

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

Направление подготовки/специальность: 01.04.02 Прикладная математика и информатика

Наименование образовательной программы: Искусственный интеллект

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

**Оценочные материалы
по дисциплине
Информационная безопасность компьютерных систем**

**Москва
2024**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Сергеев А.В.
	Идентификатор	R45d170df-SergeevAVad-0ce1748

А.В. Сергеев

СОГЛАСОВАНО:

Руководитель
образовательной
программы

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Варшавский П.Р.
	Идентификатор	R9a563c96-VarshavskyPR-efb4bbd

П.Р.
Варшавский

Заведующий
выпускающей
кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Варшавский П.Р.
	Идентификатор	R9a563c96-VarshavskyPR-efb4bbd

П.Р.
Варшавский

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 выполнять работы на всем жизненном цикле информационных систем в выбранной среде разработки компьютерного ПО

ИД-2 Демонстрирует знание современных программно-технических средств, информационных технологий и тенденции их развития

ИД-3 Демонстрирует умение выбирать и обосновывать выбор программно-технической среды реализации проектов по информационным технологиям

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

1. Компьютерная криминалистика (Лабораторная работа)
2. Криптографические средства защиты информации и анализ защиты данных (Лабораторная работа)
3. Оценка безопасности информационной системы (Лабораторная работа)
4. Стеганография. Программные средства и методы (Лабораторная работа)

БРС дисциплины

1 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	16
Основные методы реализации защиты информации в компьютерных системах.					
Основные методы реализации защиты информации в компьютерных системах.		+			
Криптографические методы защиты информации.					
Криптографические методы защиты информации.			+		
Методы скрытия информации в цифровых носителях и их анализ.					
Методы скрытия информации в цифровых носителях и их анализ				+	
Методы расследования инцидентов информационной безопасности.					
Методы расследования инцидентов информационной безопасности.					+
Вес КМ:		30	20	20	30

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-2 _{ПК-1} Демонстрирует знание современных программно-технических средств, информационных технологий и тенденции их развития	Знать: Методы обнаружения угроз информационной системы Базовые структуры данных и механизмы поиска информации Уметь: Проводить исследования компьютерных систем Использовать результаты журналов событий операционной системы в рамках оценки информационной безопасности компьютерных систем	Оценка безопасности информационной системы (Лабораторная работа) Криптографические средства защиты информации и анализ защиты данных (Лабораторная работа) Компьютерная криминалистика (Лабораторная работа)
ПК-1	ИД-3 _{ПК-1} Демонстрирует умение выбирать и обосновывать выбор программно-технической среды реализации проектов по информационным технологиям	Знать: Методы и средства стеганографии Методы и средства защиты информационных процессов в компьютерных системах Уметь:	Криптографические средства защиты информации и анализ защиты данных (Лабораторная работа) Стеганография. Программные средства и методы (Лабораторная работа) Компьютерная криминалистика (Лабораторная работа)

		Применять средства защиты информации Комбинировать и адаптировать современные информационно- коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	
--	--	--	--

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Оценка безопасности информационной системы

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 30

Процедура проведения контрольного мероприятия: Выполнение и защита результатов лабораторной работы 1.

Краткое содержание задания:

Провести анализ и подготовить заключение о состоянии защищенности информационной системы на основе предоставленных данных. Провести оценку безопасности информационной системы на основе предоставленных данных и разработать рекомендации по устранению выявленных рисков.

Контрольные вопросы/задания:

Знать: Методы обнаружения угроз информационной системы	1. Назначение и содержание журнала событий. 2. Как можно использовать информацию из журнала событий для составления хронологии событий? 3. Какие настройки групповой политики могут повлиять на уровень защищенности системы?
Уметь: Проводить исследования компьютерных систем	1. Как вы можете проверить, соответствуют ли настройки групповой политики стандартам и требованиям организации? 2. Приведите пример наиболее вероятных угроз для данной системы описанной в лабораторной работе. 3. Приведите пример, как вы можете найти в журнале событий неудачные попытки входа в систему.

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Выполнено в срок практически все задание.

Оценка: 4

Нижний порог выполнения задания в процентах: 80

Описание характеристики выполнения знания: Выполнена в срок основная часть задания.

Оценка: 3

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Выполнена в срок минимальная часть задания.

Оценка: 2

Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию.

КМ-2. Криптографические средства защиты информации и анализ защиты данных

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 20

Процедура проведения контрольного мероприятия: Проверка правильности выполнения лабораторной работы.

Краткое содержание задания:

1. Использование изученных криптографических средств, а также подходов получить доступ к данным криптоконтейнера.
2. Используя особенности структуры формата данных получить полный доступ к информации.

Контрольные вопросы/задания:

Знать: Базовые структуры данных и механизмы поиска информации	1.Что такое шифрованный контейнер? 2.Какие методы шифрования используются в шифрованном файле Word?
Знать: Методы и средства защиты информационных процессов в компьютерных системах	1.В чем разница между симметричной и асимметричной криптографией? 2.Что такое отрицаемое шифрования?

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Выполнено в срок практически все задание.

Оценка: 4

Нижний порог выполнения задания в процентах: 80

Описание характеристики выполнения знания: Выполнена в срок основная часть задания.

Оценка: 3

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Выполнена в срок минимальная часть задания.

Оценка: 2

Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию.

КМ-3. Стеганография. Программные средства и методы

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 20

Процедура проведения контрольного мероприятия: Выполнение и защита результатов лабораторной работы 3.

Краткое содержание задания:

1. Изучение и освоение программных средств компьютерной стеганографии и алгоритмов скрытия информации.

Контрольные вопросы/задания:

Знать: Методы и средства стеганографии	1.Что такое стеганоанализ и какие методы используются для обнаружения скрытых сообщений? 2.Какие преимущества дает метод встраивания в частотной области по сравнению с LSB-встраиванием?
Уметь: Применять средства защиты информации	1.Какую информацию необходимо учесть при выборе метода скрытия информации для конкретной задачи? 2.Какие факторы могут повлиять на успешность скрытия информации и ее обнаружения? 3.Какие ограничения и проблемы существуют при использовании метаданных для скрытия информации?

Описание шкалы оценивания:*Оценка: 5**Нижний порог выполнения задания в процентах: 90**Описание характеристики выполнения знания: Выполнено в срок практически все задание.**Оценка: 4**Нижний порог выполнения задания в процентах: 80**Описание характеристики выполнения знания: Выполнена в срок основная часть задания.**Оценка: 3**Нижний порог выполнения задания в процентах: 70**Описание характеристики выполнения знания: Выполнена в срок минимальная часть задания.**Оценка: 2**Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию.***КМ-4. Компьютерная криминалистика****Формы реализации:** Компьютерное задание**Тип контрольного мероприятия:** Лабораторная работа**Вес контрольного мероприятия в БРС:** 30**Процедура проведения контрольного мероприятия:** Выполнение и защита результатов лабораторной работы 4.**Краткое содержание задания:**

Провести анализ предоставленного дампа файловой системы.

Идентифицировать источник и характер инцидента информационной безопасности.

Собрать доказательства и подготовить отчет.

Контрольные вопросы/задания:

Уметь: Использовать результаты журналов событий операционной системы в рамках оценки информационной безопасности компьютерных систем	1.Какие программы были запущены на компьютере пользователя в момент инцидента? 2.Назовите полное имя владельца система в предоставленном дампа.
Уметь: Комбинировать и адаптировать современные	1.Какое время было установлено на компьютере пользователя в момент создания файла secret.txt?

информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	
---	--

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Выполнено в срок практически все задание.

Оценка: 4

Нижний порог выполнения задания в процентах: 80

Описание характеристики выполнения знания: Выполнена в срок основная часть задания.

Оценка: 3

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Выполнена в срок минимальная часть задания.

Оценка: 2

Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию.

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1 семестр

Форма промежуточной аттестации: Зачет с оценкой

Пример билета

1. Угрозы и нарушители безопасности информации

Понятие криптостойкости. Условия, предъявляемые к криптостойкости.

Процедура проведения

Зачет выставляется студентам, которые не имеют задолженностей по мероприятиям текущего контроля в семестре, на основе среднего балла, полученного по совокупности всех контрольных мероприятий в балльно-рейтинговой системе для студентов НИУ «МЭИ»

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

1. Компетенция/Индикатор: ИД-2ПК-1 Демонстрирует знание современных программно-технических средств, информационных технологий и тенденции их развития

Вопросы, задания

- 1.
1. Организационные меры защиты информации
2. Роль аудит информационной безопасности как инструмента обеспечения информационной безопасности
3. Методы сбора данных как источники доказательств
4. Преимущества предоставляет использование групповой политики безопасности в организации
5. Аудит событий безопасности в ОС Windows и Unix
6. Приведите примеры угроз, которые являются нарушением целостности и доступности

Материалы для проверки остаточных знаний

1. Выберите путь хранения журнала событий Windows по умолчанию

Ответы:

- a) C:\Windows\System32\EventLog
- b) C:\Windows\System32\System\CurrentControlSet\Services\EventLog
- c) C:\Windows\System32\winevt\Logs
- d) C:\Windows\System32\LogFiles\

Верный ответ: c

2. Какова роль аудит информационной безопасности как инструмента обеспечения информационной безопасности?

Ответы:

- a) Обеспечение конфиденциальности данных.
- b) Предотвращение несанкционированного доступа к информационным ресурсам.
- c) Оценка соответствия системы информационной безопасности установленным стандартам и политикам.
- d) Разработка и внедрение политики информационной безопасности.

Верный ответ: c

3. Как называется процесс проверки соответствия системы безопасности установленным стандартам?

Ответы:

- a) Аудит информационной безопасности.
- b) Тестирование на проникновение.
- c) Анализ уязвимостей.
- d) Моделирование угроз.

Верный ответ: a

4. Как можно защитить информацию от несанкционированного доступа?

Ответы:

- a) Установкой паролей на файлы.
- b) Использованием брандмауэров.
- c) Шифрованием данных.
- d) Все вышеперечисленное.

Верный ответ: d

5. Какой из методов защиты информации не подходит для защиты от атак с использованием социальной инженерии?

Ответы:

- a) Обучение правилам информационной безопасности.
- b) Установка брандмауэра.
- c) Использование сильных паролей.
- d) Проведение регулярного аудита информационной.

Верный ответ: b

6. Какой источник поможет определить, скомпрометированы ли учетные записи пользователей в результате инцидента?

Ответы:

- a) Анализ активности пользователей в журнале событий.
- b) Проверка времени последнего входа в систему.
- c) История запросов браузера.
- d) Проверка настроек безопасности учетных записей.

Верный ответ: a

7. Как можно отличить атаку DoS (Denial of Service) и DDoS (Distributed Denial of Service) при анализе сетевого трафика?

Ответы:

- a) Проверка наличия источника атаки, расположенного в одной сети.
- b) Анализ трафика на предмет большого количества запросов с одного IP-адреса.
- c) Проверка наличия множества источников атаки, расположенных в разных сетях.
- d) Анализ трафика на предмет использования специфических методов атаки DoS.

Верный ответ: c

8. Какую основную функцию выполняет антивирусное программное обеспечение?

Ответы:

- a) Улучшение графической производительности компьютера.
- b) Исследование операционной системы на использование программ актуальных версий.
- c) Обнаружение и удаление вредоносного программного обеспечения с компьютера.
- d) Сжатие и редактирование файлов для запутывания вредоносных средств.

Верный ответ: c

9. Какой из следующих подходов является наиболее эффективным для предотвращения подобных инцидентов в будущем после завершения расследования?

Ответы:

- a) Устранение уязвимостей, которые позволили злоумышленнику осуществить атаку.
- b) Ограничение доступа к критическим системам и данным.
- c) Обучение сотрудников правилам информационной безопасности.

d) Внедрение систем мониторинга и детектирования инцидентов информационной безопасности.

Верный ответ: d

2. Компетенция/Индикатор: ИД-ЗПК-1 Демонстрирует умение выбирать и обосновывать выбор программно-технической среды реализации проектов по информационным технологиям

Вопросы, задания

1. Задачи и методы стеганографии в компьютерных системах
2. Каковы цели контроля и проверки процессов и систем
3. Системы управления криптографическими ключами.
4. Преимущества и недостатки у централизованной системы управления антивирусным программным обеспечением
5. Основные функции программного обеспечения при обследовании состояния безопасности компьютерных систем
6. MITRE ATT&CK цель и задачи в обеспечении информационной безопасности

Материалы для проверки остаточных знаний

1. Что такое стеганография?

Ответы:

- a) Метод шифрования данных с помощью алгоритмов, которые не могут быть взломаны.
- b) Метод скрытия информации в других данных, делая ее незаметной для несанкционированного доступа.
- c) Метод создания цифровых подписей для проверки подлинности данных.
- d) Метод скрытия местоположения сервера, чтобы сделать его недоступным для хакеров.

Верный ответ: b

2. Какой из следующих вариантов НЕ является принципом Керкгоффса?

Ответы:

- a) Безопасность системы должна основываться на секретности ключа, а не на секретности алгоритма.
- b) Алгоритм шифрования должен быть открытым и доступным для анализа, чтобы его безопасность можно было проверить.
- c) Открытость реализации системы не должна снижать ее безопасность.
- d) Безопасность системы зависит от секретности ключей и алгоритма шифрования.

Верный ответ: d

3. Что такое коэффициент использования контейнера

Ответы:

- a) мера того, насколько контейнер защищен от несанкционированного доступа.
- b) это коэффициент шифрования данных внутри контейнера.
- c) механизм для определения количества допустимых пользователей контейнера.
- d) мера насколько эффективно используется пространство контейнера для скрытия информации.

Верный ответ: d

4. Что такое PGP?

Ответы:

- a) Программное обеспечение для редактирования фотографий, популярное среди профессиональных дизайнеров.
- b) Система управления проектами, используемая для организации командной работы и отслеживания задач.
- c) Программное обеспечение для шифрования и электронной подписи, используемое для защиты данных и электронных коммуникаций.

d) Виртуальная среда с возможностью загружать, хранить и делиться файлами с другими пользователями.

Верный ответ: с

5.Какой из следующих методов может быть использован для анализа цифровых следов, оставленных злоумышленником?

Ответы:

- a) Анализ временных отметок файлов и папок.
- b) Анализ содержимого файлов и папок.
- c) Анализ метаданных файлов.
- d) Все вышеперечисленное.

Верный ответ: d

6.Какие из перечисленных методов защиты информации НЕ могут быть применены для предотвращения атаки “человек по середине”?

Ответы:

- a) Использовать шифрование данных с помощью SSL/TLS.
- b) Регулярное обновление программного обеспечения.
- c) Использование антивирусной защиты.
- d) Использование двухфакторной аутентификации.

Верный ответ: с

7.Какой из следующих методов наиболее эффективен для защиты конфиденциальной информации, хранящейся в файлах с открытым исходным кодом?

Ответы:

- a) Использование обфускации кода.
- b) Применение лицензионных соглашений.
- c) Разработка специальных систем защиты.
- d) Использование стеганографии.

Верный ответ: a

8.Как можно определить, был ли файл ZIP модифицирован после создания?

Ответы:

- a) Анализ времени модификации файла.
- b) Анализ структуры заголовка файла ZIP.
- c) Проверка цифровой подписи файла.
- d) Проверка контрольной суммы файла.

Верный ответ: d

9.Какой из перечисленных алгоритмов является асимметричным криптоалгоритмом?

Ответы:

- a) AES
- b) RSA
- c) SHA-256
- d) DES

Верный ответ: b

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Оценка "отлично" проставляется студентам получившим положительные оценки (5,4,3) за все мероприятия текущего контроля в семестре и имеющим балл по семестровой составляющей не ниже 4.5

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Оценка "хорошо" проставляется студентам получившим положительные оценки (5,4,3) за все мероприятия текущего контроля в семестре и имеющим балл по семестровый составляющей не ниже 3.5

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Оценка "удовлетворительно" проставляется студентам получившим положительные оценки (5,4,3) за все мероприятия текущего контроля в семестре и имеющим балл по семестровый составляющей не ниже 2.5

Оценка: 2

Описание характеристики выполнения знания: Оценка "неудовлетворительно" проставляется студентам имеющим неудовлетворительные оценки (2,0) по результатам текущего контроля в семестре

III. Правила выставления итоговой оценки по курсу

Определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»