты информации" (Решение задач) "Защита информации" (Тестирование) "Средства защиты базы данных" (Решение задач)
ПК-1	ИД-2$_{ПК-1}$ Знает методы построения функциональных схем	Знать: виды, источники и носители защищаемой	"Правовое обеспечение информационной безопасности" (Тестирование) "Проведение анализа защищенности объекта защиты информации"

	радиоэлектронного устройства и умеет выполнять компьютерное моделирование элементов радиоэлектронных устройств по типовым методикам с использованием пакетов прикладных программ	информации основные угрозы безопасности информации методы оценки угрозы инженерно-технического добывания информации концепцию инженерно-технической защиты информации Уметь: выявлять основные угрозы безопасности информации и оценивать их степень использовать основные руководящие и нормативные документы в сфере инженерно-технической защите информации	(Решение задач) "Защита информации" (Тестирование) "Средства защиты базы данных" (Решение задач)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. "Правовое обеспечение информационной безопасности"

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Технология проверки связана с выполнением контрольного теста по изученной теме. Время, отведенное на выполнение задания, устанавливается не более 30 минут. Количество попыток не более 3х. Тестирование проводится с использованием СДО "Прометей". К тестированию допускается пользователь, изучивший материалы, авторизированный уникальным логином и паролем

Краткое содержание задания:
Контрольная точка направлена на проверку знаний по теме “Правовое обеспечение информационной безопасности”

Контрольные вопросы/задания:

Знать: методику организации инженерно-технической защиты информации	1.Ответственность за правонарушения в информационной сфере реализуется в рамках 1. регулятивных правоотношений 2. правоохранительных правоотношений 3. карательных правоотношений 4. социальных правоотношений Ответ: 2 2.Правонарушения можно рассматривать в качестве информационно-правовых, если их связь с информацией является 1. непосредственной или опосредованной наличием ее материального носителя 2. опосредованной наличием ее подтверждения 3. закономерной 4. все перечисленное верно Ответ: 3 3.Чем является система обеспечения информационной безопасности РФ? 1. частью системы обеспечения национальной безопасности страны, призванной к реализации государственной политики в информационной сфере 2. системой обеспечения национальной безопасности страны, призванной к реализации государственной политики в информационной сфере 3. частью системы обеспечения национальной безопасности страны, призванной к реализации государственной политики в экономической сфере 4. системой обеспечения национальной безопасности страны, призванной к реализации государственной

	политики в экономической сфере Ответ: 1
Знать: методы оценки угрозы инженерно-технического добывания информации	1.Государственное властное принуждение является 1. содержанием юридической ответственности 2. сущностью юридической ответственности 3. функцией юридической ответственности 4. целью юридической ответственности Ответ: 1
Знать: основные угрозы безопасности информации	1.Что относится к важнейшим функциям системы обеспечения информационной безопасности? 1. разработка нормативной правовой базы в сфере обеспечения информационной безопасности 2. создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере 3. оценка состояния информационной безопасности РФ, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз 4. все перечисленное верно Ответ: 4 2.Какой закон, регламентирующий отношения в области науки и техники, занимает главенствующее место среди специально разработанных для этих целей нормативных правовых актов? 1. ФЗ «О науке и государственной научно-технической политике» 2. ФЗ «О государственной тайне» 3. ФЗ «О средствах массовой информации» 4. ФЗ «О связи» Ответ: 1

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 80

Описание характеристики выполнения знания: Оценка «отлично» выставляется если задание выполнено в полном объеме или выбрано верно на 80 %

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Оценка «хорошо» выставляется если большинство вопросов раскрыто. Выбрано верное направления для решения задач

Оценка: 3

Нижний порог выполнения задания в процентах: 55

Описание характеристики выполнения знания: Оценка «удовлетворительно» выставляется если задания преимущественно выполнены

КМ-2. "Проведение анализа защищенности объекта защиты информации"

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Решение задач
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Решенные задания по вариантам отправляются в СДО "Прометей" в рамках функционала "письменная работа"

Краткое содержание задания:
Контрольная точка направлена на закрепление знаний основного понятийного аппарата, применяемого в области защиты информации

Контрольные вопросы/задания:

<table>
<tr>
<td>Уметь: различать виды защищаемой информации, идентифицировать её источники и носители</td>
<td>1.Провести анализ защищенности объекта защиты информации по разделу “Виды возможных угроз”
<table>
<tr><th rowspan="2">Приоритет</th><th rowspan="2">Виды угроз</th><th colspan="3">Субъекты угроз</th></tr>
<tr><th>Стихия</th><th>Нарушитель</th><th>Злоумышленник</th></tr>
<tr><td></td><td></td><td></td><td></td><td>На территории</td><td>Вне территории</td></tr>
<tr><td>1</td><td>Травмы и гибель людей</td><td>+</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>2</td><td>Повреждение оборудование, техники</td><td>+</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>3</td><td>Повреждение систем жизнеобеспечения</td><td>+</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>4</td><td>Несанкционированное изменение технологического процесса</td><td></td><td>+</td><td>+</td><td></td></tr>
<tr><td>5</td><td>Использование нерегламентированных технических и программных средств</td><td></td><td>+</td><td>+</td><td></td></tr>
<tr><td>6</td><td>Дезорганизация функционирования предприятия</td><td>+</td><td></td><td>+</td><td></td></tr>
<tr><td>7</td><td>Хищение материальных ценностей</td><td></td><td></td><td>+</td><td></td></tr>
<tr><td>8</td><td>Уничтожение или перехват данных путем хищения носителей информации</td><td></td><td></td><td>+</td><td></td></tr>
<tr><td>9</td><td>Устное разглашение конфиденциальной информации</td><td></td><td>+</td><td></td><td></td></tr>
<tr><td>10</td><td>Несанкционированный съем информации</td><td></td><td></td><td>+</td><td>+</td></tr>
</table>
2.Провести анализ защищенности объекта защиты информации по разделу “Характер происхождения угроз"
3. Определить класс защищенности автоматизированной системы</td>
</tr>
<tr>
<td>Уметь: выявлять основные угрозы безопасности информации и оценивать их степень</td>
<td>1.Провести анализ защищенности объекта защиты информации по разделу “Классы каналов несанкционированного получения информации"
2.Провести анализ защищенности объекта защиты информации по разделу “Источники появления угроз"</td>
</tr>
<tr>
<td>Уметь: использовать основные руководящие и нормативные документы в сфере инженерно-технической защите информации</td>
<td>1.Провести анализ защищенности объекта защиты информации по разделу “Причины нарушения целостности информации"
2.Провести анализ защищенности объекта защиты информации по разделу “Потенциально возможные злоумышленные действия"</td>
</tr>
</table>

Описание шкалы оценивания:

Оценка: зачтено

Описание характеристики выполнения знания: Выставляется "зачтено" если работа выполнена в соответствии с заданием

Оценка: не зачтено
Описание характеристики выполнения знания: Выставляется «не зачтено», если работа не представлена на проверку, выполнена не верно или выполнена с ошибками

КМ-3. "Защита информации"

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Технология проверки связана с выполнением контрольного теста по изученной теме. Время, отведенное на выполнение задания, устанавливается не более 30 минут. Количество попыток не более 3х. Тестирование проводится с использованием СДО "Прометей". К тестированию допускается пользователь, изучивший материалы, авторизированный уникальным логином и паролем

Краткое содержание задания:
Контрольная точка направлена на проверку знаний по основам защиты информации

Контрольные вопросы/задания:

Знать: основные принципы организации и методы реализации технической защиты информации	1.1. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)? A. Препятствие B. Управление доступом C. Маскировка Ответ: A 2.1. Какие средства защиты информации предназначены для внешней охраны территории объектов и защиты компонентов информационной системы организации? A. Аппаратные B. Программные C. Физические Ответ: C 3.1. К каким средствам защиты информации относятся мероприятия, регламентирующие поведение сотрудника организации? A. Организационные средства B. Аппаратно-программные C. Криптографические средства Ответ: A
Знать: основные руководящие и нормативные документы в сфере инженерно-технической защите информации	1.1. Как называется защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации? A. Информационная защита информации B. Информационная безопасность C. Зашита информации Ответ: B 2.Система криптографической защиты информации:

	A) BFox Pro B) CAudit Pro C) Крипто Про Ответ: C
Знать: виды, источники и носители защищаемой информации	1.1. При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности? A. Принуждение B. Маскировка C. Идентификация Ответ: A 2.Разновидностями угроз безопасности (сети, системы) являются: A) Программные, технические, организационные, технологические B) Серверные, клиентские, спутниковые, наземные C) Личные, корпоративные, социальные, национальные Ответ: A
Знать: концепцию инженерно-технической защиты информации	1.1. Как называется защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации? A. Информационная защита информации B. Информационная безопасность C. Зашита информации Ответ: B 2.1. Как называется установления подлинности объекта по предъявленному им идентификатору (имени)? A. Аутентификация B. Идентификация C. Маскировка Ответ: A
Знать: методы оценки угрозы инженерно-технического добывания информации	1.1. Какие средства защиты информации регламентируют правила использования, обработки и передачи информации и устанавливают меры ответственности? A. Законодательные средства B. Организационные средства C. Аппаратно-программные Ответ: A

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 80

Описание характеристики выполнения знания: Оценка «отлично» выставляется если задание выполнено в полном объеме или выбрано верно на 80 %

Оценка: 4

Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка «хорошо» выставляется если большинство вопросов раскрыто. Выбрано верное направления для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 55
Описание характеристики выполнения знания: Оценка «удовлетворительно» выставляется если задания преимущественно выполнены

КМ-4. "Средства защиты базы данных"

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Решение задач
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Решенные задания по вариантам отправляются в СДО "Прометей" в рамках функционала "письменная работа"

Краткое содержание задания:
Контрольная точка направлена на умение применить полученные знания по теме "Защита информации на уровне систем управления базами данных"

Контрольные вопросы/задания:

Уметь: использовать основные принципы и методы инженерно-технической защиты информации

1.Установите соответствие

1. Сервер	А) операционные системы и сетевые приложения или сетевые службы
2. Сетевая карта	Б) устройства сети, которое соединяют два отдельных сегмента, ограниченных своей физической длиной, и передают трафик между ними
3. Витая пара	В) специальный компьютер, который предназначен для удаленного запуска приложений, обработки запросов на получение информации из баз данных и обеспечения связи с общими внешними устройствами
4.Коаксиальный кабель	Г) устройство для разделения или объединения нескольких компьютерных сетей
5. Мост	Д) это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами
6.Маршрутизатор	Е) специальная плата в корпусе настольного компьютера или ноутбука, позволяющая подключать его в локальную сеть с помощью специального кабеля
7. Рабочая станция	Ж) набор из 8 проводов, скрученных попарно и заключенных в общую изолирующую трубку.
8.Программное	З) представляет собой проводник,

	обеспечение сетей | заключенный в экранирующую оплетку. 2.Составить отчет по выполненной работе
Уметь: различать виды защищаемой информации, идентифицировать её источники и носители	1.Создать копию БД в отдельном каталоге и с помощью мастера защиты создать файл рабочей группы, добавить пользователей, определить их права, пароли и уникальный личный код 2. • Выполнить кодирование и декодирование защищенной БД
Уметь: выявлять основные угрозы безопасности информации и оценивать их степень	1.Обеспечить защиту созданной БД установкой пароля для открытия БД
Уметь: использовать основные руководящие и нормативные документы в сфере инженерно-технической защите информации	1.Изучить теоретический материал по теме "Защита информации на уровне систем управления базами данных"

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Выставляется "зачтено" если работа выполнена в соответствии с заданием

Оценка: не зачтено
Описание характеристики выполнения знания: Выставляется «не зачтено», если работа не представлена на проверку, выполнена не верно или выполнена с ошибками

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

1. Методы разграничения доступа. Криптографические методы обеспечения конфиденциальности информации
2. Информационная безопасность. Основные определения

Процедура проведения

Решенные задания по вариантам отправляются в СДО "Прометей" в рамках функционала "письменная работа"

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-1$_{ПК-1}$ Умеет проводить сбор и анализ научно-технической информации для проведения оценочных расчетов параметров элементов радиоэлектронных устройств, составлять научно-технические отчеты по результатам работы

Вопросы, задания

1.Информационная безопасность. Основные определения
2.Угрозы информационной безопасности
3.Модель системы зашиты
4.Организационные меры и меры обеспечения физической безопасности
5.Построение систем защиты от угроз нарушения целостности: типовая структура такой системы
6.Структура системы защиты от угроз нарушения доступности: поясните основные составляющие

Материалы для проверки остаточных знаний

1.Ответственность за правонарушения в информационной сфере реализуется в рамках
Ответы:
1. регулятивных правоотношений
2. правоохранительных правоотношений
3. карательных правоотношений
4. социальных правоотношений
Верный ответ: 2

2.Наиболее важным при реализации защитных мер политики безопасности является следующее:
Ответы:
1. Аудит, анализ затрат на проведение защитных мер
2. Аудит, анализ безопасности
3. Аудит, анализ уязвимостей, риск-ситуаций
Верный ответ: 3

3.Конфиденциальность:
Ответы:

1. защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
2. описание процедур
3. защита от несанкционированного доступа к информации

Верный ответ: 3

4.Наиболее распространены средства воздействия на сеть офиса:

Ответы:

1. Слабый трафик, информационный обман, вирусы в интернет
2. Вирусы в сети, логические мины (закладки), информационный перехват
3. Компьютерные сбои, изменение администрирования, топологии

Верный ответ: 2

5.Какие угрозы безопасности информации являются преднамеренными?

Ответы:

1. ошибки персонала
2. открытие электронного письма, содержащего вирус
3. не авторизованный доступ

Верный ответ: 3

2. Компетенция/Индикатор: ИД-2$_{ПК-1}$ Знает методы построения функциональных схем радиоэлектронного устройства и умеет выполнять компьютерное моделирование элементов радиоэлектронных устройств по типовым методикам с использованием пакетов прикладных программ

Вопросы, задания

1.Правовое регулирование в области безопасности информации: законодательная база информатизации общества; структура государственных органов, обеспечивающих безопасность информационных технологий
2.Идентификация и аутентификация. Методы аутентификации
3.Особенности парольных систем аутентификации: рекомендации по практической реализации парольных систем, оценка стойкости парольных систем, методы хранения паролей
4.Методы разграничения доступа. Криптографические методы обеспечения конфиденциальности информации
5.Методы зашиты внешнего периметра
6.Протоколирование и аудит

Материалы для проверки остаточных знаний

1.

Правонарушения можно рассматривать в качестве информационно-правовых, если их связь с информацией является

Ответы:

1. непосредственной или опосредованной наличием ее материального носителя
2. опосредованной наличием ее подтверждения
3. закономерной
4. все перечисленное верно

Верный ответ: 3

2.Система криптографической защиты информации:

Ответы:

1. BFox Pro
2. CAudit Pro
3. Крипто Про

Верный ответ: 3

3.Вирусы, которые активизируются в самом начале работы с операционной системой:

Ответы:

1. загрузочные вирусы
2. троянцы
3. черви

Верный ответ: 1

4.Выберите, что самое главное должно продумать руководство при классификации данных:

Ответы:

1. управление доступом, которое должно защищать данные
2. оценить уровень риска и отменить контрмеры
3. необходимый уровень доступности, целостности и конфиденциальности

Верный ответ: 3

5.Разновидностями угроз безопасности (сети, системы) являются:

Ответы:

1. Программные, технические, организационные, технологические
2. Серверные, клиентские, спутниковые, наземные
3. Личные, корпоративные, социальные, национальные

Верный ответ: 1

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка «отлично» выставляется если задание выполнено в полном объеме или выбрано верно на 80 %

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка «отлично» выставляется если задание выполнено в полном объеме или выбрано верно на 80 %

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка «удовлетворительно» выставляется если задания преимущественно выполнены

III. Правила выставления итоговой оценки по курсу

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ "МЭИ"