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

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Управление инцидентами информационной безопасности

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Писаренко И.В. Идентификатор: R2828e375-PisarenkoIV-105ccd67	И.В. Писаренко
(должность)	(подпись)	(расшифровка подписи)

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
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(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. ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

2. ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

3. ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

4. ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Контрольная работа № 1 (Контрольная работа)
2. Контрольная работа № 2 (Контрольная работа)
3. Тест № 1 (Тестирование)
4. Тест № 2 (Тестирование)

БРС дисциплины

8 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Вводная лекция					
Предмет и задачи курса.		+	+		
Управление инцидентами информационной безопасности					

Тема 1. Общая характеристика инцидентов информационной безопасности			+	+
Тема 2. Основные способы и методы выявления инцидентов информационной безопасности			+	+
Тема 3. Управление инцидентами информационной безопасности.			+	+
Проведение расследований инцидентов информационной безопасности				
Тема 4. Расследование инцидентов информационной безопасности				+
Тема 5. Порядок действий при расследовании инцидентов информационной безопасности				+
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
ОПК-7	ОПК-7(Компетенция)	Знать: направления и перспективы дальнейшего совершенствования систем обеспечения безопасности хозяйствующих субъектов Уметь: определять виды и формы информации, подверженной угрозам, виды и возможные методы, и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	Тест № 1 (Тестирование) Контрольная работа № 1 (Контрольная работа)
ПК-4	ПК-4(Компетенция)	Уметь: выполнять работы по эксплуатации подсистем управления информационной безопасностью предприятия	Контрольная работа № 2 (Контрольная работа)

ПК-10	ПК-10(Компетенция)	Уметь: проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью	Контрольная работа № 2 (Контрольная работа)
ПК-12	ПК-12(Компетенция)	Уметь: проводить экспериментальные исследования системы защиты информации	Тест № 2 (Тестирование)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Тест № 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Тест состоит их 5 вопросов, на каждый может быть от 1 до 4 ответов. На проведение теста дается 15 минут.

Краткое содержание задания:
Дать ответ на заданные вопросы

Контрольные вопросы/задания:

Уметь: определять виды и формы информации, подверженной угрозам, виды и возможные методы, и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	1.*Какой закон устанавливает требования к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак?*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
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: 60
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: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-2. Контрольная работа № 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Дается письменное задание, по вариантам. Время работы - до 20 минут.

Краткое содержание задания:
Дать правильные ответы на заданные вопросы.

Контрольные вопросы/задания:

Знать: направления и перспективы дальнейшего совершенствования систем обеспечения безопасности хозяйствующих субъектов	1.*Система менеджмента инцидентами информационной безопасности.*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
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: 60
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: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-3. Тест № 2

Формы реализации: Письменная работа
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Тест состоит их 5 вопросов, на каждый может быть от 1 до 4 ответов. На проведение теста дается 15 минут.

Краткое содержание задания:
Дать ответ на заданные вопросы

Контрольные вопросы/задания:

Уметь: проводить экспериментальные исследования системы защиты информации	1.*Основные виды угроз информационной безопасности :…*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
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: 60
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: 50

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

КМ-4. Контрольная работа № 2

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Дается письменное задание, по вариантам. Время работы - до 20 минут.

Краткое содержание задания:
Дать правильные ответы на заданные вопросы.

Контрольные вопросы/задания:

Уметь: выполнять работы по эксплуатации подсистем управления информационной безопасностью предприятия	1.*Документация системы менеджмента инцидентов информационной безопасности.*
Уметь: проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью	1.*Расследование инцидентов информационной безопасности.*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
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: 60
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: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

<table>
<tr><td rowspan="4">М Э И</td><td colspan="2">ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № “Инженерно-экономический институт” МЭИ (ТУ)</td><td>Утверждаю

_____202_ г.</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td>Дисциплина</td><td colspan="2">Управление инцидентами информационной безопасности</td></tr>
<tr><td>Преподаватель</td><td colspan="2">К.т.н., доцент Писаренко И.В.</td></tr>
<tr><td colspan="4">1. Понятие инцидента информационной безопасности. Основные причины возникновения инцидентов информационной безопасности. Примеры инцидентов информационной безопасности.
2. Создание и деятельность группы реагирования на инциденты информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
3. Составить план расследования инцидента информационной безопасности по факту умышленного разглашения конфиденциальной информации (на основе собственного примера).</td></tr>
</table>

Процедура проведения

Экзамен проводится по билетам, в письменной форме. Время написания ответа - 20-25 минут.

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

1. Компетенция/Индикатор: ОПК-7(Компетенция)

Вопросы, задания

1. Основные предпосылки возникновения инцидентов ИБ. Краткий анализ основных предпосылок возникновения инцидентов ИБ.
2. Политика информационной безопасности организации. Основные положения политики информационной безопасности, порядок разработки и утверждения.
3. Концепция и структура построения системы управления инцидентами информационной безопасности.
4. Анализ и приоритезация инцидентов информационной безопасности.
5. Понятие мониторинга информационной безопасности. Виды и средства мониторинга информационной безопасности.
6. Аппаратно-программные средства мониторинга и аудита информационной безопасности.

Материалы для проверки остаточных знаний

1. Понятие менеджмента инцидентов ИБ. Этапы менеджмента инцидентов ИБ в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология.

Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

Ответы:

Ответ дается в письменном виде, возможны уточнения преподавателем.

Верный ответ: ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» в соответствии с процессной моделью Деминга (используемых в международных стандартах ИСО 9000 и ИСО 14000), выделяет четыре основных этапа менеджмента инцидентов ИБ (рис.1): Планирование и подготовка; Использование; Анализ; Улучшение. Целями такого подхода является обеспечение следующих условий: события ИБ должны быть обнаружены и эффективно обработаны, в частности, определены как относящиеся или не относящиеся к инцидентам ИБ; идентифицированные инциденты ИБ должны быть оценены, и реагирование на них должно быть осуществлено наиболее целесообразным и результативным способом; воздействия инцидентов ИБ на организацию и ее бизнес-операции необходимо минимизировать соответствующими защитными мерами, являющимися частью процесса реагирования на инцидент, иногда наряду с применением соответствующих элементов плана обеспечения непрерывности бизнеса; из инцидентов ИБ и их менеджмента необходимо быстро извлечь уроки. Это делается с целью повышения шансов предотвращения инцидентов ИБ в будущем, улучшения внедрения и использования защитных мер ИБ, улучшения общей системы менеджмента инцидентов ИБ.

2. Компетенция/Индикатор: ПК-4(Компетенция)

Вопросы, задания

1.Понятие инцидента ИБ. Основные причины возникновения инцидентов ИБ. Примеры инцидентов ИБ.

2.Основные стадии развития инцидентов ИБ (подготовка, развитие, скрытие следов).

3.Возможные последствия инцидентов ИБ. Понятие ущерба. Виды ущерба. Оценка ущерба.

4.Организация процесса управления инцидентами информационной безопасности в организации.

Материалы для проверки остаточных знаний

1.Документация системы менеджмента инцидентов ИБ. Политика менеджмента инцидентов ИБ.

Ответы:

Ответ дается в письменном виде, возможны уточнения преподавателем.

Верный ответ: Основные документом, регламентирующим организацию реагирования на инциденты, является Положение о менеджменте инцидентов ИБ, содержащее описание ролей по обработке инцидента. Кроме того, разрабатываются регламенты, конкретизирующие требования к отдельным процессам обработки инцидентов, например: регламент мониторинга событий и обнаружения инцидентов; регламент сбора информации и классификации инцидентов; регламент регистрации и оповещения об инцидентах; регламент реагирования на инциденты на различных уровнях; регламент проведения анализа инцидентов и функционирования процесса управления инцидентами; регламент внесения изменений в систему управления инцидентами на основе данных процесса управления инцидентами. Действия, описанные в регламентах, определяются значениями атрибутов записи о данном инциденте; одновременно в ходе обработки инцидента производится изменение значений определенных атрибутов записи согласно регламентам. Документация системы менеджмента инцидентов ИБ,

рекомендуемая ГОСТ Р ИСО/МЭК 18044, должна содержать следующие элементы: шкалу серьезности для классификации инцидентов ИБ; формы докладов о событиях и инцидентах ИБ (примеры форм приведены в приложении А ГОСТ 18044), соответствующие документированные процедуры и действия, связанные со ссылками на нормальные процедуры использования данных и системы, сервисов и(или) сетевого резервирования, планами обеспечения непрерывности бизнеса; операционные процедуры для ГРИИБ с документированными обязанностями и распределением функций среди назначенных ответственных лиц для осуществления различных видов деятельности.

3. Компетенция/Индикатор: ПК-10(Компетенция)

Вопросы, задания

1.Этап планирования и подготовки менеджмента инцидентов ИБ в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
2.Этап использования менеджмента инцидентов ИБ в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
3.Этап анализа менеджмента инцидентов ИБ в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
4.Этап улучшения менеджмента инцидентов ИБ в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
5.Особенности практического использования системы менеджмента инцидентов ИБ в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
6.Создание и деятельность группы реагирования на инциденты информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
7.Права и полномочия руководителя группы реагирования на инциденты информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
8.Документация системы менеджмента инцидентов ИБ. Политика менеджмента инцидентов ИБ.

Материалы для проверки остаточных знаний

1.Понятие расследования инцидента информационной безопасности. Решаемые задачи. Типовые ситуации, возникающие при расследовании инцидентов информационной безопасности.

Ответы:

Ответ дается в письменном виде, возможны уточнения преподавателем.

Верный ответ: Под расследованием (служебным расследованием) инцидента ИБ обычно понимают комплекс оперативных и технических мероприятий, направленных на выяснение причин инцидента ИБ, установление лиц, виновных в нем, всех обстоятельств и последствий, связанных с конкретным инцидентом ИБ. Расследование инцидента включает в себя определение виновных в его возникновении, сбор доказательств и улик инцидента, определение соответствующих дисциплинарных взысканий. В крупных компаниях, как правило,

выделяют комиссию по расследованию инцидентов ИБ (в состав которой может входить сотрудник, регистрирующий инциденты). Фаза расследования призвана определить: кто, что, когда, где, как и почему были вовлечены в инцидент. Расследование включает проверку и сбор доказательств с серверов, сетевых устройств, а также традиционные мероприятия нетехнического характера. Оно может быть разделено на два этапа: сбор данных и их криминалистический анализ. Информация, собранная в ходе выполнения первого этапа расследования, служит в дальнейшем для выработки стратегии реагирования на инцидент. На этапе анализа, собственно, и определяется, кто, что, как, когда, где и почему были вовлечены в инцидент. Расследование служебное — установление причин и лиц, виновных в разглашении или утечке информации, утрате документа, носителя или конфиденциальности информации, утраты продукции, содержащей ценные новшества, и других грубых нарушениях правил защиты информации. Проводится сотрудниками службы безопасности организации и предназначено для выяснения всех обстоятельств и их последствий, связанных с конкретным фактом. В ходе расследования устанавливаются причины случившегося и виновные лица. По результатам расследования делаются выводы о мере ответственности виновных лиц, даются рекомендации по устранению причин случившегося и исключению подобных фактов в будущем. При необходимости к расследованию привлекаются частные детективные агентства.

4. Компетенция/Индикатор: ПК-12(Компетенция)

Вопросы, задания

1.Классификация инцидентов ИБ.
2.Основные способы и методы выявления инцидентов информационной безопасности. Признаки инцидентов информационной безопасности.
3. Системы предотвращения утечек информации, DLP-системы.
4.Системы обнаружения вторжений (IDS).
5.Автоматизация процессов управления инцидентами. Системы управления инцидентами и событиями информационной безопасности.
6.Понятие менеджмента инцидентов ИБ. Этапы менеджмента инцидентов ИБ в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
7.Правовые основы проведения расследований инцидентов информационной безопасности. Законодательство РФ.
8.Кодекс об административных правонарушениях. Краткий анализ статей КоАП РФ, связанных с компьютерными правонарушениями.
9.Алгоритм действий при возникновении инцидентов информационной безопасности.
10.Основные этапы процесса реагирования на инцидент информационной безопасности.
11.Разработать план и оформить акт служебного расследования по факту нарушения договора о защищенном электронном документообороте (компрометация криптографических ключей)
12.Разработать план и оформить акт служебного расследования по факту нарушения антивирусной политики организации
13.Разработать план и оформить акт служебного расследования по факту действий пользователя, приведших к непреднамеренному уничтожению или модификации информации
14.Разработать план и оформить акт служебного расследования по факту рассылки СПАМа по локальной сети организации

Материалы для проверки остаточных знаний

1.Основные предпосылки возникновения инцидентов ИБ. Краткий анализ основных предпосылок возникновения инцидентов ИБ.

Ответы:

Ответ дается в письменном виде, возможны уточнения преподавателем.

Верный ответ: В целом все предпосылки можно объединить (достаточно условно) в две большие группы: организационно-правовые и технические. Среди организационно-правовых можно выделить следующие основные предпосылки: •отсутствие или слабая политика ИБ; •отсутствие или недостаточная квалификация специалистов по ИБ; •ошибки в подборе персонала (особенно связанного с обработкой КИ); •неправильно построенная деятельность службы ИБ; •беспечность ответственных работников; •недочеты в работе подразделения ИТ. К техническим предпосылкам можно отнести следующие: •ошибки в настройке технических средств защиты информации; •уязвимости ИС, обрабатывающих КИ; •бесконтрольное с точки зрения ИБ развитие ИС, внедрение новых способов обработки информации.

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 70

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: 60

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: 50

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

Итоговая оценка выставляется по итогам экзамена, с учетом оценки за курсовую работу и оценок по текущей успеваемости.