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 (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Технологии компьютерного аудита

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-3 Способен администрировать средства защиты информации в компьютерных системах и сетях

ПК-3.1 Администрирует подсистемы защиты информации в операционных системах

ПК-3.3 Администрирует средства защиты информации прикладного и системного программного обеспечения

и включает:

для текущего контроля успеваемости:

Форма реализации: Проверка задания

1. Задание 1; Задание 2 (Отчет)
2. Задание 3; Задание 4 (Отчет)
3. Задание 5; Задание 6 (Отчет)
4. Задание 7; Задание 8 (Отчет)

БРС дисциплины

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Раздел 1					
Тема 1. Введение в дисциплину. Основные термины и определения		+			
Тема 2. Нормативно-правовые требования по аудиту информационной безопасности. Виды аудита		+			
Раздел 2					
Тема 3. Этапы проведения аудита и используемые технологии			+		
Тема 4. Аудит информационных технологий с использованием сканеров безопасности			+		
Тема 5. Аудит событий на объекте исследования				+	+
	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
ПК-3	ПК-3.1$_{ПК-3}$ Администрирует подсистемы защиты информации в операционных системах	Знать: нормативно-правовые требования по проведению компьютерного аудита цели, принципы и методы проведения компьютерного аудита источники информации о защищенности компьютера технологии, применяемые при проведении компьютерного аудита этапы проведения аудита Уметь: определить конфигурацию рабочего места для проведения компьютерного аудита собрать (добыть) информацию об исследуемом объекте использовать технологии для оценки защищенности объекта исследования	Задание 1; Задание 2 (Отчет) Задание 3; Задание 4 (Отчет) Задание 5; Задание 6 (Отчет) Задание 7; Задание 8 (Отчет)
ПК-3	ПК-3.3$_{ПК-3}$	Знать:	Задание 3; Задание 4 (Отчет)

	Администрирует средства защиты информации прикладного и системного программного обеспечения	назначение, принципы работы и технология анализа событий в исследуемом объекте основные технологии тестирования объекта исследования Уметь: развертывать и использовать ИТ для анализа событий на объекте исследования SIEM (ELK) применять сканеры безопасности для оценки защищенности объекта исследования	Задание 5; Задание 6 (Отчет) Задание 7; Задание 8 (Отчет)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Задание 1; Задание 2

Формы реализации: Проверка задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
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: источники информации о защищенности компьютера	1.Укажите нормативно-правовые требования по проведению компьютерного аудита. 2.Назовите цели, принципы и методы проведения компьютерного аудита.
Знать: этапы проведения аудита	1.Перечислите этапы проведения аудита.
Уметь: использовать технологии для оценки защищенности объекта исследования	1.Определите конфигурацию рабочего места для проведения компьютерного аудита. 2.Разъясните, как собрать (добыть) информацию об исследуемом объекте.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
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: 70
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. Задание 3; Задание 4

Формы реализации: Проверка задания
Тип контрольного мероприятия: Отчет

Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Задания 3, 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 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.

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: нормативно-правовые требования по проведению компьютерного аудита	1.Охарактеризовать источники информации о защищенности компьютера.
Знать: назначение, принципы работы и технология анализа событий в исследуемом объекте	1.Дать характеристику технологиям, применяемые при проведении компьютерного аудита. 2.Назвать и охарактеризовать основные технологии тестирования объекта исследования.
Уметь: определить конфигурацию рабочего места для проведения компьютерного аудита	1.Разъяснить порядок и способы использования технологий для оценки защищенности объекта исследования.
Уметь: собрать (добыть) информацию об исследуемом объекте	1.Охарактеризовать применение сканеров безопасности для оценки защищенности объекта исследования.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
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: 70
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. Задание 5; Задание 6

Формы реализации: Проверка задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
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: технологии, применяемые при проведении компьютерного аудита	1.Охарактеризовать назначение анализа событий в исследуемом объекте. 2.Дать характеристику анализа событий в исследуемом объекте.
Уметь: применять сканеры безопасности для оценки защищенности объекта исследования	1.Разъяснить способы развёртывания ИТ для анализа событий на объекте исследования SIEM (ELK)

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
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: 70
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. Задание 7; Задание 8

Формы реализации: Проверка задания

Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
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: цели, принципы и методы проведения компьютерного аудита	1.Охарактеризовать принципы работы анализа событий в исследуемом объекте.
Знать: основные технологии тестирования объекта исследования	1.Дать характеристику технологии анализа событий в исследуемом объекте.
Уметь: развертывать и использовать ИТ для анализа событий на объекте исследования SIEM (ELK)	1.Разъяснить способы развёртывания использования ИТ для анализа событий на объекте исследования SIEM (ELK)

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
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: 70
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

7 семестр

Форма промежуточной аттестации: Зачет с оценкой

Процедура проведения

Зачет проводится в устной форме по билетам согласно программе зачета

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

1. Компетенция/Индикатор: ПК-3.1$_{ПК-3}$ Администрирует подсистемы защиты информации в операционных системах

Вопросы, задания

1.Понятие Компьютерный аудит и методы его проведения.
2.Модели аудита.
3.Этапы проведения компьютерного аудита.
4.Кто проводит аудит?
5.Цели, программа и план аудита.
6.Принципы аудита.
7.Виды аудита и формы его проведения.
8.Методы тестирования penetrationtesting (PT).
9.Этапы работы технического эксперта по компьютерному аудиту.
10.Формальное описание системы в модели Харрисона-Руззо-Ульмана.
11.Модель целостности Кларка-Вилсона. Достоинства и недостатки модели целостности Кларка-Вильсона.
12.Модель безопасности ОС Windows. Подсистемы Windows, обеспечивающие безопасность.
13.Что такое идентификаторы безопасности SID (SecureIdentifier)?
14.Примеры SID безопасности.
15.Как узнать значение SID конкретного пользователя?
16.Подсистемы аудита событий ОС Windows
17.Что сохраняется в журналах событий?
18.Схема шифрования EFS в ОС Windows/
19.В каком направлении развиваются современные ОС?
20.Как обеспечить доверие к рассмотренным механизмам безопасности ОС?
21.Почему нельзя строить ответственные информационные системы на зарубежных ОС?

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

2.Чем не обеспечивается безопасность при использовании мобильных программ?

Ответы:

a 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-3.З$_{ПК-3}$ Администрирует средства защиты информации прикладного и системного программного обеспечения

Вопросы, задания

1.Методы получения информации из открытых источников.
2.Предложить способ выявления возможных инсайдеров при приеме сотрудников по открытым вакансиям в организацию.
3.Предложить способ наиболее полного сбора открытой информации на человека, претендующего на вакансию.
4.С какой целью ведется сбор открытой информации об объекте аудита?
5.Как обнаружить информацию о конфигурационных файлах в открытых web-приложениях?
6.Как используются социальные сети для сбора информации о претенденте на вакансию?
7.Аудит физического контроля доступа в помещения.
8.Аудит безопасности информационных активов организации.
9.Аудит организационного обеспечения.
10.Аудит соответствия нормативному обеспечению.
11.Аудит безопасности IT-структуры.
12.Проведение экспресс-тестов по оценке эффективности защиты информации в ИС.
13.Анализ защищенности по ГОСТ Р ИСО/МЭК 27001.
14.Анализ возможностей применения технологий социальной инженерии.
15.Анализ эффективности защиты от вредоносного кода.
16.Технологии компьютерного аудита на основе SIEM.
17.Оценка эффективности защиты веб-приложений.
18.Анализ получения информации от сетевых сервисов.
19.Оценка защищенности беспроводных сетей.
20.Анализ возможностей обхода систем безопасности.
21.Технологии выполнения тестирования на проникновение.

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;
e) 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

III. Правила выставления итоговой оценки по курсу

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