

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

**Направление подготовки/специальность: 09.03.01 Информатика и вычислительная техника**

**Наименование образовательной программы: Системы автоматизированного проектирования**

**Уровень образования: высшее образование - бакалавриат**

**Форма обучения: Очная**

**Оценочные материалы  
по дисциплине  
Защита информации**

**Москва  
2021**

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Андреева И.Н.
	Идентификатор	Rb5322c60-AndreevaIN-0472a135

(подпись)

И.Н.

Андреева

(расшифровка  
подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной  
программы

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Андреева И.Н.
	Идентификатор	Rb5322c60-AndreevaIN-0472a135

(подпись)

И.Н.

Андреева

(расшифровка  
подписи)

Заведующий  
выпускающей кафедры

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Топорков В.В.
	Идентификатор	Rc76a6458-ToporkovVV-1f71a135

(подпись)

В.В.

Топорков

(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. ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ИД-2 Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью

2. ПК-2 Способен определять конфигурацию и технические характеристики оборудования, необходимые для установки программного продукта

ИД-3 Демонстрирует знание методов средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Билеты (письменный опрос)

1. Нормативные документы (Контрольная работа)

Форма реализации: Компьютерное задание

1. Защиты ПО с использованием криптографических алгоритмов (Лабораторная работа)

2. Идентификация и аутентификация субъектов и объектов (Лабораторная работа)

3. Изучение алгоритмов асимметричного шифрования и ЭЦП (Лабораторная работа)

## БРС дисциплины

8 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	3	5	9	13
Основные правовые нормы и классификация средств защиты информации и программного обеспечения от несанкционированного доступа					
Основополагающие документы по информационной безопасности	+				
Идентификация и установление подлинности пользователей, устройств, вычислительных систем					
Идентификация и аутентификация субъектов и объектов			+		
Криптографические методы защиты					

Системы шифрования			+	
Методы и средства защиты компьютерных сетей				
Функции и сервисы безопасности сетей				+
Вес КМ:	15	30	30	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
ОПК-3	ИД-2 <sub>ОПК-3</sub> Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью	Знать: основные правовые нормы и базовые принципы организации систем защиты данных ПЭВМ и компьютерных сетей	Нормативные документы (Контрольная работа)
ПК-2	ИД-3 <sub>ПК-2</sub> Демонстрирует знание методов средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа	Знать: методику оптимального выбора программных, технических средств и их конфигурации для задач защиты от не-санкционированного доступа Уметь: использовать приемы безопасной работы в сетях, включая поиск профильной информации в Интернет определять состав, устанавливать и работать с современными системами программирования для	Идентификация и аутентификация субъектов и объектов (Лабораторная работа) Защиты ПО с использованием криптографических алгоритмов (Лабораторная работа) Изучение алгоритмов асимметричного шифрования и ЭЦП (Лабораторная работа)

		разработки средств защиты ПЭВМ и компьютерных сетей	
--	--	---	--

## II. Содержание оценочных средств. Шкала и критерии оценивания

### КМ-1. Нормативные документы

**Формы реализации:** Билеты (письменный опрос)

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 15

**Процедура проведения контрольного мероприятия:** Ответы на вопросы КР

#### Краткое содержание задания:

Основные правовые нормы и базовые принципы организации систем защиты данных

#### Контрольные вопросы/задания:

Знать: основные правовые нормы и базовые принципы организации систем защиты данных ПЭВМ и компьютерных сетей	1. Назовите основные документы РФ по информационной безопасности 2. Назовите классификационные признаки трёх типов классов безопасности
--	--

#### Описание шкалы оценивания:

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания:* Оценка "отлично" выставляется, если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 75*

*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется, если большинство вопросов раскрыто, выбрано верное направление для решения задач

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется, если задание преимущественно выполнено

### КМ-2. Идентификация и аутентификация субъектов и объектов

**Формы реализации:** Компьютерное задание

**Тип контрольного мероприятия:** Лабораторная работа

**Вес контрольного мероприятия в БРС:** 30

**Процедура проведения контрольного мероприятия:** Домашняя подготовка и выполнение лабораторной работы. Демонстрация разработанных проектов и ответы на вопросы преподавателя

#### Краткое содержание задания:

Создание приложения для защиты ПО

#### Контрольные вопросы/задания:

Знать: методику оптимального выбора программных, технических средств и их	1. Назовите базовые механизмы защиты информации 2. В чём заключается произвольность дискреционного управления доступом
---	---

конфигурации для задач защиты от не-санкционированного доступа	
--	--

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 75*

*Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено*

**КМ-3. Защиты ПО с использованием криптографических алгоритмов**

**Формы реализации:** Компьютерное задание

**Тип контрольного мероприятия:** Лабораторная работа

**Вес контрольного мероприятия в БРС:** 30

**Процедура проведения контрольного мероприятия:** Домашняя подготовка и выполнение лабораторной работы. Демонстрация разработанных проектов и ответы на вопросы преподавателя

**Краткое содержание задания:**

Использование симметричных алгоритмов шифрования

**Контрольные вопросы/задания:**

Уметь: использовать приемы безопасной работы в сетях, включая поиск профильной информации в Интернет	<ol style="list-style-type: none"> <li>1.Продемонстрируйте использование криптопровайдеров</li> <li>2.Продемонстрируйте методику формирования ключей для алгоритмов шифрования</li> </ol>
--	---

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 75*

*Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено*



## КМ-4. Изучение алгоритмов асимметричного шифрования и ЭЦП

**Формы реализации:** Компьютерное задание

**Тип контрольного мероприятия:** Лабораторная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Домашняя подготовка и выполнение лабораторной работы. Демонстрация разработанных проектов и ответы на вопросы преподавателя

**Краткое содержание задания:**

Изучение алгоритмов асимметричного шифрования и ЭЦП

**Контрольные вопросы/задания:**

Уметь: определять состав, устанавливать и работать с современными системами программирования для разработки средств защиты ПЭВМ и компьютерных сетей	1.Продемонстрируйте методику выбора алгоритма хеширования 2.Создайте модель электронной цифровой подписи
--	---

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 75*

*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

# СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

## 8 семестр

Форма промежуточной аттестации: Экзамен

### Пример билета

1. Каналы утечки информации. Защита информации. Политика безопасности. Основные элементы политики безопасности.
2. Базовые криптоалгоритмы: маршруты Гамильтона, гаммирование, аналитическое преобразование.

### Процедура проведения

Устные ответы на вопросы экзаменационного билета

#### *1. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины*

**1. Компетенция/Индикатор:** ИД-2<sub>ОПК-3</sub> Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью

#### **Вопросы, задания**

1. Понятие защиты информации. Какая система считается надёжной?
2. Отечественные и международные стандарты в области информационной безопасности
3. Основные критерии оценки надёжности: политика безопасности и гарантированность
4. Классификация угроз информационной безопасности: для личности, для общества, для государства

#### **Материалы для проверки остаточных знаний**

**1. К правовым методам, обеспечивающим информационную безопасность, относятся:**

Ответы:

- а) Разработка аппаратных средств обеспечения правовых данных б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Верный ответ: в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

**2. Цели информационной безопасности – своевременное обнаружение, предупреждение:**

Ответы:

- а) несанкционированного доступа, воздействия в сети б) инсайдерства в организации в) чрезвычайных ситуаций

Верный ответ: а) несанкционированного доступа, воздействия в сети

**3. Виды информационной безопасности:**

Ответы:

- а) Персональная, корпоративная, государственная б) Клиентская, серверная, сетевая в) Локальная, глобальная, смешанная

Верный ответ: а) Персональная, корпоративная, государственная

**4. Основные объекты информационной безопасности:**

Ответы:

- а) Компьютерные сети, базы данных б) Информационные системы, психологическое состояние пользователей в) Бизнес-ориентированные, коммерческие системы

Верный ответ: а) Компьютерные сети, базы данных

**5. Основными рисками информационной безопасности являются:**

Ответы:

- а) Искажение, уменьшение объема, перекодировка информации б) Техническое вмешательство, выведение из строя оборудования сети в) Потеря, искажение, утечка информации

Верный ответ: в) Потеря, искажение, утечка информации

**6. К основным принципам обеспечения информационной безопасности относится:**

Ответы:

- а) Экономической эффективности системы безопасности б) Многоплатформенной реализации системы в) Усиления защищенности всех звеньев системы

Верный ответ: а) Экономической эффективности системы безопасности

**7. Основными субъектами информационной безопасности являются:**

Ответы:

- а) руководители, менеджеры, администраторы компаний б) органы права, государства, бизнеса в) сетевые базы данных, фаерволлы

Верный ответ: б) органы права, государства, бизнеса

**8. Наиболее распространены угрозы информационной безопасности корпоративной системы:**

Ответы:

- а) Покупка нелегального ПО б) Ошибки эксплуатации и неумышленного изменения режима работы системы в) Сознательного внедрения сетевых вирусов

Верный ответ: б) Ошибки эксплуатации и неумышленного изменения режима работы системы

**9. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:**

Ответы:

- а) Регламентированной б) Правовой в) Защищаемой

Верный ответ: в) Защищаемой

**10. Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:**

Ответы:

- а) Программные, технические, организационные, технологические б) Серверные, клиентские, спутниковые, наземные в) Личные, корпоративные, социальные, национальные

Верный ответ: а) Программные, технические, организационные, технологические

**11. Окончательно, ответственность за защищенность данных в компьютерной сети несет:**

Ответы:

- а) Владелец сети б) Администратор сети в) Пользователь сети

Верный ответ: а) Владелец сети

**12. Политика безопасности в системе (сети) – это комплекс:**

Ответы:

- а) Руководств, требований обеспечения необходимого уровня безопасности б) Инструкций, алгоритмов поведения пользователя в сети в) Нормы информационного права, соблюдаемые в сети

Верный ответ: а) Руководств, требований обеспечения необходимого уровня безопасности

**2. Компетенция/Индикатор:** ИД-3ПК-2 Демонстрирует знание методов средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа

### **Вопросы, задания**

1. Аутентификация пользователей и используемых компонентов обработки информации. Пароли и их оценки.
2. Криптографические методы защиты информации. Симметричные криптосистемы. Требования к криптографическим системам защиты информации.
3. Системы с открытым ключом. Электронная (цифровая) подпись. Алгоритмы формирования и верификации электронной цифровой подписи.
4. Проблемы защиты информации в вычислительных сетях.
5. Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление

### **Материалы для проверки остаточных знаний**

**1. Основными источниками угроз информационной безопасности являются все указанное в списке**

Ответы:

- а) Хищение жестких дисков, подключение к сети, инсайдерство б) Перехват данных, хищение данных, изменение архитектуры системы в) Хищение данных, подкуп системных администраторов, нарушение регламента работы

Верный ответ: б) Перехват данных, хищение данных, изменение архитектуры системы

**2. К основным функциям системы безопасности можно отнести все перечисленное:**

Ответы:

- а) Установление регламента, аудит системы, выявление рисков б) Установка новых офисных приложений, смена хостинг-компании в) Внедрение аутентификации, проверки контактных данных пользователей

Верный ответ: а) Установление регламента, аудит системы, выявление рисков

**3. Принципом информационной безопасности является принцип недопущения:**

Ответы:

- а) Неоправданных ограничений при работе в сети (системе) б) Рисков безопасности сети, системы в) Презумпции секретности

Верный ответ: а) Неоправданных ограничений при работе в сети (системе)

**4. Принципом политики информационной безопасности является принцип:**

Ответы:

- а) Невозможности миновать защитные средства сети (системы) б) Усиления основного звена сети, системы в) Полного блокирования доступа при риск-ситуациях

Верный ответ: а) Невозможности миновать защитные средства сети (системы)

**5. Принципом политики информационной безопасности является принцип:**

Ответы:

- а) Усиления защищенности самого незащищенного звена сети (системы) б) Перехода в безопасное состояние работы сети, системы в) Полного доступа пользователей ко всем ресурсам сети, системы

Верный ответ: а) Усиления защищенности самого незащищенного звена сети (системы)

**6. Принципом политики информационной безопасности является принцип:**

Ответы:

а) Разделения доступа (обязанностей, привилегий) клиентам сети (системы) б) Одноуровневой защиты сети, системы в) Совместимых, однотипных программно-технических средств сети, системы

Верный ответ: а) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

**7. Когда получен спам по e-mail с приложенным файлом, следует:**

Ответы:

а) Прочитать приложение, если оно не содержит ничего ценного – удалить б) Сохранить приложение в папке «Спам», выяснить затем IP-адрес генератора спама в) Удалить письмо с приложением, не раскрывая (не читая) его

Верный ответ: в) Удалить письмо с приложением, не раскрывая (не читая) его

**8. ЭЦП – это:**

Ответы:

а) Электронно-цифровой преобразователь б) Электронно-цифровая подпись в) Электронно-цифровой процессор

Верный ответ: б) Электронно-цифровая подпись

**9. Наиболее распространены угрозы информационной безопасности сети:**

Ответы:

а) Распределенный доступ клиент, отказ оборудования б) Моральный износ сети, инсайдерство в) Сбой (отказ) оборудования, нелегальное копирование данных

Верный ответ: в) Сбой (отказ) оборудования, нелегальное копирование данных

**10. Наиболее распространены средства воздействия на сеть офиса:**

Ответы:

а) Слабый трафик, информационный обман, вирусы в интернет б) Вирусы в сети, логические мины (закладки), информационный перехват в) Компьютерные сбои, изменение администрирования, топологии

Верный ответ: в) Вирусы в сети, логические мины (закладки), информационный перехват

**11. Утечкой информации в системе называется ситуация, характеризуемая:**

Ответы:

а) Потерей данных в системе б) Изменением формы информации в) Изменением содержания информации

Верный ответ: а) Потерей данных в системе

**12. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:**

Ответы:

а) Целостность б) Доступность в) Актуальность

Верный ответ: а) Целостность

**13. Угроза информационной системе (компьютерной сети) – это:**

Ответы:

а) Вероятное событие б) Детерминированное (всегда определенное) событие в) Событие, происходящее периодически

Верный ответ: а) Вероятное событие

## **II. Описание шкалы оценивания**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 75*

*Описание характеристики выполнения знания:* Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

*Оценка:* 3

*Нижний порог выполнения задания в процентах:* 60

*Описание характеристики выполнения знания:* Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

### ***III. Правила выставления итоговой оценки по курсу***

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и аттестационной составляющих.