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

# Анализ вредоносного ПО и снижение угроз Руководство

**Трояны, программы-вымогатели, шпионское ПО, руткиты, песочницы виртуализации, изоляция**

## ОБЗОР ОБУЧЕНИЯ: АНАЛИЗ ВРЕДОНОСНОГО 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 анализ вредоносного ПО и защиту от него. Вы изучите шпионское ПО, трояны, вредоносные нагрузки программ-вымогателей, инструменты обратной разработки, поведение руткитов и стратегии сдерживания.

### 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/vredonosnoe-po/

# Ваша дорожная карта обучения: снижение угрозы вредоносного ПО

- Различайте типы вредоносного ПО: троян, червь и руткит.
- Внедрите виртуализацию с песочницей для выполнения кода при анализе.
- Разработайте планы изоляции и очистки от активной вредоносной нагрузки программ-вымогателей.

## ИНСТРУКЦИИ К РУКОВОДСТВУ ПО АНАЛИЗУ ВРЕДОНОСНОГО ПО

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: снижению рисков от вредоносного ПО. Завершите работу дополнительным заданием «Думай быстро».

## АНАЛИЗ ВРЕДОНОСНОГО ПО И СДЕРЖИВАНИЕ УГРОЗ (ВВЕДЕНИЕ)

Вредоносный код, такой как трояны, черви и программы-вымогатели, представляет серьёзную угрозу для конечных устройств и серверов. Команды безопасности анализируют вредоносное ПО в виртуальных песочницах и быстро изолируют сеть, чтобы остановить распространение полезной нагрузки.

**ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ КАЖДУЮ КОНТРОЛЬНУЮ ТОЧКУ И ВЫБЕРИТЕ ИЛИ НАПИШИТЕ ПРАВИЛЬНЫЙ ОТВЕТ.**

## Контрольная точка 1: Задание с выбором ответа

**1. В чём определяющая особенность троянского коня?**

- A. Маскируется под легальную программу, чтобы обманом заставить пользователей её запустить
- B. Он автоматически распространяется по линиям локальной сети
- C. Заражает файлы внутри изолированных виртуальных песочниц
- D. Перехватывает трафик интернет-провайдера

**2. Какой тип вредоносного ПО шифрует файлы и требует выкуп?**

- A. Программа-вымогатель
- B. Шпионское ПО
- C. Руткит
- D. Рекламное ПО

**3. Что представляет собой шпионское ПО?**

- A. Вредоносное ПО, предназначенное для скрытого отслеживания нажатий клавиш и действий пользователя в браузере
- B. Программный код, выполняющийся внутри изолированного виртуального контейнера
- C. Обновления антивредоносного ПО, загруженные из реестров баз данных
- D. Автоматическая регулировка яркости экрана

**4. Зачем разработчики вредоносного ПО используют руткиты?**

- A. Чтобы скрыть активные процессы и вредоносные файлы от операционной системы
- B. Чтобы повысить скорость обработки процессора на конечных устройствах
- C. Чтобы создавать резервные копии файлов базы данных в защищённых облачных хранилищах
- D. Чтобы продлить время работы ноутбуков от батареи

**5. Что означает песочница при анализе вредоносного ПО?**

- A. Запуск подозрительных файлов в изолированном виртуальном хранилище для безопасного наблюдения за поведением
- B. Сканирование хэшей файлов по базам данных известных угроз
- C. Восстановление резервных копий базы данных после вторжения
- D. Отключение локальных сетевых маршрутизаторов от общедоступных линий

## Контрольная точка 2: Задание «верно или неверно»

### 6 Вопрос 6

6. Компьютерным червям требуется взаимодействие пользователя, чтобы распространяться по локальным сетям.

○ Верно ○ Неверно

### 7 Вопрос 7

7. Рекламное ПО всегда безвредно и не отслеживает поведение пользователя и историю браузера.

○ Верно ○ Неверно

### 8 Вопрос 8

8. Восстановление чистых резервных копий из офлайн-хранилища позволяет жертвам вернуть зашифрованные файлы, не платя выкуп.

○ Верно ○ Неверно

### 9 Вопрос 9

9. Антивирус на основе сигнатур надёжно останавливает вредоносное ПО нулевого дня ещё до появления его сигнатуры.

○ Верно ○ Неверно

### 10 Вопрос 10

10. Бесфайловое вредоносное ПО выполняет вредоносные скрипты в системной памяти, не записывая файлы на диск.

○ Верно ○ Неверно

## Контрольная точка 3: Вставьте ключевые термины

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

**1. Вредоносная программа, замаскированная под безопасную утилиту, — это** _____ .

**2. Вредоносный код, блокирующий базы данных ради денег, — это программа-** _____ .

**3. Кейлоггеры, тайно записывающие пароли, — это пример:** _____ .

**4. Скрытие глубоко в ядре операционной системы требует использовать** _____ .

**5. Для анализа подозрительных файлов в изолированном хранилище применяют виртуальную среду —** _____ .

**6. Чтобы остановить распространение активной вредоносной нагрузки, необходима немедленная сетевая** _____ .

**СЛОВАРНЫЙ БАНК СЛОВ**

БЕЗФАЙЛОВЫЙ ВЫМОГАТЕЛЬ ЛОКАЛИЗАЦИЯ ПЕСОЧНИЦА РУТКИТ
ТРОЯН ЧЕРВЬ ШПИОНСКОЕ ПО

**Напишите свои ответы здесь:**

**1.** **2.**

**3.** **4.**

**5.** **6.**

# Контрольная точка 4: Сопоставление понятий о безопасности

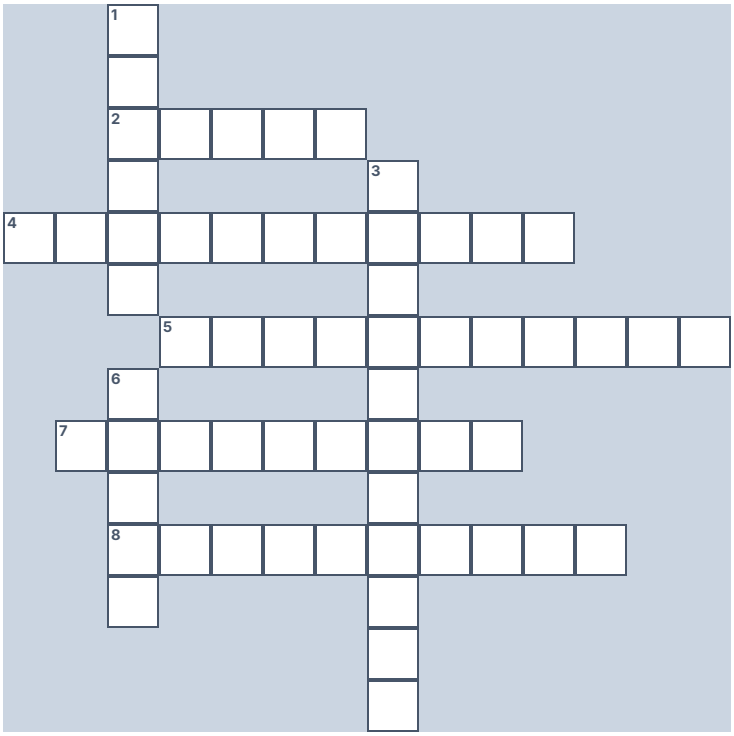
## СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

| | | | |
|---|---|---|---|
| ☐ | 1. ТРОЯН | A | Программа, предназначенная для скрытого наблюдения и записи действий и вводимых данных пользователя. |
| ☐ | 2. ПРОГРАММА-ВЫМОГАТЕЛЬ | B | Вредоносное ПО, работающее прямо в ОЗУ, чтобы избежать обнаружения сканерами дисков. |
| ☐ | 3. ШПИОНСКОЕ ПО | C | Изоляция заражённых конечных точек для предотвращения распространения вредоносной нагрузки. |
| ☐ | 4. РУТКИТ | D | Вредоносное ПО, замаскированное под безобидную или полезную утилиту. |
| ☐ | 5. ПЕСОЧНИЦА | E | Самораспространяющееся вредоносное ПО, которое передаётся по сетям без участия человека. |
| ☐ | 6. СДЕРЖИВАНИЕ | F | Вредоносное ПО, шифрующее системное хранилище и требующее оплату за выдачу ключа. |
| ☐ | 7. WORM | G | Изолированная виртуальная среда для безопасного анализа вредоносных файлов. |
| ☐ | 8. БЕЗФАЙЛОВЫЙ | H | Скрытое вредоносное ПО, глубоко внедряющееся в ядро системы, чтобы сохранять административный контроль. |

## Контрольная точка 5: Кроссворд

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




### ПО ГОРИЗОНТАЛИ

**2. Вредоносная программа, замаскированная под безвредную или полезную утилиту. (5)**

**4. Программа, предназначенная для тайного наблюдения за действиями пользователя и вводимыми данными и их записи. (11)**

**5. Вредоносный код, выполняемый прямо в ОЗУ, чтобы избежать обнаружения дисковыми сканерами. (11)**

**7. Изолированная виртуальная среда для безопасного анализа вредоносных файлов. (9)**

**8. Вредоносная программа, шифрующая хранилище системы и требующая оплату за выдачу ключа. (10)**

### ПО ВЕРТИКАЛИ

**1. Скрытая вредоносная программа, засевшая глубоко в ядре системы, чтобы сохранять административный контроль. (6)**

**3. Ограничение зараженных конечных узлов, чтобы не допустить распространения вредоносной нагрузки. (11)**

**6. Самореплицирующаяся вредоносная программа, распространяющаяся по сетям без участия человека. (5)**

# 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

**2 по горизонтали: Вредоносная программа, замаскированная под безвредную или полезную утилиту. (5 букв):**

**4 по горизонтали: Программа, предназначенная для тайного наблюдения за действиями пользователя и вводимыми данными и их записи. (11 букв):**

**5 по горизонтали: Вредоносный код, выполняемый прямо в ОЗУ, чтобы избежать обнаружения дисковыми сканерами. (11 букв):**

**7 по горизонтали: Изолированная виртуальная среда для безопасного анализа вредоносных файлов. (9 букв):**

**8 по горизонтали: Вредоносная программа, шифрующая хранилище системы и требующая оплату за выдачу ключа. (10 букв):**

## ПО ВЕРТИКАЛИ

**1 по вертикали: Скрытая вредоносная программа, засевшая глубоко в ядре системы, чтобы сохранять административный контроль. (6 букв):**

**3 по вертикали: Ограничение зараженных конечных узлов, чтобы не допустить распространения вредоносной нагрузки. (11 букв):**

**6 по вертикали: Самореплицирующаяся вредоносная программа, распространяющаяся по сетям без участия человека. (5 букв):**

## Контрольная точка 6: Поиск скрытых слов

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

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

**СПИСОК СЛОВ СЛОВАРЯ**

ТРОЯН ВЫМОГАТЕЛЬ ШПИОНСКОЕПО РУТКИТ ПЕСОЧНИЦА
ЛОКАЛИЗАЦИЯ ЧЕРВЬ БЕЗФАЙЛОВЫЙ

# 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. ТРОЯН**
- **B. ВЫМОГАТЕЛЬ**
- **C. ШПИОНСКОЕПО**
- **D. РУТКИТ**
- **E. ПЕСОЧНИЦА**
- **F. ЛОКАЛИЗАЦИЯ**
- **G. ЧЕРВЬ**
- **H. БЕЗФАЙЛОВЫЙ**

**ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ**

_____ 1. Скрытая вредоносная программа, засевшая глубоко в ядре системы, чтобы сохранять административный контроль.

_____ 2. Ограничение зараженных конечных узлов, чтобы не допустить распространения вредоносной нагрузки.

_____ 3. Вредоносный код, выполняемый прямо в ОЗУ, чтобы избежать обнаружения дисковыми сканерами.

_____ 4. Самореплицирующаяся вредоносная программа, распространяющаяся по сетям без участия человека.

_____ 5. Вредоносная программа, шифрующая хранилище системы и требующая оплату за выдачу ключа.

_____ 6. Программа, предназначенная для тайного наблюдения за действиями пользователя и вводимыми данными и их записи.

_____ 7. Вредоносная программа, замаскированная под безвредную или полезную утилиту.

_____ 8. Изолированная виртуальная среда для безопасного анализа вредоносных файлов.

## 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. **ЯОТНР** _____
2. **НОПШПСИЕОКО** _____
3. **ПНЧЕИАОЦС** _____
4. **РЬВЧЕ** _____
5. **ЕАЬЫОТГВЛМ** _____
6. **ИКРТТУ** _____
7. **АЛЛОЗЯЦИКИА** _____
8. **ВЛЙЙЗБАЕЫОФ** _____

# Дополнительное задание: Думай быстро

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

| | | | | |
|---|---|---|---|---|
| 1 | Места, где можно скачивать безопасные приложения | | | |
| 2 | Устройства, которые могут быть взломаны | | | |
| 3 | То, для чего вы делаете резервные копии | | | |
| 4 | Тревожные признаки в электронном письме | | | |
| 5 | Признаки того, что на телефоне есть вредоносное ПО | | | |
| 6 | Известные вам виды вредоносного ПО | | | |
| 7 | Типы файлов, с которыми нужно быть осторожным | | | |
| 8 | Способы, которыми вредоносное ПО попадает на ПК | | | |
| 9 | Безопасные привычки, которые можно начать уже сегодня | | | |
| 10 | Слова, связанные с кибербезопасностью | | | |
| 11 | Что делать после утечки данных | | | |
| 12 | Причины обновлять программы | | | |
| 13 | Животные или персонажи с названиями, похожими на вредоносное ПО | | | |
| 14 | То, что может украсть вредоносное ПО | | | |
| 15 | Что делать, если вы перешли по неверной ссылке | | | |

# Контрольная точка 8: Кейсы по кибербезопасности

Примените изученные понятия к реальным ситуациям ниже.

## КЕЙС 1: СДЕРЖИВАНИЕ ВРЕДОНОСНОЙ НАГРУЗКИ ПРОГРАММЫ-ВЫМОГАТЕЛЯ В КОМПАНИИ



**Ситуация: корпоративная локальная сеть заражена активной программой-вымогателем.** На ключевых файловых серверах начали появляться файлы с расширением .locked. Установите политики локализации.

**Вопрос для обсуждения:** Опишите шаги по локализации и протокол восстановления данных.

## КЕЙС 2: БЕСФАЙЛОВОЕ ВРЕДОНОСНОЕ ПО И ВНЕДРЕНИЕ В ПАМЯТЬ



**Ситуация:** Аналитик обнаруживает подозрительные скриптовые шаблоны, выполняющиеся прямо в энергозависимой оперативной памяти системы с помощью стандартных административных инструментов, но вредоносных файлов на диске нет.

**Вопрос для обсуждения:** Объясните стратегию анализа памяти и укажите инструменты для блокировки бесфайлового выполнения.

## 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

| 16 | 2 | 15 | 1 | 18 | 21 | 8 | 10 | 3 | 1 | 11 | 20 | 6 | | 21 | 4 | 18 | 16 | 9 | 29 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | |

| 17 | 16 | 3 | 6 | 5 | 6 | 15 | 25 | 6 | 19 | 12 | 10 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | |

| 14 | 16 | 15 | 10 | 20 | 16 | 18 | 10 | 15 | 4 | 16 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |

**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: Что такое вредоносное ПО?

Вредоносное ПО, созданное злоумышленниками, чтобы повреждать устройства и сети, захватывать над ними контроль или красть данные.

### Q2: В чём разница между вирусом и червём?

Вирусу для распространения нужны действия человека (например, открытие файла), а червь распространяется по сетям автоматически.

### Q3: Как троян заражает компьютер?

Обманывает пользователей, выдавая себя за безобидную или безопасную программу и скрывая внутри вредоносную нагрузку.

### Q4: Что такое программа-вымогатель?

Тип вредоносного ПО, которое шифрует файлы в целевой системе и требует деньги за ключ расшифровки. [1]

### Q5: Что такое шпионское ПО?

Вредоносное ПО, которое тайно записывает нажатия клавиш, пароли и привычки просмотра пользователя, чтобы отправлять их злоумышленникам.

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

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

### Q6: Что означает песочница (sandboxing)?

Запуск подозрительных файлов в защищённой изолированной виртуальной среде, чтобы наблюдать за их поведением без риска для рабочих систем.

### Q7: Что такое бесфайловое вредоносное ПО?

Вредоносное ПО, которое работает прямо в системной памяти (ОЗУ) с помощью легитимных утилит и не записывает файлы на диск, чтобы обойти простые сканеры.

### Q8: Как руткит защищает вредоносное ПО?

Скрывает вредоносные процессы и файлы, часто подменяя ядро операционной системы, поэтому антивирусные сканеры могут их пропустить.

### Q9: Что такое динамический мониторинг поведения?

Антивирусное сканирование, которое в реальном времени отслеживает активные процессы, чтобы блокировать действия, типичные для вредоносного ПО, например массовое шифрование файлов.

### Q10: Почему сдерживание так срочно при реагировании на инциденты?

Изоляция скомпрометированных конечных точек не позволяет активной вредоносной нагрузке распространяться на другие сетевые устройства.

# 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 разработчики вредоносного ПО обходят антивирусные сканеры на основе сигнатур?

Они используют полиморфизм: при каждом заражении меняют хеш и структуру кода файла, сохраняя то же вредоносное поведение.

### Q2: В чём риск инструментов двойного назначения в кампаниях с вредоносным ПО?

Злоумышленники используют легитимные административные инструменты (например, PowerShell или Sysinternals), чтобы сливаться с обычным сетевым трафиком, из-за чего обнаружить их трудно.

### Q3: Как process hollowing запускает вредоносную нагрузку?

Запускает легитимный системный процесс в приостановленном состоянии, подменяет его код в памяти вредоносным и возобновляет выполнение.

### Q4: Какую роль играет сервер управления и контроля (C2)?

Удалённый сервер, которым управляют хакеры, чтобы отправлять инструкции и вредоносные модули программам на скомпрометированных машинах.

### Q5: Почему кейлоггинг трудно обнаружить?

Простые кейлоггеры потребляют минимум ресурсов процессора и скрывают свои процессы внутри легитимных утилит пользовательского пространства.

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

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

### Q6: Как запутывание кода замедляет анализ вредоносных программ?

Шифрует или переставляет исходный код, делая его нечитаемым для инструментов аналитиков и сканеров безопасности.

### Q7: Каковы функции буткита?

Руткит, заражающий процесс загрузки (MBR, загрузочный сектор или прошивку UEFI), поэтому он запускается до загрузки операционной системы.

### Q8: Как эвристическое сканирование выявляет угрозы нулевого дня?

Ищет подозрительные шаблоны кода и административные команды, а не совпадающий хеш в базе данных.

### Q9: В чём угроза перехвата DLL (DLL hijacking)?

Принуждение легитимного приложения загрузить вредоносную динамически подключаемую библиотеку (DLL), размещённую в каталоге этого приложения.

### Q10: Как автоматизированные конвейеры анализа вредоносного ПО используют виртуализацию?

Они запускают подозрительные файлы на нескольких виртуальных машинах с разными ОС и автоматически создают журналы поведения и сетевые файлы PCAP.

## Часть 11: 10 реальных фактов и выводов о кибербезопасности

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

**1. АНАЛИЗ БЕЗОПАСНОСТИ**

Троянские кони остаются распространённым способом заражения, поскольку прячут вредоносный код в программах, выглядящих безобидно.

**2. АНАЛИЗ БЕЗОПАСНОСТИ**

IC3 ФБР получил в 2025 году более 3600 жалоб на программы-вымогатели, а заявленные потери превысили 32 миллиона долларов. [3]

**3. АНАЛИЗ БЕЗОПАСНОСТИ**

Черви могут быстро распространяться по сетям, используя непропатченные уязвимости протоколов, например EternalBlue в SMB.

**4. АНАЛИЗ БЕЗОПАСНОСТИ**

Бесфайловое вредоносное ПО трудно обнаружить, потому что оно работает в памяти через легитимные инструменты и оставляет на диске мало следов.

**5. АНАЛИЗ БЕЗОПАСНОСТИ**

Песочницы для анализа обычно возвращаются к чистому снимку после каждого запуска, чтобы каждый тест начинался с известного состояния.

**6. АНАЛИЗ БЕЗОПАСНОСТИ**

Руткиты могут изменять системные вызовы ядра, сообщая антивирусным сканерам ложные результаты диагностики.

**7. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ**

Обфускация кода использует утилиты-упаковщики для сжатия и сокрытия истинной структуры двоичной нагрузки вредоносного ПО.

**8. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ**

Полиморфное вредоносное ПО изменяет свой код, а значит и хеш файла, с каждой новой копией, чтобы обходить проверки сигнатур.

**9. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ**

Перехват DLL использует порядок поиска библиотек в стандартных операционных системах, например в Windows.

**10. АНАЛИЗ БЕЗОПАСНОСТИ**

Разработчики систем безопасности ежедневно обнаруживают огромное количество новых образцов вредоносного ПО, поэтому сигнатуры нужно постоянно обновлять.

# 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

[1] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

## Ответы: контрольная точка 1 – вопросы с выбором ответа

### 1 Вопрос 1

**Правильный ответ: A**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

В чём определяющая особенность троянского коня? → Маскируется под легальную программу, чтобы обманом заставить пользователей её запустить

### 2 Вопрос 2

**Правильный ответ: A**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Какой тип вредоносного ПО шифрует файлы и требует выкуп? → Программа-вымогатель

### 3 Вопрос 3

**Правильный ответ: A**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что представляет собой шпионское ПО? → Вредоносное ПО, предназначенное для скрытого отслеживания нажатий клавиш и действий пользователя в браузере

### 4 Вопрос 4

**Правильный ответ: A**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Зачем разработчики вредоносного ПО используют руткиты? → Чтобы скрыть активные процессы и вредоносные файлы от операционной системы

### 5 Вопрос 5

**Правильный ответ: A**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что означает песочница при анализе вредоносного ПО? → Запуск подозрительных файлов в изолированном виртуальном хранилище для безопасного наблюдения за поведением

## Ответы: контрольная точка 2 – верно или неверно

### 6 Вопрос 6

**Правильный ответ: Неверно**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: черви самовоспроизводятся и распространяются по сетям без каких-либо действий пользователя.

### 7 Вопрос 7

**Правильный ответ: Неверно**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: рекламное ПО не всегда безвредно; многие такие программы отслеживают просмотр сайтов для таргетинга рекламы.

### 8 Вопрос 8

**Правильный ответ: Верно**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Верно: чистые офлайн-резервные копии восстанавливают зашифрованные файлы без выплаты выкупа, хотя украденные данные всё равно могут утечь.

### 9 Вопрос 9

**Правильный ответ: Неверно**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: сигнатурным сканерам нужен известный образец, поэтому совершенно новое вредоносное ПО нулевого дня может проскользнуть мимо них.

### 10 Вопрос 10

**Правильный ответ: Верно**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Бесфайловое вредоносное ПО выполняет вредоносные скрипты в системной памяти, не записывая файлы на диск.

# 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. ТРОЯН | F 2. ПРОГРАММА-ВЫМОГАТЕЛЬ | A 3. ШПИОНСКОЕ ПО | H 4. РУТКИТ |
| G 5. ПЕСОЧНИЦА | C 6. СДЕРЖИВАНИЕ | E 7. WORM | B 8. БЕЗФАЙЛОВЫЙ |

## КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

| | | | |
|---|---|---|---|
| 1 ТРОЯН | 2 ВЫМОГАТЕЛЬ | 3 ШПИОНСКОЕ ПО | 4 РУТКИТ |
| 5 ПЕСОЧНИЦА | 6 ЛОКАЛИЗАЦИЯ | | |

## КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

| | | | |
|---|---|---|---|
| 1 D – РУТКИТ | 2 F – ЛОКАЛИЗАЦИЯ | 3 H – БЕЗФАЙЛОВЫЙ | 4 G – ЧЕРВЬ |
| 5 B – ВЫМОГАТЕЛЬ | 6 C – ШПИОНСКОЕПО | 7 A – ТРОЯН | 8 E – ПЕСОЧНИЦА |

## ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

**Ключевые термины:**
Проверьте, могут ли учащиеся своими словами объяснить ТРОЯН, ПРОГРАММА-ВЫМОГАТЕЛЬ и ШПИОНСКОЕ ПО и привести пример для каждого термина.

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

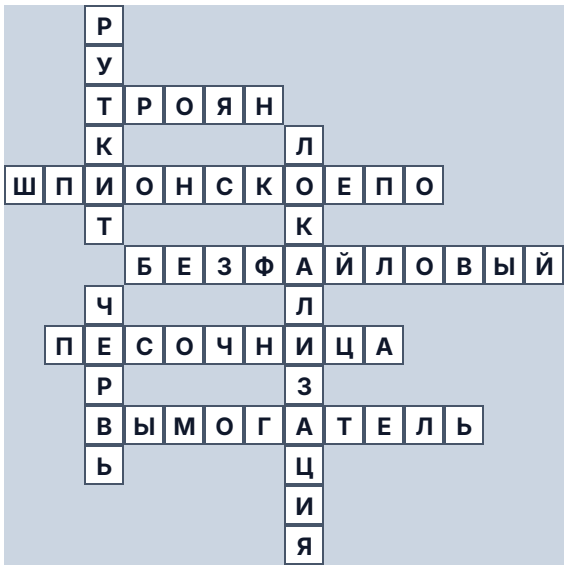
**Оценка источников:**
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

# Ключи к головоломкам и примечания для преподавателя

## РЕШЕНИЕ К ПОИСКУ СЛОВ

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

## РЕШЕНИЕ КРОССВОРДА




## РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

### ПО ГОРИЗОНТАЛИ

**2 по горизонтали: ТРОЯН** Вредоносная программа, замаскированная под безвредную или полезную утилиту. (5 букв)

**4 по горизонтали: ШПИОНСКОЕПО** Программа, предназначенная для тайного наблюдения за действиями пользователя и вводимыми данными и их записи. (11 букв)

**5 по горизонтали: БЕЗФАЙЛОВЫЙ** Вредоносный код, выполняемый прямо в ОЗУ, чтобы избежать обнаружения дисковыми сканерами. (11 букв)

**7 по горизонтали: ПЕСОЧНИЦА** Изолированная виртуальная среда для безопасного анализа вредоносных файлов. (9 букв)

**8 по горизонтали: ВЫМОГАТЕЛЬ** Вредоносная программа, шифрующая хранилище системы и требующая оплату за выдачу ключа. (10 букв)

### ПО ВЕРТИКАЛИ

**1 по вертикали: РУТКИТ** Скрытая вредоносная программа, засевшая глубоко в ядре системы, чтобы сохранять административный контроль. (6 букв)

**3 по вертикали: ЛОКАЛИЗАЦИЯ** Ограничение зараженных конечных узлов, чтобы не допустить распространения вредоносной нагрузки. (11 букв)

**6 по вертикали: ЧЕРВЬ** Самореплицирующаяся вредоносная программа, распространяющаяся по сетям без участия человека. (5 букв)

# Ключ к словам-перевёртышам и шифру

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

### КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. ЯОТНР — **ТРОЯН**
2. НОПШПСИЕОКО — **ШПИОНСКОЕПО**
3. ПНЧЕИАОЦС — **ПЕСОЧНИЦА**
4. РЬВЧЕ — **ЧЕРВЬ**
5. ЕАЬЫОТГВЛМ — **ВЫМОГАТЕЛЬ**
6. ИКРТТУ — **РУТКИТ**
7. АЛЛОЗЯЦИКИА — **ЛОКАЛИЗАЦИЯ**
8. ВЛЙЙЗБАЕЫОФ — **БЕЗФАЙЛОВЫЙ**

### КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

**"ОБНАРУЖИВАЙТЕ УГРОЗЫ ПОВЕДЕНЧЕСКИМ МОНИТОРИНГОМ"**

# Ответы к кейсам

## A Кейс 1: Сдерживание вредоносной нагрузки программы-вымогателя в компании

Решение для преподавателя

### РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

**В ответах студентов должны быть отражены следующие пункты:**

- Анализ ситуации: корпоративная локальная сеть взломана активной программой-вымогателем. На ключевых файловых серверах у файлов появились расширения .locked. Определите политики сдерживания.
- Рекомендуемая стратегия и решение: отключите все затронутые серверы от локальной сети. Завершите активные административные сеансы. Восстановите неповреждённые файлы из защищённой от записи автономной системы резервного копирования.

## B Кейс 2: Бесфайловое вредоносное ПО и внедрение в память

Решение для преподавателя

### РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

**В ответах студентов должны быть отражены следующие пункты:**

- Анализ ситуации: аналитик обнаруживает подозрительные скриптовые шаблоны, выполняющиеся прямо в энергозависимой оперативной памяти системы с помощью стандартных административных средств, но на диске нет вредоносных файлов.
- Рекомендуемая стратегия и решение: Изолируйте затронутые конечные точки и сначала снимите образ памяти. Просмотрите журналы PowerShell и WMI, заблокируйте неутверждённые скрипты с помощью AppLocker, затем перезагрузите систему, чтобы удалить вредоносную нагрузку.