Имя: _____ **Дата:** _____ **Баллы:** _____

Антивирусное ПО и защита конечных устройств Руководство по защите

Обнаружение по сигнатурам, эвристика, мониторинг поведения, песочница, обновления

ОБЗОР ОБУЧЕНИЯ ПО АНТИВИРУСНОМУ ПО

ЗАЩИЩЁННЫЙ
ШИФРОВАНИЕ ДАННЫХ
Стандарт AES 256 бит

СООТВЕТСТВУЮЩИЙ
ГЛОБАЛЬНЫЕ СТАНДАРТЫ
Нормативные рамки GDPR и CCPA

НУЛЕВОЕ ДОВЕРИЕ
ПОЛИТИКА ДОСТУПА
Многофакторная аутентификация

Добро пожаловать! Этот пакет заданий проведёт вас через антивирусное ПО и защиту конечных точек. Вы изучите базы сигнатур, эвристические сканеры, поведенческий мониторинг, виртуальные файлы песочницы и снижение числа ложных срабатываний.

КОНТРОЛЬНЫЕ ТОЧКИ РАБОЧЕГО ЛИСТА

- [ ] **Части 1-4: освойте кибербезопасность и предотвращение угроз.**
- [ ] **Части 5-7: решите кроссворд и головоломки «поиск слов».**
- [ ] **Части 8-9: решите кейсы и задание с шифром.**
- [ ] **Часть 10: изучите страницы часто задаваемых вопросов (базовый и продвинутый уровень).**
- [ ] **Часть 11: изучите 10 интересных фактов из реальной жизни.**
- [ ] **Дополнительно: задание «Думай быстро».**

Открыть руководство VPN.com по кибербезопасности

URL: https://www.vpn.com/ru/kiberbezopasnost/antivirus/

Ваша дорожная карта обучения: стратегия антивирусной защиты

- Различайте сигнатурное и эвристическое обнаружение вредоносного ПО.
- Разберитесь, как работают мониторинг поведения и протоколы изоляции в песочнице.
- Оцените влияние сканирования в реальном времени на производительность системы и конечных точек.
- Уменьшайте ложные срабатывания классификации с помощью проверки цифровых сертификатов.
- Управляйте ежедневным распространением обновлений определений на корпоративных конечных устройствах.

ИНСТРУКЦИЯ ПО АНТИВИРУСАМ

Ответьте на вопросы с выбором ответа и вопросы «верно/неверно», дополните предложения с пропусками, используя банк слов, сопоставьте определения и решите кроссворд и головоломку «поиск слов». Примените свои знания по теме: антивирусной защите конечных устройств. Завершите работу дополнительным заданием «Думай быстро».

ЗАЩИТА АНТИВИРУСОМ И СИГНАТУРНОЕ СКАНИРОВАНИЕ (ВВЕДЕНИЕ)

Антивирусное ПО защищает конечные устройства, выявляя вредоносное ПО, помещая его в карантин и удаляя. Современные системы сочетают базы сигнатур (сопоставление с хэшами известных угроз) с эвристикой (анализ структуры файла) и мониторингом поведения для обнаружения эксплойтов нулевого дня.

ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ КАЖДУЮ КОНТРОЛЬНУЮ ТОЧКУ И ВЫБЕРИТЕ ИЛИ НАПИШИТЕ ПРАВИЛЬНЫЙ

Контрольная точка 1: Задание с выбором ответа

1. В чём ограничение обнаружения на основе сигнатур?

- A. Не может обнаружить неизвестное или изменённое вредоносное ПО
- B. Он даёт много ложных срабатываний
- C. Требует высокой вычислительной мощности процессора
- D. Работает только при подключении к интернету

2. Как эвристические сканеры обнаруживают новые варианты вредоносного ПО?

- A. Выявляя подозрительные закономерности и структуры кода
- B. Сопоставлением хэшей файлов с базой данных угроз
- C. Автоматическое удаление всех неподписанных исполняемых файлов
- D. Загрузкой каждого файла в общедоступную облачную папку

3. Для чего нужно выполнение в песочнице антивируса?

- A. Изоляция и анализ файлов в защищённом виртуальном хранилище
- B. Ускорение передачи резервной копии локальной файловой системы
- C. Обновление исправлений безопасности локальной операционной системы
- D. Сжатие больших файлов документов для экономии места

4. Какой метод обнаружения выявляет опасное поведение в реальном времени?

- A. Поведенческий анализ, отслеживающий действия программ
- B. Проверка исторических журналов, выполняемая ночью
- C. Ручное сообщение пользователей о медленных приложениях
- D. Еженедельная ручная проверка установленных программ

5. Почему регулярные обновления определений критически важны для сканеров?

- A. Чтобы передавать сигнатурным движкам идентификаторы угроз из базы данных
- B. Чтобы повысить тактовую частоту процессора во время работы
- C. Чтобы изменять время кэширования глобальных DNS-серверов имён
- D. Чтобы разрешить настройки cookie веб-браузера

Контрольная точка 2: Задание «верно или неверно»

6 **Вопрос «верно/неверно» 6**

6. Обнаружение по сигнатурам сопоставляет криптографические хеши файлов со списками в базе данных.

○ Верно ○ Неверно

7 **Вопрос «верно/неверно» 7**

7. Эвристические сканеры могут вызывать ложные срабатывания на безопасных файлах.

○ Верно ○ Неверно

8 **Вопрос «верно/неверно» 8**

8. Песочница позволяет вредоносному ПО без ограничений обращаться к сетевым файлам.

○ Верно ○ Неверно

9 **Вопрос «верно/неверно» 9**

9. Поведенческое сканирование блокирует файлы, когда они совершают вредоносные действия.

○ Верно ○ Неверно

10 **Вопрос «верно/неверно» 10**

10. Стандартное антивирусное ПО полностью останавливает все атаки нулевого дня.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

Прочитайте каждое предложение ниже и вставьте пропущенный термин из банка слов.

1. Уникальные цифровые отпечатки, по которым традиционный сканер опознаёт известное вредоносное ПО, называются _____ .

2. Анализ шаблонов кода в файлах называется _____ .

3. Антивирусы изолируют подозрительные файлы в среде, которая называется _____ .

4. При мониторинге в реальном времени на подозрительные действия проверяется _____ программ.

5. Чтобы распознавать новые угрозы, сканеры ежедневно загружают _____ базы.

6. Когда безопасную программу помечают как вредоносную, возникает _____ .

СЛОВАРНЫЙ БАНК СЛОВ

БРАНДМАУЭР КАРАНТИН ЛОЖНАЯ ТРЕВОГА ОБНОВЛЕНИЯ ПЕСОЧНИЦА ПОВЕДЕНИЕ СИГНАТУРЫ ЭВРИСТИКА

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление понятий о безопасности

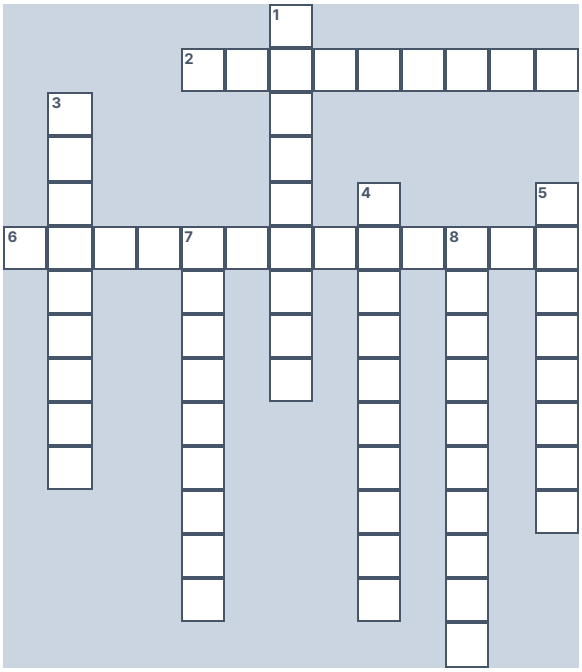
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

Сопоставьте каждый термин слева с правильным определением справа, введя соответствующую букву (A–H) в заполняемое поле.

☐	1. Хеш-подпись	A	Помещение подозрительных файлов в изоляцию, чтобы не допустить воздействия на локальную систему.
☐	2. Эвристика кода	B	Набор программ для сканирования и защиты конечных устройств от эксплойтов.
☐	3. Песочница для файлов	C	Наблюдение за действиями запущенного ПО на предмет шаблонов вредоносной работы.
☐	4. Поведенческое сканирование	D	Уникальный криптографический отпечаток в базе данных, используемый для выявления известных угроз.
☐	5. Ежедневные обновления	E	Защищённая виртуальная тестовая среда для безопасного запуска недоверенного кода.
☐	6. Ложное срабатывание	F	Регулярные загрузки определений, пополняющие базу данных угроз.
☐	7. Изоляция угроз	G	Анализ на основе правил, помечающий файлы с подозрительной структурой кода.
☐	8. Антивирус	H	Оповещение системы безопасности, ошибочно относящее безопасное ПО к вредоносному.

Контрольная точка 5: Кроссворд

Решите кроссворд, вводя буквы в активные белые клетки. Номера соответствуют подсказкам ниже.



ПО ГОРИЗОНТАЛИ

2. Наблюдение за действиями запущенных программ в поисках шаблонов вредоносной работы (9)

6. Оповещение системы безопасности, ошибочно относящее безопасную программу к вредоносным (13)

ПО ВЕРТИКАЛИ

1. Анализ на основе правил, помечающий файлы с подозрительной структурой кода (9)

3. Защищённая виртуальная тестовая среда для безопасного запуска недоверенного кода (9)

4. Уникальный криптографический отпечаток в базе данных, по которому опознают известные угрозы (10)

5. Помещение подозрительных файлов в изоляцию, чтобы они не угрожали локальной системе (8)

7. Пакет программ, сканирующий и защищающий конечные устройства от эксплойтов (9)

8. Регулярные загрузки определений, пополняющие базу угроз (10)

Контрольная точка 5, альтернативный вариант: Доступные подсказки к кроссворду

Пользователи программ чтения с экрана и клавиатуры могут вводить ответы на кроссворд прямо в текстовые поля ниже. ПО ГОРИЗОНТАЛИ ПО ВЕРТИКАЛИ

ПО ГОРИЗОНТАЛИ

2 по горизонтали: Наблюдение за действиями запущенных программ в поисках шаблонов вредоносной работы (9 букв):

6 по горизонтали: Оповещение системы безопасности, ошибочно относящее безопасную программу к вредоносным (13 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Анализ на основе правил, помечающий файлы с подозрительной структурой кода (9 букв):

3 по вертикали: Защищённая виртуальная тестовая среда для безопасного запуска недоверенного кода (9 букв):

4 по вертикали: Уникальный криптографический отпечаток в базе данных, по которому опознают известные угрозы (10 букв):

5 по вертикали: Помещение подозрительных файлов в изоляцию, чтобы они не угрожали локальной системе (8 букв):

7 по вертикали: Пакет программ, сканирующий и защищающий конечные устройства от эксплойтов (9 букв):

8 по вертикали: Регулярные загрузки определений, пополняющие базу угроз (10 букв):

Контрольная точка 6: Поиск скрытых слов

Найдите в сетке ниже 8 ключевых терминов. Слова могут идти по горизонтали, по вертикали или по диагонали.

К А У Ч Й Т Ъ О Ш Т Щ Ш М А Е

Т Ц П Н Б С Ъ Б З И Э У Ф Ь Ю

Ь И Л М Щ Л Ю Н Ы Э В Т М К Я

С Н К Л Р А Е О К Б Р Ч А Л Ж

И Ч Ы Е М Я М В Е Н И Ф Р Л А

П О З Т М С Г Л Р В С Д И К Б

Д С Б Т Х О У Е Ы Ш Т К Ю З Ю

О Е Ц И Э Ы Й Н Ж Х И Ш С Щ М

П П Х Д Ш Ц О И У Н К П Ц Й М

Ш У Й Ю Т О Ь Я Щ Р А Ю Ф Ф Б

Е Л О Ж Н А Я Т Р Е В О Г А А

Х О Т А Н Т И В И Р У С П Б Н

К Ж П О В Е Д Е Н И Е Л Р Ю В

Я Я Ю В Р Ъ Э О Г Ж Т Ь У Ф Э

Й Н И Т Н А Р А К Е Ю В Ы О Ж

СПИСОК СЛОВ СЛОВАРЯ

ХЕШПОДПИСЬ ЭВРИСТИКА ПЕСОЧНИЦА ПОВЕДЕНИЕ ОБНОВЛЕНИЯ
ЛОЖНАЯТРЕВОГА КАРАНТИН АНТИВИРУС

Контрольная точка 6, альтернативный вариант: Доступное сопоставление терминов

Сопоставьте каждый из 8 терминов из поиска слов с правильным определением, написав букву (A–H) на пустой строке.

ТЕРМИНЫ СЛОВАРЯ

- **A. ХЕШПОДПИСЬ**
- **B. ЭВРИСТИКА**
- **C. ПЕСОЧНИЦА**
- **D. ПОВЕДЕНИЕ**
- **E. ОБНОВЛЕНИЯ**
- **F. ЛОЖНАЯТРЕВОГА**
- **G. КАРАНТИН**
- **H. АНТИВИРУС**

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Наблюдение за действиями запущенных программ в поисках шаблонов вредоносной работы.

_____ 2. Пакет программ, сканирующий и защищающий конечные устройства от эксплойтов.

_____ 3. Регулярные загрузки определений, пополняющие базу угроз.

_____ 4. Анализ на основе правил, помечающий файлы с подозрительной структурой кода.

_____ 5. Помещение подозрительных файлов в изоляцию, чтобы они не угрожали локальной системе.

_____ 6. Уникальный криптографический отпечаток в базе данных, по которому опознают известные угрозы.

_____ 7. Защищённая виртуальная тестовая среда для безопасного запуска недоверенного кода.

_____ 8. Оповещение системы безопасности, ошибочно относящее безопасную программу к вредоносным.

Контрольная точка 7: Задание с перепутанными словами

Расставьте буквы ниже в правильном порядке, чтобы получить ключевые понятия и термины кибербезопасности. Запишите ответы в предусмотренные поля.

1. СПДОЕХИЬПШ
2. АПЦОЕНИЧС
3. ОЛИЕБВЯОНН
4. АИНТНКАР
5. ИСВАТИЭКР
6. ИЕОНЕПДЕВ
7. ВОРЯЛОЕААГЖТН
8. СВУАИНИРТ

Дополнительное задание: Думай быстро

ПО 3 ОТВЕТА В КАЖДОЙ КАТЕГОРИИ. ПОБЕЖДАЕТ ТОТ, КТО ПЕРВЫМ ЗАПОЛНИТ СПИСОК.

1	Причины обновлять программы			
2	Люди, у которых можно попросить помощи по ИТ			
3	Что делать, когда антивирус что-то обнаружил			
4	Признаки компьютерного вируса			
5	То, что отправляется в карантин			
6	Места, где прячутся вирусы			
7	Информация, которой нельзя делиться			
8	Виды вредоносного ПО			
9	Известные вам инструменты безопасности			
10	То, что проверяет антивирус			
11	То, для чего вы делаете резервные копии			
12	Устройства, которые могут быть взломаны			
13	Известные вам антивирусные программы			
14	Причины ложных срабатываний			
15	Безопасные привычки, которые можно начать уже сегодня			

Контрольная точка 8: Кейсы по кибербезопасности

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: СИГНАТУРНОЕ И ЭВРИСТИЧЕСКОЕ СКАНИРОВАНИЕ



Ситуация: Сотрудник скачивает специальную утилиту, созданную внутри компании другой командой. Сигнатурный сканер её пропускает, но эвристический сканер помечает её как подозрительную.

Вопрос для обсуждения: Объясните, почему так произошло и как проверить, безопасен ли файл.

КЕЙС 2: ОБРАБОТКА ЛОЖНЫХ СРАБАТЫВАНИЙ



Ситуация: Разработчик программного обеспечения компилирует своё приложение. Системный антивирус помечает новый исполняемый файл как вредоносное ПО и отправляет его в карантин.

Вопрос для обсуждения: Опишите риски добавления в белый список и расскажите, как правильно решить эту ситуацию.

Контрольная точка 9: Расшифруйте шифр

Специалист по кибербезопасности защищает сетевые ресурсы от онлайн-злоумышленников. Используйте ключ «буква–число» ниже, чтобы расшифровать сообщение, вписав соответствующие буквы в пустые места.

КЛЮЧ ШИФРОВАНИЯ «БУКВА В ЧИСЛО»

А=1 Б=2 В=3 Г=4 Д=5 Е=6 Ё=7 Ж=8 З=9 И=10 Й=11

К=12 Л=13 М=14 Н=15 О=16 П=17 Р=18 С=19 Т=20 У=21 Ф=22

Х=23 Ц=24 Ч=25 Ш=26 Щ=27 Ъ=28 Ы=29 Ь=30 Э=31 Ю=32 Я=33

31	3	18	10	19	20	10	12	1		3	29	33	3	13	33	6	20

15	16	3	16	6		3	18	6	5	16	15	16	19	15	16	6		17	16

Расшифрованное сообщение:

СОВЕТ: КАЖДОЕ ЧИСЛО ОБОЗНАЧАЕТ ПОЗИЦИЮ ЭТОЙ БУКВЫ В АЛФАВИТЕ (НАПРИМЕР, 1 = А, 2 = Б, 33 = Я).

Контрольная точка 10: Базовые вопросы о кибербезопасности (Часть A)

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q1: Как антивирусное ПО распознаёт вредоносное ПО?

Выявляет вредоносное ПО по сопоставлению сигнатур в базе данных, эвристическому анализу структуры кода и мониторингу поведения в реальном времени.

Q2: Что такое обнаружение на основе сигнатур?

Это метод сканирования, сопоставляющий криптографические хеши файлов с базами известных угроз вредоносного ПО.

Q3: Что такое эвристический сканер?

Эвристика анализирует структуру файла и инструкции кода, отмечая подозрительные шаблоны, характерные для вариантов вредоносного ПО.

Q4: Что означает помещение файла в карантин?

Антивирус перемещает файл в защищённую изолированную папку и блокирует его запуск, чтобы защитить операционную систему.

Q5: Что такое ложное срабатывание антивируса?

Это ошибка, при которой законное безопасное ПО ошибочно помечается алгоритмами сканирования как вредоносное.

Контрольная точка 10: Базовые вопросы о кибербезопасности (Часть B)

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q6: Как мониторинг поведения защищает системы?

Отслеживает работающее ПО в реальном времени и блокирует процессы, пытающиеся вносить подозрительные изменения, например внедрять код.

Q7: Почему важно тестирование в песочнице?

Песочница запускает ненадёжные файлы в изолированной виртуальной машине, безопасно наблюдая за их действиями без риска для системы.

Q8: Как часто следует обновлять антивирусные базы?

Сканеры следует обновлять ежедневно или ежечасно, чтобы они распознавали недавно обнаруженные штаммы вредоносного ПО.

Q9: Чем антивирус отличается от EDR?

Антивирус сосредоточен на сканировании файлов, а Endpoint Detection and Response (EDR) обеспечивает отслеживание и сдерживание угроз во всей сети.

Q10: Можно ли запускать две антивирусные программы одновременно?

Нет. Работа двух активных сканеров вызывает системные конфликты, замедляет производительность и может блокировать работу друг друга.

Контрольная точка 10: Продвинутые вопросы о безопасности (Часть C)

Изучите продвинутые технические аспекты систем безопасности, анализа вредоносного ПО и соответствия требованиям к данным.

Q1: Как эвристические правила сводят к минимуму обход защиты от угроз?

Эвристика анализирует общие шаблоны угроз, а не конкретные сигнатуры, и выявляет модифицированные варианты известных семейств вредоносного ПО.

Q2: Что такое полиморфный вирус?

Это вредоносное ПО, которое при каждом запуске меняет структуру файла и процедуру расшифровки, из-за чего сканирование по сигнатурам неэффективно.

Q3: Как песочницы обнаруживают попытки обхода виртуальных машин?

Современные песочницы имитируют щелчки мыши и время работы системы, обманывая вредоносное ПО, которое скрывается при запуске в виртуальных машинах.

Q4: В каких форматах загружаются обновления сигнатур?

Обновления обычно представляют собой лёгкие инкрементные двоичные файлы различий, что снижает потребление сетевого трафика клиента.

Q5: Как агенты на конечных точках управляют локальным сканированием?

Агенты выполняют лёгкие фоновые проверки, перекладывая глубокий поиск криптографических хешей на облачные базы данных угроз.

Контрольная точка 10: Продвинутые вопросы о безопасности (Часть D)

Изучите продвинутые технические аспекты систем безопасности, анализа вредоносного ПО и соответствия требованиям к данным.

Q6: Что такое сканирование на руткиты?

Сканирует таблицы памяти на уровне ядра в обход API ОС, которые руткиты перехватывают, чтобы скрыть свои активные потоки.

Q7: Как поведенческое сканирование блокирует программы-вымогатели?

Обнаруживает автоматические циклы массового шифрования файлов и завершает процесс хоста до блокировки системных баз данных.

Q8: Что такое проверка сертификата подписи кода?

Сканеры сверяют цифровые подписи кода с доверенными корневыми центрами сертификации, подтверждая личность разработчика программы.

Q9: Как упаковщики влияют на движки сканирования?

Упаковщики сжимают или шифруют полезную нагрузку вредоносного ПО. Сканеры должны распаковать файл в памяти, прежде чем сработает проверка сигнатур.

Q10: Как инструменты EDR автоматизируют изоляцию?

Агенты EDR помещают скомпрометированные конечные точки в карантин на сетевом уровне, блокируя боковое перемещение, но сохраняя доступ для аналитика.

Часть 11: 10 реальных фактов и выводов о кибербезопасности

Ознакомьтесь с реальными фактами об инцидентах безопасности, механизмах защиты и стандартах соответствия.

1. АНАЛИЗ БЕЗОПАСНОСТИ

Базы данных сигнатур хранят хеши известного вредоносного ПО, поэтому совершенно новые или изменённые файлы остаются незамеченными до обновления определений.

2. АНАЛИЗ БЕЗОПАСНОСТИ

Эвристические движки могут пометить некоторые новые варианты вредоносного ПО ещё до появления сигнатур, но ценой большего числа ложных срабатываний.

3. АНАЛИЗ БЕЗОПАСНОСТИ

Ложные срабатывания отнимают у ИТ-команд время на проверку и восстановление файлов, ошибочно помещённых в карантин.

4. АНАЛИЗ БЕЗОПАСНОСТИ

Полиморфное вредоносное ПО изменяет свой код с каждой копией, поэтому защитники сочетают сигнатуры с эвристическими и поведенческими проверками.

6. АНАЛИЗ БЕЗОПАСНОСТИ

Авторы вредоносного ПО пишут собственный код, проверяющий среду песочницы, и откладывают выполнение, чтобы обойти таймеры.

5. АНАЛИЗ БЕЗОПАСНОСТИ

Облачные антивирусные движки почти в реальном времени сверяют хеши подозрительных файлов с большими онлайн-базами угроз.

7. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Поставщики регулярно отправляют обновления определений на конечные устройства, чтобы сканеры могли распознавать недавно подтверждённые угрозы.

8. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Поведенческие мониторы программ-вымогателей отслеживают определённые вызовы Win32 API, связанные с шифрованием файлов и удалением теневых копий.

9. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Действительные подписи кода могут снизить риск ложных срабатываний, но подписанные файлы всё равно сканируются, поскольку вредоносное ПО тоже может быть подписано.

10. АНАЛИЗ БЕЗОПАСНОСТИ

Руткиты изменяют структуры ядра системы, поэтому для их обнаружения и удаления нужны специализированные сканеры, работающие при загрузке.

Технические ссылки и источники

Учебное пособие и интерактивные головоломки составлены на основе мировых стандартов NIST, OWASP и требований к соблюдению правил конфиденциальности данных. НАУЧНЫЕ И ОТРАСЛЕВЫЕ ИСТОЧНИКИ

НАУЧНЫЕ И ОТРАСЛЕВЫЕ ИСТОЧНИКИ

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

https://csrc.nist.gov/pubs/sp/800/83/r1/final

[2] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[3] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[5] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.

https://csrc.nist.gov/pubs/sp/800/61/r3/final

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 **Вопрос 1** СИГНАТУРЫ **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Сигнатурное сканирование опирается на известные хеши из базы данных и не обнаруживает неизвестное или изменённое вредоносное ПО. Источник: OWASP Secure Configuration.

2 **Вопрос 2** ЭВРИСТИКА **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Эвристика анализирует структуру кода и команды, чтобы выявлять подозрительные признаки новых вариантов угроз. Источник: Center for Internet Security (CIS).

3 **Вопрос 3** ИЗОЛЯЦИЯ В ПЕСОЧНИЦЕ **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Песочница запускает подозрительные файлы в изолированной виртуальной машине, чтобы безопасно наблюдать за их поведением при выполнении. Источник: NIST Digital Identity.

4 **Вопрос 4** ПОВЕДЕНЧЕСКИЙ **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Сканирование поведения отслеживает работающие программы в реальном времени, чтобы блокировать несанкционированные изменения системы. Источник: Center for Internet Security (CIS).

5 **Вопрос 5** ОБНОВЛЕНИЯ **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Сканеры загружают ежедневные инкрементальные обновления определений, чтобы оставаться в курсе актуальных угроз. Источник: OWASP Secure Configuration.

Ответы: контрольная точка 2 – верно или неверно

6 **Вопрос 6** СИГНАТУРЫ **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Сигнатурные инструменты вычисляют криптографические хеши и сопоставляют их с базой данных хешей известных угроз. Источник: OWASP Secure Configuration.

7 **Вопрос 7** ЭВРИСТИКА **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Эвристические движки применяют правила, основанные на структуре, и могут помечать как подозрительные законные, безопасные файлы. Источник: Center for Internet Security (CIS).

8 **Вопрос 8** ИЗОЛЯЦИЯ В ПЕСОЧНИЦЕ **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Песочница запускает код в виртуальном контейнере, строго блокируя доступ к сетевым папкам общего доступа. Источник: NIST Digital Identity.

9 **Вопрос 9** ПОВЕДЕНЧЕСКИЙ **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Мониторинг в реальном времени помечает работающие процессы, которые пытаются выполнить недопустимую запись или блокировку файлов. Источник: Center for Internet Security (CIS).

10 **Вопрос 10** **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Ни один антивирус не останавливает каждую атаку нулевого дня; неизвестные угрозы могут обойти сигнатуры и эвристику.

Ключи к словарю и критерии оценивания

Критерии оценивания для преподавателя: ставьте 1 балл за каждое верное сопоставление (всего 8 баллов) и за каждый контекстный термин (всего 6 баллов).

КОНТРОЛЬНАЯ ТОЧКА 4: ОТВЕТЫ – СОПОСТАВЛЕНИЕ ПОНЯТИЙ

D 1. Хеш-подпись	G 2. Эвристика кода	E 3. Песочница для файлов	C 4. Поведенческое сканирование
F 5. Ежедневные обновления	H 6. Ложное срабатывание	A 7. Изоляция угроз	B 8. Антивирус

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 СИГНАТУРЫ	2 ЭВРИСТИКА	3 ПЕСОЧНИЦА	4 ПОВЕДЕНИЕ
5 ОБНОВЛЕНИЯ	6 ЛОЖНАЯ ТРЕВОГА		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 D – ПОВЕДЕНИЕ	2 H – АНТИВИРУС	3 E – ОБНОВЛЕНИЯ	4 B – ЭВРИСТИКА
5 G – КАРАНТИН	6 A – ХЕШПОДПИСЬ	7 C – ПЕСОЧНИЦА	8 F – ЛОЖНАЯТРЕВОГА

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить Хеш-подпись, Эвристика кода и Песочница для файлов и привести пример для каждого термина.

Кейсы:
Попросите учащихся обосновывать свои рекомендации фактами из рабочего листа, а не мнениями.

Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

К	А	У	Ч	Й	Т	Ъ	О	Ш	Т	Щ	Ш	М	А	Е
Т	Ц	П	Н	Б	С	Ъ	Б	З	И	Э	У	Ф	Ь	Ю
Ь	И	Л	М	Щ	Л	Ю	Н	Ы	Э	В	Т	М	К	Я
С	Н	К	Л	Р	А	Е	О	К	Б	Р	Ч	А	Л	Ж
И	Ч	Ы	Е	М	Я	М	В	Е	Н	И	Ф	Р	Л	А
П	О	З	Т	М	С	Г	Л	Р	В	С	Д	И	К	Б
Д	С	Б	Т	Х	О	У	Е	Ы	Ш	Т	К	Ю	З	Ю
О	Е	Ц	И	Э	Ы	Й	Н	Ж	Х	И	Ш	С	Щ	М
П	П	Х	Д	Ш	Ц	О	И	У	Н	К	П	Ц	Й	М
Ш	У	Й	Ю	Т	О	Ь	Я	Щ	Р	А	Ю	Ф	Ф	Б
Е	Л	О	Ж	Н	А	Я	Т	Р	Е	В	О	Г	А	А
Х	О	Т	А	Н	Т	И	В	И	Р	У	С	П	Б	Н
К	Ж	П	О	В	Е	Д	Е	Н	И	Е	Л	Р	Ю	В
Я	Я	Ю	В	Р	Ъ	Э	О	Г	Ж	Т	Ь	У	Ф	Э
Й	Н	И	Т	Н	А	Р	А	К	Е	Ю	В	Ы	О	Ж

РЕШЕНИЕ КРОССВОРДА



ПО ГОРИЗОНТАЛИ

2 по горизонтали: ПОВЕДЕНИЕ Наблюдение за действиями запущенных программ в поисках шаблонов вредоносной работы (9 букв)

6 по горизонтали: ЛОЖНАЯТРЕВОГА Оповещение системы безопасности, ошибочно относящее безопасную программу к вредоносным (13 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: ЭВРИСТИКА Анализ на основе правил, помечающий файлы с подозрительной структурой кода (9 букв)

3 по вертикали: ПЕСОЧНИЦА Защищённая виртуальная тестовая среда для безопасного запуска недоверенного кода (9 букв)

4 по вертикали: ХЕШПОДПИСЬ Уникальный криптографический отпечаток в базе данных, по которому опознают известные угрозы (10 букв)

5 по вертикали: КАРАНТИН Помещение подозрительных файлов в изоляцию, чтобы они не угрожали локальной системе (8 букв)

7 по вертикали: АНТИВИРУС Пакет программ, сканирующий и защищающий конечные устройства от эксплойтов (9 букв)

8 по вертикали: ОБНОВЛЕНИЯ Регулярные загрузки определений, пополняющие базу угроз (10 букв)

Ключ к словам-перевёртышам и шифру

Ключ для проверки заданий на расшифровку слов и «Секретного шифра».

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. СПДОЕХИЬПШ — **ХЕШПОДПИСЬ**
2. АПЦОЕНИЧС — **ПЕСОЧНИЦА**
3. ОЛИЕБВЯОНН — **ОБНОВЛЕНИЯ**
4. АИНТНКАР — **КАРАНТИН**
5. ИСВАТИЭКР — **ЭВРИСТИКА**
6. ИЕОНЕПДЕВ — **ПОВЕДЕНИЕ**
7. ВОРЯЛОЕААГЖТН — **ЛОЖНАЯТРЕВОГА**
8. СВУАИНИРТ — **АНТИВИРУС**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ЭВРИСТИКА ВЫЯВЛЯЕТ НОВОЕ ВРЕДОНОСНОЕ ПО"

Ответы к кейсам

A Кейс 1: Сигнатурное и эвристическое сканирование

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: сотрудник скачивает специальную утилиту, созданную внутри компании другой командой. Сигнатурный сканер её пропускает, но эвристический сканер помечает как подозрительную.
- Рекомендуемая стратегия и решение: Почему это произошло: сигнатурное сканирование проверяет хеши файлов; поскольку файл нестандартный, его нет в базе угроз. Эвристика анализирует структуру и отметила подозрительные действия (например, записи в реестр). Проверка: запустите файл в песочнице, чтобы понаблюдать за действиями, проверьте цифровые подписи и отправьте хеш на порталы анализа угроз.

B Кейс 2: Обработка ложных срабатываний

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: разработчик программного обеспечения компилирует своё приложение. Системный антивирус помечает новый исполняемый файл как вредоносный и помещает его в карантин.
- Рекомендуемая стратегия и решение: Риски белого списка: обход сканеров может позволить запуститься реальному заражённому коду. Путь решения: отправьте файл антивирусному вендору на анализ, подпишите код цифровой подписью через центры сертификации и временно настройте исключения для конкретных папок вместо отключения антивируса.