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

Направление подготовки: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: очная

Оценочные материалы по практике

Производственная практика: технологическая практика

Москва 2024

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ СОСТАВИЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Артёмов А.С. Идентификатор: R5d220836-ArtiomovAlS-e034a28b	А.С. Артёмов

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

Оценочные материалы по практике предназначены для оценки достижения обучающимися запланированных результатов обучения по практике, этапа формирования запланированных компетенций, прохождения практики.

Оценочные материалы по практике включают оценочные средства для проведения текущего контроля и промежуточной аттестации.

Запланированные результаты обучения по практике, соотнесенные с индикаторами достижения компетенций:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ПК-1 Готов к внедрению систем защиты информации автоматизированных систем	ПК-2.1$_{ПК-1}$ Устанавливает и настраивает средства защиты информации в автоматизированных системах	знать: - сущность и значение информации в развитии современного общества. уметь: - устанавливать и настраивать средства защиты информации в автоматизированных системах;.
	ПК-2.2$_{ПК-1}$ Разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах	знать: - методы анализа изучаемых явлений, процессов и проектных решений. уметь: - разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах.
	ПК-2.3$_{ПК-1}$ Внедряет организационные меры по защите информации в автоматизированных системах	знать: - организационные меры по защите информации в автоматизированных системах. уметь: - внедрять организационные меры по защите информации в автоматизированных системах.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
ПК-2 Способен администрировать средства защиты информации в компьютерных системах и сетях	ПК-3.1$_{ПК-2}$ Администрирует подсистемы защиты информации в операционных системах	знать: - администрирование подсистем защиты информации в операционных системах. уметь: - оценивать угрозы безопасности информации операционных систем.
	ПК-3.2$_{ПК-2}$ Администрирует программно-аппаратные средства защиты информации в компьютерных сетях	знать: - администрирование программно-аппаратных средств защиты информации в компьютерных сетях. уметь: - оценивать угрозы безопасности информации в компьютерных сетях.
	ПК-3.3$_{ПК-2}$ Администрирует средства защиты информации прикладного и системного программного обеспечения	знать: - администрирование средств защиты информации прикладного и системного программного обеспечения. уметь: - анализировать угрозы безопасности информации программного обеспечения.
РПК-1 Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации	ИД-1$_{РПК-1}$ Администрирует системы защиты информации автоматизированных систем	знать: - администрирование системы защиты информации автоматизированных систем. уметь: - организовывать работы по выявлению угроз безопасности информации в автоматизированных

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		системах.
	ИД-2$_{РПК-1}$ Управляет защитой информации в автоматизированных системах	знать: - управление защитой информации в автоматизированных системах. уметь: - проводить анализ возможностей потенциальных нарушителей по добыванию информации ограниченного доступа, обрабатываемой в автоматизированных системах.
	ИД-3$_{РПК-1}$ Выполняет мониторинг защищенности информации в автоматизированных системах	знать: - мониторинг защищенности информации в автоматизированных системах. уметь: - планировать и разрабатывать мероприятия по защите информации, обрабатываемой в автоматизированных системах, и оценивать их достаточность.
	ИД-4$_{РПК-1}$ Выполняет аудит защищенности информации в автоматизированных системах	знать: - аудит защищенности информации в автоматизированных системах. уметь: - применять организационные меры и средства защиты информации при её обработке в автоматизированных системах.

Содержание оценочных средств. Шкала и критерии оценивания.

Текущий контроль

Текущий контроль проводится в течение периода прохождения практики.

6 семестр

№	Контрольные мероприятия	Оценка	Шкала оценивания
1	Получение задания на практику	5	Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно
		4	Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач
		3	Оценка "удовлетворительно" выставляется если задание преимущественно выполнено
		2	Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено
2	Равномерность работы в течении практики	5	Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно
		4	Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач
		3	Оценка "удовлетворительно" выставляется если задание преимущественно выполнено
		2	Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено
3	Выполнение задания на практику в полном объеме	5	Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно
		4	Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач
		3	Оценка "удовлетворительно" выставляется если задание преимущественно выполнено
		2	Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

Промежуточная аттестация

Форма промежуточной аттестации в 6 семестре: зачет с оценкой

Промежуточная аттестация проводится в соответствии с положением о промежуточной аттестации ФГБОУ ВО «НИУ «МЭИ».

К промежуточной аттестации допускаются студенты, предоставившие комплект документов по результатам практики, проверенный руководителем практики от МЭИ, и получившие положительную оценку по текущему контролю по практике.

На промежуточной аттестации по результатам прохождения практики обучающемуся задаются теоретические и практические вопросы по представленному отчету и/или презентации.

Примерный перечень вопросов к промежуточной аттестации по практике:

1.Анализ угроз доступности информации программного обеспечения

2.Анализ вероятности реализации угрозы и ущерба от нее в операционных системах

3.Способы разработки мероприятий по защите информации, обрабатываемой в автоматизированных системах.

4.Способы планирования мероприятий по защите информации, обрабатываемой в автоматизированных системах.

5.Построение систем защиты от угрозы нарушения конфиденциальности информации

6.Модели угроз безопасности информации и модели нарушителя по добыванию информации ограниченного доступа, обрабатываемой в автоматизированных системах

7.Методы проведения анализа возможностей потенциальных нарушителей по добыванию информации ограниченного доступа, обрабатываемой в автоматизированных системах

8.Оценка актуальности угроз безопасности информации в автоматизированных системах

9.Применение методики оценки угроз безопасности информации в автоматизированных системах

10.Оценка результативности разработанных организационно-распорядительных документов по защите информации в автоматизированных системах в организации

11.Методы внедрения организационных мер по защите информации в автоматизированных системах

12.Особенности разрабатываемых организационно-распорядительных документов по защите информации в автоматизированных системах в организации

13.Виды организационно-распорядительных документов по защите информации в автоматизированных системах

14.Оценка способов установки и настройки средств защиты информации в автоматизированных системах в организации

15.Практические способы настройки средств защиты информации в автоматизированных системах

16.Практические способы установки средств защиты информации в автоматизированных системах

17.Оценка применяемых организационных мер и средств защиты информации при её обработке в автоматизированных системах в организации.

18.Методы оценки достаточности мероприятий по защите информации, обрабатываемой в автоматизированных системах.

19.Измеряемые физические величины специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации

20.Способы организации работы по выявлению угроз безопасности информации в автоматизированных системах

21.Способы применения организационных мер защиты информации при её обработке в автоматизированных системах

22.Способы применения средств защиты информации при её обработке в автоматизированных системах
23.Кадровое обеспечение функционирования мер по защите информации в автоматизированных системах
24.Инструментальный контроль защищенности речевой информации от утечки по каналу акустоэлектрического преобразования, формируемого методом высокочастотного навязывания
25.Методы контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок
26.Контроль защищенности средствами пассивной защиты информации от утечки за счет побочных электромагнитных излучений и наводок
27.Контроль защищенности средствами активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок
28.Контрольно-измерительная аппаратура специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации
29.Особенности поиска и идентификации сигналов специальными исследованиями на побочные электромагнитные излучения и наводки технических средств обработки информации
30.Порядок оценки угроз безопасности информации операционных систем
31.Инструментальный контроль защищенности речевой информации от утечки по каналу низкочастотного акустоэлектрического преобразования
32.Анализ угроз конфиденциальности информации программного обеспечения
33.Оценка угрозы безопасности информации в компьютерных сетях на этапе эксплуатации
34.Оценка угрозы безопасности информации в компьютерных сетях на этапе создания
35.Определение возможных объектов воздействия угроз безопасности информации операционных систем
36.Инструментальный контроль защищенности речевой информации от утечки по каналу высокочастотного акустоэлектрического преобразования
37.Анализ угроз целостности информации программного обеспечения
38.Оценка угроз безопасности информации с использованием экспертного метода
39.Технологическое и организационное построение мер по защите информации в автоматизированных системах

По результатам прохождения практики выставляется:

– оценка 5 («отлично») - Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений;

– оценка 4 («хорошо») - Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки;

– оценка 3 («удовлетворительно») - Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня;

– оценка 2 («неудовлетворительно») - Работа не выполнена или выполнена преимущественно неправильно.

В приложение к диплому выносится оценка за 6 семестр.

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ПРАКТИКИ

Производственная практика: технологическая практика

(название практики)

6 семестр

Перечень контрольных мероприятий текущего контроля успеваемости:

КМ-1 Получение задания на практику
КМ-2 Равномерность работы в течении практики
КМ-3 Выполнение задания на практику в полном объеме

Вид промежуточной аттестации – зачет с оценкой

Трудоемкость практики - 3 з.е.

Раздел дисциплины	Веса контрольных мероприятий, %			
	Индекс КМ:	КМ-1	КМ-2	КМ-3
	Срок КМ:	4	8	13
Текущий контроль прохождения практики		+	+	+
	Вес КМ:	10	30	60