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: ЭТАЛОН: информационная безопасность

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. ПК-1 Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации

ПК-1.4 Выполняет аудит защищенности информации в автоматизированных системах

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Коллоквиум № 1 (Коллоквиум)
2. Коллоквиум № 2 (Коллоквиум)
3. Коллоквиум № 3 (Коллоквиум)
4. Контрольная работа № 1 (Контрольная работа)
5. Контрольная работа № 2 (Контрольная работа)
6. Тест № 1 (Тестирование)
7. Тест № 2 (Тестирование)

БРС дисциплины

8 семестр

Раздел дисциплины	Веса контрольных мероприятий, %							
	Индекс КМ:	КМ-1	КМ-1	КМ-2	КМ-2	КМ-3	КМ-4	КМ-4
	Срок КМ:	4	4	8	8	12	15	15
Введение								
Введение			+					
Управление инцидентами информационной безопасности								
Инциденты информационной безопасности		+	+		+	+		
Основные причины и предпосылки возникновения инцидентов информационной безопасности		+	+		+	+		
Правовые основы управления инцидентами информационной безопасности			+		+	+		
Основные способы и методы выявления инцидентов информационной безопасности		+	+		+	+		

Менеджмент инцидентов информационной безопасности	+	+		+	+		
Проведение расследований инцидентов информационной безопасности							
Правовые основы проведения расследований инцидентов информационной безопасности	+		+			+	+
Реагирование на инциденты информационной безопасности			+			+	+
Расследование инцидентов информационной безопасности.			+			+	+
Изъятие компьютерной техники и носителей информации			+			+	+
Проведение экспертиз при расследованиях компьютерных преступлений			+			+	+
Основы форензики (компьютерной криминалистики)			+			+	+
Вес КМ:	10	15	10	15	25	10	15

$Общая часть/Для промежуточной аттестации$

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	ПК-1.4$_{ПК-1}$ Выполняет аудит защищенности информации в автоматизированных системах	Знать: особенности управления инцидентами информационной безопасности применительно к различным сферам деятельности. основы управления инцидентами информационной безопасности на предприятии; требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины; Уметь: определять основные виды угроз информационной безопасности, возможные методы и пути реализации угроз; выявлять события и	Тест № 1 (Тестирование) Контрольная работа № 1 (Контрольная работа) Тест № 2 (Тестирование) Контрольная работа № 2 (Контрольная работа) Коллоквиум № 1 (Коллоквиум) Коллоквиум № 2 (Коллоквиум) Коллоквиум № 3 (Коллоквиум)

		реагировать на инциденты информационной безопасности; проводить расследования по инцидентам информационной безопасности; оформлять необходимые документы по расследованиям инцидентов информационной безопасности.	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольная работа № 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 10
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: основы управления инцидентами информационной безопасности на предприятии;	1.*Источники инцидентов информационной безопасности.*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны правильные ответы на все поставленные вопросы. Возможна одна небольшая неточность.

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Возможен один неправильный ответ, либо две небольшие неточности.

Оценка: 3
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Один полностью правильный ответ, либо неточности в каждом ответе.

КМ-1. Тест № 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 15
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:

Знать: требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины;	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: 90
Описание характеристики выполнения знания: Даны правильные ответы на все вопросы, возможна несущественная ошибка

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Возможен неправильный ответ на 1-2 вопроса

Оценка: 3
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Возможен неправильный ответ на 3 вопроса

КМ-2. Контрольная работа № 2

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 10
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: особенности управления инцидентами информационной безопасности применительно к различным сферам деятельности.	1.*Основные этапы реагирования на инцидент информационной безопасности.*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны правильные ответы на все поставленные вопросы. Возможна одна небольшая неточность.

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Возможен один неправильный ответ, либо две небольшие неточности.

Оценка: 3
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Один полностью правильный ответ, либо неточности в каждом ответе.

КМ-2. Тест № 2

Формы реализации: Письменная работа
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 15

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 основные виды угроз информационной безопасности, возможные методы и пути реализации угроз;	1.*Основные виды угроз информационной безопасности :…*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны правильные ответы на все вопросы, возможна несущественная ошибка

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Возможен неправильный ответ на 1-2 вопроса

Оценка: 3
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Возможен неправильный ответ на 3 вопроса

КМ-3. Коллоквиум № 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Выполняется практическое задание, по рекомендациям преподавателя

Краткое содержание задания:
Преподаватель выдает практическое задание (кейс) по заданной теме

Контрольные вопросы/задания:

Уметь: выявлять события и реагировать на инциденты информационной безопасности;	1.*определить возможные угрозы информационной безопасности и пути их реализации применительно к различным организациям.*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Задание полностью и правильно выполнено, возможны небольшие неточности (1-2)

Оценка: 4
Нижний порог выполнения задания в процентах: 75
Описание характеристики выполнения знания: Задание в основном выполнено, возможны одна существенная ошибка или несколько неточностей.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Задание выполнено частично, возможны 2-3 ошибки.

КМ-4. Коллоквиум № 3

Формы реализации: Письменная работа
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Выполняется практическое задание, по рекомендациям преподавателя

Краткое содержание задания:
Преподаватель выдает практическое задание (кейс) по заданной теме

Контрольные вопросы/задания:

Уметь: оформлять необходимые документы по расследованиям инцидентов информационной безопасности.	1.*разработать план проведения расследования по выявленному инциденту информационной безопасности;*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Задание полностью и правильно выполнено, возможны небольшие неточности (1-2)

Оценка: 4
Нижний порог выполнения задания в процентах: 75
Описание характеристики выполнения знания: Задание в основном выполнено, возможны одна существенная ошибка или несколько неточностей.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Задание выполнено частично, возможны 2-3 ошибки.

КМ-4. Коллоквиум № 2

Формы реализации: Письменная работа
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: Выполняется практическое задание, по рекомендациям преподавателя

Краткое содержание задания:
Преподаватель выдает практическое задание (кейс) по заданной теме

Контрольные вопросы/задания:

Уметь: проводить расследования по инцидентам информационной безопасности;	1.*разработать план проведения расследования инцидента информационной безопасности;*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Задание полностью и правильно выполнено, возможны небольшие неточности (1-2)

Оценка: 4
Нижний порог выполнения задания в процентах: 75
Описание характеристики выполнения знания: Задание в основном выполнено, возможны одна существенная ошибка или несколько неточностей.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Задание выполнено частично, возможны 2-3 ошибки.

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>1</td><td>Утверждаю
_____2021 г.</td></tr>
<tr><td colspan="2">Дисциплина</td><td colspan="2">Управление инцидентами информационной безопасности</td></tr>
<tr><td colspan="2">Преподаватель</td><td colspan="2">К.т.н., доцент Писаренко И.В.</td></tr>
<tr><td colspan="5">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: ПК-1.4$_{ПК-1}$ Выполняет аудит защищенности информации в автоматизированных системах

Вопросы, задания

1.Понятие инцидента ИБ. Основные причины возникновения инцидентов ИБ. Примеры инцидентов ИБ.
2.Классификация инцидентов ИБ.
3.Основные стадии развития инцидентов ИБ (подготовка, развитие, скрытие следов).
4.Возможные последствия инцидентов ИБ. Понятие ущерба. Виды ущерба. Оценка ущерба.
5. Основные предпосылки возникновения инцидентов ИБ. Краткий анализ основных предпосылок возникновения инцидентов ИБ.
6.Политика информационной безопасности организации. Основные положения политики информационной безопасности, порядок разработки и утверждения.
7.Основные способы и методы выявления инцидентов информационной безопасности. Признаки инцидентов информационной безопасности.
8. Концепция и структура построения системы управления инцидентами информационной безопасности.

9. Анализ и приоритезация инцидентов информационной безопасности.
10.Понятие мониторинга информационной безопасности. Виды и средства мониторинга информационной безопасности.
11.Аппаратно-программные средства мониторинга и аудита информационной безопасности.
12. Системы предотвращения утечек информации, DLP-системы.
13.Системы обнаружения вторжений (IDS).
14.Автоматизация процессов управления инцидентами. Системы управления инцидентами и событиями информационной безопасности.
15.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».
16.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».
17.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».
18.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».
19.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».
20.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».
21.Организация процесса управления инцидентами информационной безопасности в организации.
22.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».
23.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».
24.Документация системы менеджмента инцидентов ИБ. Политика менеджмента инцидентов ИБ.
25.Программа менеджмента инцидентов ИБ. Особенности ее внедрения и реализации.
26.Правовые основы проведения расследований инцидентов информационной безопасности. Законодательство РФ.
27. Уголовный кодекс Российской Федерации. Краткий анализ статей УК РФ, связанных с компьютерными преступлениями.
28.Кодекс об административных правонарушениях. Краткий анализ статей КоАП РФ, связанных с компьютерными правонарушениями.
29.Особенности применения Трудового кодекса Российской Федерации при проведении расследований инцидентов информационной безопасности.
30.Государственные органы РФ, проводящие расследования. Порядок взаимодействия с правоохранительными органами.

31.Негосударственные организации, занимающиеся расследованием инцидентов ИБ на территории РФ, и их возможности.
32.Алгоритм действий при возникновении инцидентов информационной безопасности.
33.Основные этапы процесса реагирования на инцидент информационной безопасности.
34.Понятие расследования инцидента информационной безопасности. Решаемые задачи. Типовые ситуации, возникающие при расследовании инцидентов информационной безопасности.
35.Проведение расследований инцидентов информационной безопасности. Примерный алгоритм проведения расследования инцидента информационной безопасности.
36. Процедура ликвидации последствий инцидента информационной безопасности.
37.Документирование инцидента информационной безопасности.
38.Правовые основы для изъятия и исследования компьютерной техники. Основные ошибки, встречающиеся при изъятии имущества в ходе расследования инцидента ИБ.
39.Методика изъятия компьютерной техники и носителей информации. Обеспечение доказательственного значения изъятых материалов. Описание и пломбирование техники.
40.Методика исследования компьютерной техники. Общие принципы исследования техники. Техническое обеспечение исследования. Выводы эксперта и экспертное заключение.
41.Разработать план и оформить акт служебного расследования по факту разглашения конфиденциальной информации
42.Разработать план и оформить акт служебного расследования по факту утраты съемного носителя информации с конфиденциальной информацией
43.Разработать план и оформить акт служебного расследования по факту кражи ноутбука с конфиденциальной информацией
44.Разработать план и оформить акт служебного расследования по факту несанкционированного копирования конфиденциальной информации на съемный носитель
45.Разработать план и оформить акт служебного расследования по факту несанкционированной распечатки конфиденциальной информации
46.Разработать план и оформить акт служебного расследования по факту пересылки конфиденциальной информации на внешний адрес сети Интернет
47.Разработать план и оформить акт служебного расследования по факту нарушения договора о защищенном электронном документообороте (компрометация криптографических ключей)
48.Разработать план и оформить акт служебного расследования по факту нарушения антивирусной политики организации
49.Разработать план и оформить акт служебного расследования по факту действий пользователя, приведших к непреднамеренному уничтожению или модификации информации
50.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.

2.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.

3.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.

4.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.

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны полные и правильные ответы на поставленные вопросы. Возможна одна небольшая неточность.

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Даны в целом правильные ответы, возможна одна ошибка, либо две-три небольшие неточности.

Оценка: 3
Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Дан правильный ответ на один вопрос, либо имеются ошибки в обеих ответах на вопросы.

III. Правила выставления итоговой оценки по курсу

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