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
Технологии компьютерного аудита

Москва
2024

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

СОГЛАСОВАНО:

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

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-3 Способностью администрировать подсистемы информационной безопасности объекта защиты

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

3. ПСК-1 Способность администрировать подсистемы информационной безопасности объектов, объекты энергетики КВО РФ, эксплуатирующие АСУ ТП

и включает:

для текущего контроля успеваемости:

Форма реализации: Проверка задания

1. КМ-1 (Семинар)
2. КМ-2 (Семинар)
3. КМ-3 (Семинар)
4. КМ-4 (Семинар)
5. КМ-5 (Семинар)

БРС дисциплины

8 семестр

Раздел дисциплины	Веса контрольных мероприятий, %					
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5
	Срок КМ:	4	6	8	12	15
Теоретические основы компьютерного аудита безопасности информационных систем						
Теоретические основы компьютерного аудита безопасности информационных систем		+	+	+		
Технологии компьютерного аудита						
Технологии компьютерного аудита				+	+	+
	Вес КМ:	10	20	20	20	30

$Общая часть/Для промежуточной аттестации$

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-3	ПК-3(Компетенция)	Знать: перечень и содержание информации аудита, получаемой из программных приложений перечень и возможности программных приложений по выполнению основных функций аудита, включая open source решения Уметь: применять результаты анализа информации аудита для принятия управленческих решений в информационной системе организации выполнять перечень операций по работе с программными приложениями, выполняющими функции аудита, включая open source решения	КМ-3 (Семинар) КМ-4 (Семинар) КМ-5 (Семинар)
ПК-10	ПК-10(Компетенция)	Знать:	КМ-1 (Семинар)

		перечень и содержание требований руководящих документов к аудиту некоторых информационных систем: ИСПДН, КИИ, ГИС перечень и содержание стандартов серии ГОСТ Р ИСО/МЭК 27000 в области аудита информационной безопасности Уметь: разработать и корректировать план выполнения требований руководящих документов по обеспечению безопасности информационных систем на основе данных аудита разработать и реализовать план проведения аудита информационной системы организации	КМ-5 (Семинар)
ПСК-1	ПСК-1(Компетенция)	Знать: возможности компьютерного аудита, встроенные в операционные системы, базы данных и другие программные приложения основы аудита безопасности	КМ-1 (Семинар) КМ-2 (Семинар) КМ-3 (Семинар)

		информационных систем, включая отраслевые системы (объекты энергетики, относящиеся к КВО РФ) Уметь: настраивать приложения аудита, встроенные в операционные системы, базы данных и другие программные комплексы проводить анализ сведений аудита, получаемых из программных приложений, включая и используемые в отраслевых системах (объекты энергетики, относящиеся к КВО РФ)	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. КМ-1

Формы реализации: Проверка задания
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Задания 1,2 для индивидуального выполнения Условия проведения Учебная группа: 1 человек. Используемые технические и программные средства: Компьютер с ОС Linux, Windows. Встроенное программное обеспечение

Краткое содержание задания:

Задание 1.1.
1). Определить текущую конфигурацию оборудования компьютера (используемый CPU, количество ядер, ОЗУ и т.д.).
2). Определить текущую нагрузку на ОС.
3). Определить установленную ОС и архитектуру.
4). Определить какие процессы потребляют больше всего ресурсов. Можно ли оптимизировать потребление системных ресурсов данными процессами?

Задание 1.2.
1). Определить IP-адрес, маску, шлюз и используемые DNS сервера.
2). Определить MAC-адрес сетевой карты.
3). Определить внешний IP-адрес компьютера.
4). Определить количество сетевых адаптеров и их предназначение.

Задание 1.3.
1). Определить MAC адрес шлюза по умолчанию.
2). Определить совпадает ли ответ вашего DNS сервера с ответом DNS сервера 77.88.8.3.
3). Определить доступность узла 8.8.8.8 с вашего компьютера.
4). Определить маршрут до узла 8.8.8.8.
5). Определить какие порты открыты на вашем компьютеры и какими процессами. Результат сохранить в файл.

Задание 1.4.
1). Определить используется ли антивирусное программное обеспечение.
2). Определить используется ли межсетевой экран.
3). Определить уровень UAC (для Windows).

Задание 2.1.
1). Ознакомиться с функционалом приложения Просмотр событий
2). Создать предустановленный фильтр для фильтрации ошибок и предупреждений из журнала приложений и системы
3). Проанализировать полученный результат.
4). Сохранить полученный результат в файл

Задание 2.2.
1). Настроить аудит Windows на успешные попытки входа в систему и на отказ входа в систему.

2). Настроить аудит на назначение пароля длиной менее 5 символов.
3). Создать предустановленные фильтры для настроенных событий аудита.
4). Проверить работоспособность созданных политик аудита Для настройки аудита использовать редактор локальных групповых политик. Win+R и ввести gpedit.msc.

Задание 2.3.
1). Настроить политики аудита на попытку доступа к директории.
2). Создать двух пользователей. Ограничить доступ к директории для второго пользователя. Первому дать максимальные права.
3). Проверить работоспособность созданных политик аудита. Создать предустановленный фильтр для настроенных политик аудита. Сохранить результаты в файл.

Задание 2.4.
1). Настроить мониторинг использования съемных носителей. При фиксации такого события оповещать пользователя с помощью отправки e-mail или запуском программы (скрипта) о том, что произошло событие.
2). Можно ли настроить отслеживание открытия портов приложениями или службами Windows?
3). Какие возможности аудита существует для отслеживания поведения приложений, служб в ОС Windows? (продемонстрировать)

Контрольные вопросы/задания:

Знать: перечень и содержание стандартов серии ГОСТ Р ИСО/МЭК 27000 в области аудита информационной безопасности	1.Назовите перечень стандартов серии ГОСТ Р ИСО/МЭК 27000+
Знать: перечень и содержание требований руководящих документов к аудиту некоторых информационных систем: ИСПДН, КИИ, ГИС	1.Изложите основное содержание стандарта серии ГОСТ Р ИСО/МЭК 27002 2.Изложите основное содержание стандарта серии ГОСТ Р ИСО/МЭК 27005
Уметь: настраивать приложения аудита, встроенные в операционные системы, базы данных и другие программные комплексы	1.Определите конфигурацию рабочего места для проведения компьютерного аудита. 2.Разъясните, как настраивать приложения аудита

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

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-2. КМ-2

Формы реализации: Проверка задания
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Задания 3 для индивидуального выполнения Условия проведения Учебная группа: 1 человек. Используемые технические и программные средства: Компьютер с ОС Linux, Windows. Встроенное программное обеспечение

Краткое содержание задания:

Задание 3.1.
Необходимо получить контактную информацию и адрес расположения основного офиса:
Ресурсы для исследования:
https://www.booking.com/index.ru.html
https://www.facebook.com/
https://lenta.ru/
https://www.ozon.ru/
https://magnit.ru/
https://www.croc.ru/
https://mail.ru/
https://www.tadviser.ru/
https://www.lada.ru/
https://aliexpress.ru/

Задание 3.2.
1). Выяснить кто глава компании. Его контактные данные. Страницы в социальных сетях.
2). Определить структуру организации.
3). Проверить компанию по ИНН. Выяснить размер уставного капитала, учредителей, основной вид деятельности, участие в судебных делах. (https://kontur.ru/compass/spravka-compass/606-bankrotstvo).
4). Проверить компанию на банкротство (https://kontur.ru/articles/401).
5). Оценить благонадежность компании (https://www.nalog.ru/rn72/news/tax_doc_news/5404050/).

Задание 3.3.
1). Определить используемый веб-сервер и версию. Возможная ОС.
2). Определить используемые IP-адреса веб-сервером. В какой стране расположен веб-сервер?
3). Определить используется ли CMS. Если используется, то какая.
4). Какие страницы запрещены для индексации? Возможная причина.
5). На кого зарегистрировано доменное имя? контактная информация владельца.
6). Кто является хостинг провайдером?

Задание 3.4.

1). Сколько страниц проиндексировано в поисковой системе Google?
2). Основной источник трафика?
3). География аудитории.
4). Какие поддомены зарегистрированы? Возможное предназначение.
5). Размещены ли в общем доступе конфиденциальные документы?
6). Содержаться ли в индексе поисковых систем файлы с паролем?
7). Сделать вывод о целевой аудитории.
8). Определить служебные страницы для управления контентом сайта (страница доступа к СУБД, страница входа для администрирования и т.д.).

Задание 3.5.
1). Проанализировать полученную информацию.
2). Определить какие уязвимости могут присутствовать на исследуемом ресурсе.

Контрольные вопросы/задания:

Знать: возможности компьютерного аудита, встроенные в операционные системы, базы данных и другие программные приложения	1.Каковы возможности компьютерного аудита для операционных систем? 2.Каковы возможности компьютерного аудита для баз данных?
Уметь: проводить анализ сведений аудита, получаемых из программных приложений, включая и используемые в отраслевых системах (объекты энергетики, относящиеся к КВО РФ)	1.Как проводить анализ сведений аудита, получаемых из программных приложений? 2.Как проводить анализ сведений аудита, получаемых из программных приложений объектов энергетики?

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

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-3. КМ-3

Формы реализации: Проверка задания
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 20

Процедура проведения контрольного мероприятия: Задания 4 для индивидуального выполнения Условия проведения Учебная группа: 1 человек. Используемые технические и программные средства: Компьютер с ОС Linux, Windows. Встроенное программное обеспечение

Краткое содержание задания:

Задание 4.1.

Для работы необходимо установить 2 виртуальные машины:

1) PC1 - машина с ОС Windows или Linux с GUI и установленным ПО Zenmap (https://nmap.org/zenmap/).

2) IPS - виртуальная машина с 2 сетевыми адаптерами и с установленной системой pfsense (https://www.pfsense.org/download/) или opnsense (https://opnsense.org/download/).

Задание 4.2.

1). Необходимо сконфигурировать сетевые интерфейсы на виртуальной машине с IPS: https://itarticle.ru/console-setup-pfsense-opnsense/ и на виртуальной машине PC1.

2). Для упрощения настройки сетевого адаптера на виртуальной машины PC1 можно активировать DHCP-сервер на виртуальной машине IPS на LAN интерфейсе.

3). Для наглядности рекомендуется использовать адресацию внутренней сети 10.10.x.x/24.

Задание 4.3.

1). Установить пакет Snort или Suricata для добавления функционала IPS (система - установка пакетов).

Задание 4.4.

1). Настроить правила для обнаружения сканирования nmap для WAN интерфейса.

2). Произвести сканирование и продемонстрировать результаты обнаружения сканирования системой предотвращения вторжений.

Задание 4.5.

1. Настроить блокировку трафика в случае обнаружения сканирования.

Контрольные вопросы/задания:

Знать: основы аудита безопасности информационных систем, включая отраслевые системы (объекты энергетики, относящиеся к КВО РФ)	1.Перечислите основы аудита безопасности информационных систем 2.Перечислите основы аудита безопасности отраслевых информационных систем объектов энергетики
Уметь: выполнять перечень операций по работе с программными приложениями, выполняющими функции аудита, включая open source решения	1.Какие операций следует выполнить в работе с представленным программным приложением, включающим open source решения и выполняющим функции аудита? 2.Какие операций следует выполнить в работе с представленным программным приложением, выполняющим функции аудита?

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

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-4. КМ-4

Формы реализации: Проверка задания
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Задания 5, 6 для индивидуального выполнения Условия проведения Учебная группа: 1 человек. Используемые технические и программные средства: Компьютер с ОС Linux, Windows. Встроенное программное обеспечение Docker, docker-compose, Elasticsearch, Logstash, Kibana, Filebeat

Краткое содержание задания:
Задание 5.1.
Развернуть ELK с помощью docker-compose. Проверить доступность всех сервисов.

Задание 5.2.
1) На виртуальной машине установить: *filebeat*
2) Далее необходимо настроить конфигурацию *filebeat.yml*, для чего указать IP-адрес для Elasticsearch, в типе аутентификации указывать логин и пароль.
3) После настройки отправки журналов событий в Kibana в режиме реального времени можно наблюдать события, которые приходят от filebeat.

Задание 5.3.
1) Для визуализации журналов событий можно выбрать готовый Dashboard или создать новый. Выбор или настройка на вкладке Dashboard.
2) После выбора соответствующей вкладки выбрать предустановленный Dashboard: [Filebeat System] Syslog dashboard ECS.
3) Акцентировать внимание на возможных ошибках при настройке и определить вариант решения.

Задание 6.1.
. Смоделировать атаку на ssh-сервер.
1) Использовать утилит *Ncrack*. Вместо «*ncrack*» возможно использовать любые подобные утилиты.
2) Установить утилит *Ncrack* на компьютер, с которого есть возможность провести атаку на подготовленный стенд. Запуск утилиты происходит из командной строки.
3) Запустить командную строку в папке установки утилиты и выполняем следующую команду.
3) Войти в систему используя полученный логин и пароль. После успешного входа в систему необходимо перейти в режим суперпользователя (*root*) и произвести добавление нового пользователя в систему.

Задание 6.2.
1) В Kibana необходимо создать или выбрать готовый *Dashboard* ([Filebeat System] New users and groups ECS) для анализа системных журналов событий.
2) Для определения попыток входа *SSH* используется предустановленный *Dashboard* ([Filebeat System] SSH login attempts ECS). Несанкционированные попытки входа можно достаточно просто определить по диаграмме *SSHlogin attempts* [Filebeat System] ECS, на которой все попытки разделены на категории Accepted, Failed, Invalid, error.
3) По диаграмме необходимо определить время начала и окончания атаки; несанкционированные попытки входа определить по диаграмме *SSHlogin attempts* [Filebeat System] ECS, на которой все попытки разделены на категории Accepted, Failed, Invalid, error.
4) необходимо добавить фильтр по времени для текущего *Dashborad*, для этого нажимаем на Add filter и указываем значения даты и времени.
5) Определить успешные попытки входа, для чего ввести в строке поиска запрос: *system.auth.ssh.event :"Accepted"*.
6) По полю *source.ip* определить ip-адрес машины, с которой был произведен вход.
7) Изменить запрос поиска на следующий:
source.ip : "ip_адрес_машины_с_успешным_входом"
8) В случае, если с этого ip-адреса было много запросов Failed и Invalid, необходимо определить какие действия совершил злоумышленник после входа в систему.

Задание 6.3.
1) Определить имя пользователя, под которым был совершен вход.
2) Какие действия были совершены после входа в систему.

Контрольные вопросы/задания:

Знать: перечень и возможности программных приложений по выполнению основных функций аудита, включая open source решения	1.Перечислите перечень программных приложений по выполнению основных функций аудита, включая open source решения 2.Дайте анализ возможностей программных приложений по выполнению основных функций аудита, включая open source решения
Уметь: применять результаты анализа информации аудита для принятия управленческих решений в информационной системе организации	1.Как применить результаты анализа информации аудита для принятия управленческих решений в информационной системе предложенной организации? 2.Предложите алгоритм анализа информации аудита для принятия управленческих решений в информационной системе организации

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

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-5. КМ-5

Формы реализации: Проверка задания
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Задания 7, 8 для индивидуального выполнения Условия проведения Учебная группа: 1 человек. Используемые технические и программные средства: Компьютер с ОС Linux, Windows. Встроенное программное обеспечение Docker, docker-compose, Elasticsearch, Logstash, Kibana, Filebeat

Краткое содержание задания:
Задание 7.1.
Для выполнения работы с помощью виртуальной машины необходимо:
1) Получить у преподавателя виртуальную машину с настроенными сервисами.
2) Иметь настроенный ELK.
3) Получить набор скриптов для выполнения атак.
4) Скачать live-образ *kali linux* (https://www.kali.org/downloads/) и запустить его на виртуальной машине.
5) Настроить подключение полученной виртуальной машины к ELK.
При выполнении работы на подготовленном стенде необходимо:
1) Получить учетные данные для подключения к стенду
2) Запустить атаки (запуск атак может запускаться преподавателем или в автоматическом режиме по расписанию)
Для отправки и анализа логов будут использоваться:
1) *Auditbeat* - позволяет анализировать действия пользователей и процессов в системе. (https://www.elastic.co/guide/en/beats/auditbeat/7.6/auditbeat-overview.html)
Для настройки подключения (только в случае использования подготовленной виртуальной машины) необходимо отредактировать файл */etc/auditbeat/auditbeat.yml* и указать параметры подключения к ELK.

Задание 7.2.
используя виртуальную машину на *kali linux* необходимо произвести атаки на виртуальную машину (в случае использования стенда, атакует преподаватель или атак происходит по расписанию).
Рекомендуемые этапы при выполнении задания:
а) Открыть раздел SIEM и/или открыть предустановленный *Dashboard.*
б) Запустить скрипт для атаки: *bash attackN.sh.*
в) Проанализировать какие изменения происходят в системе при атаке.
г) Описать по каким признакам можно понять, что происходит атака.
д) Выбрать/создать *Dashboard* оптимальный для определения атак данного типа.
е) Определить какая атака была произведена.

Задание 7.3.

1) Необходимо создать рациональный *Dashboard*, который бы позволил определять начало атаки, имел возможность оперативно переключаться для более детального определения типа атаки.

Задание 8.1.
1). Установить zabbix на виртуальную машину.
Предлагается установка zabbix с помощью импорта ovf образа в VirtualBox
https://cdn.zabbix.com/zabbix/appliances/stable/5.2/5.2.6/zabbix_appliance-5.2.6-ovf.tar.gz
2). На другой машине установить агент заббикса. И добавить узел сети в систему мониторинга
https://www.zabbix.com/ru/download_agents
3). Убедиться, что данные приходят в заббикс.

Задание 8.2.
1). Настроить автоматическую инвентаризацию узла.
Название процессора - wmi.get[root\cimv2,select name from Win32_Processor].
Архитектура ОС - wmi.get[root\cimv2,select OSArchitecture from Win32_OperatingSystem].
Версия ОС - wmi.get[root\cimv2,select version from Win32_OperatingSystem].
Полное название ОС - wmi.get[root\cimv2,select name from Win32_OperatingSystem].
2). Настроить отправку логов. Рекомендуется настраивать отправку логов с Linux машины. Например, с сервера zabbix.
3). Настроить триггер.

Контрольные вопросы/задания:

Знать: перечень и содержание информации аудита, получаемой из программных приложений	1.Перечислите перечень информации аудита, получаемой из программных приложений 2.Перечислите содержание информации аудита, получаемой из программных приложений
Уметь: разработать и корректировать план выполнения требований руководящих документов по обеспечению безопасности информационных систем на основе данных аудита	1.Предложите общий план проведения аудита информационной системы предложенной организации
Уметь: разработать и реализовать план проведения аудита информационной системы организации	1.Предложите коррекцию плана выполнения требований руководящих документов по обеспечению безопасности информационных систем на основе данных аудита предложенной организации

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

Оценка: 2

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

НИУ МЭИ	**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1** Кафедра *Безопасности и информационных технологий* Дисциплина «Основы управления информационной безопасностью»	*Утверждаю:* *Зав. каф. БИТ* *А.Ю.Невский* Протокол № от 20__ года
1. Методы тестирования penetrationtesting (PT). 2. Аудит безопасности информационных активов организации. Доцент, к.т.н. А.Ю.Невский		

Процедура проведения

Экзамен проводится в устной форме по билетам согласно программе экзамена

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

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

Вопросы, задания

1.Этапы проведения компьютерного аудита.
2.Этапы работы технического эксперта по компьютерному аудиту.
3.Подсистемы аудита событий ОС Windows
4.Что сохраняется в журналах событий?
5.В каком направлении развиваются современные ОС?
6.Как обеспечить доверие к рассмотренным механизмам безопасности ОС?
7.Почему нельзя строить ответственные информационные системы на зарубежных ОС?
8.Предложить способ наиболее полного сбора открытой информации на человека, претендующего на вакансию.
9.С какой целью ведется сбор открытой информации об объекте аудита?
10.Как обнаружить информацию о конфигурационных файлах в открытых web-приложениях?
11.Как используются социальные сети для сбора информации о претенденте на вакансию?
12.Проведение экспресс-тестов по оценке эффективности защиты информации в ИС.
13.Анализ защищенности по ГОСТ Р ИСО/МЭК 27001.
14.Оценка эффективности защиты веб-приложений.
15.Технологии выполнения тестирования на проникновение.

Материалы для проверки остаточных знаний

1.Чем не обеспечивается безопасность при использовании мобильных программ?
Ответы:
а логически изолированной средой;

b блокированием любого несанкционированного использования мобильной программы;
c не блокированием приема мобильной программы;
d обеспечением уверенности в отсутствии мобильной программы;
e контроле ресурсов доступных мобильной программе;
f применением криптографических мер и средств контроля и управления для однозначной аутентификации мобильной программы.

Верный ответ: cd

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

Вопросы, задания

1.Методы тестирования penetrationtesting (PT).
2.Что такое идентификаторы безопасности SID (SecureIdentifier)?
3.Примеры SID безопасности.
4.Как узнать значение SID конкретного пользователя?
5.Схема шифрования EFS в ОС Windows
6.Методы получения информации из открытых источников.
7.Технологии компьютерного аудита на основе SIEM.

Материалы для проверки остаточных знаний

1.С какой целью проводится управление производительностью информационных систем?

Ответы:

a прогнозирования производительности оборудования исходя будущих целей обработки информации
b оптимизация производительности информационных систем
c разработки требований к производительности оборудования по обработки информации

Верный ответ: ac

3. Компетенция/Индикатор: ПСК-1(Компетенция)

Вопросы, задания

1.Понятие Компьютерный аудит и методы его проведения.
2.Модели аудита.
3.Кто проводит аудит?
4.Цели, программа и план аудита.
5.Принципы аудита.
6.Виды аудита и формы его проведения.
7.Формальное описание системы в модели Харрисона-Руззо-Ульмана.
8.Модель целостности Кларка-Вилсона. Достоинства и недостатки модели целостности Кларка-Вильсона.
9.Модель безопасности ОС Windows. Подсистемы Windows, обеспечивающие безопасность.
10.Предложить способ выявления возможных инсайдеров при приеме сотрудников по открытым вакансиям в организацию.
11.Аудит физического контроля доступа в помещения.
12.Аудит безопасности информационных активов организации.
13.Аудит организационного обеспечения.
14.Аудит соответствия нормативному обеспечению.
15.Аудит безопасности IT-структуры.
16.Анализ возможностей применения технологий социальной инженерии.
17.Анализ эффективности защиты от вредоносного кода.
18.Анализ получения информации от сетевых сервисов.

19.Оценка защищенности беспроводных сетей.
20.Анализ возможностей обхода систем безопасности.

Материалы для проверки остаточных знаний

1.Решение каких вопросов включает резервирование?

Ответы:

a необходимо определить количество копий, формы их хранения и обновления;
b шифрование копий;
c тестирование копий;
d обеспечение физической защиты;
t централизованное хранение;
f объем (т.е. полное или выборочное резервирование) и частота резервирования должны отражать требования бизнеса организации, требования к безопасности затрагиваемой информации и критичность информации для непрерывной работы организации;
g аудит резервных копий

Верный ответ: abcdf

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

Оценка: 2
Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

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 зачетной / экзаменационной составляющих.