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

Архитектура и безопасность нулевого доверия

Непрерывная проверка, микросегментация сети, управление идентификацией и доступом (IAM), минимальные привилегии и проверки состояния защиты.

ОБЗОР ОБУЧЕНИЯ ПО БЕЗОПАСНОСТИ НУЛЕВОГО ДОВЕРИЯ

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 архитектуру и безопасность Zero Trust. Вы изучите непрерывную проверку, микросегментацию сети, управление идентификацией и доступом (IAM), принцип наименьших привилегий и аудит сеансов.

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/zero-trust-kiberbezopasnost/

Ваша дорожная карта обучения: стратегия нулевого доверия

- Усвойте основной принцип непрерывной проверки.
- Внедрите микросегментацию сети и доступ по принципу наименьших привилегий.
- Настройте проверки состояния защиты устройств и активный аудит сеансов.

ИНСТРУКЦИИ К РУКОВОДСТВУ ПО БЕЗОПАСНОСТИ НУЛЕВОГО ДОВЕРИЯ

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: архитектуре Zero Trust. Завершите работу дополнительным заданием «Думай быстро».

АРХИТЕКТУРА И БЕЗОПАСНОСТЬ НУЛЕВОГО ДОВЕРИЯ (ВВЕДЕНИЕ)

Безопасность нулевого доверия заменяет старые модели периметра сети строгим принципом «никогда не доверяй, всегда проверяй». Микросегментация, управление идентификацией и доступом (IAM), права с минимально необходимыми привилегиями и проверки состояния устройств блокируют перемещение угроз внутри сети.

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

Контрольная точка 1: Задание с выбором ответа

1. В чём основной принцип безопасности Zero Trust?

- A. Никогда не доверять, всегда проверять каждый запрос доступа независимо от источника
- B. Предположение, что весь трафик внутри корпоративного межсетевого экрана безопасен
- C. Хранение файлов базы данных без шифрования для повышения скорости
- D. Принудительная аутентификация электронной почты только с помощью записей SPF

2. Что такое микросегментация сети?

- A. Разделение сетей на небольшие изолированные зоны для сдерживания горизонтального перемещения
- B. Шифрование сетевых карт при передаче данных
- C. Подключение всех локальных серверов к одному публичному IP-адресу
- D. Отслеживание нажатий клавиш пользователя в сеансах браузера

3. Что такое принцип наименьших привилегий?

- A. Ограничение прав доступа пользователя только тем, что необходимо для его работы
- B. Предоставление всех системных привилегий каждому пользователю по умолчанию
- C. Разрешение анонимного входа на серверы корпоративных баз данных
- D. Настройка общедоступных маршрутизаторов Wi-Fi без паролей

4. Что такое управление идентификацией и доступом (IAM)?

- A. Фреймворки для управления цифровыми идентификаторами и контроля системных привилегий
- B. Антивирусные утилиты, сканирующие локальные каталоги файлов
- C. Система резервного хранения на изолированных носителях (air-gapped)
- D. Протокол почтового шлюза, отклоняющий подменённые домены

5. Что означает непрерывная аутентификация?

- A. Многократная проверка личности пользователя и состояния устройства во время активного сеанса
- B. Смена мастер-пароля каждые 10 минут
- C. Хеширование записей базы данных несколькими алгоритмами
- D. Шифрование сетевых пакетов при передаче с помощью ключей TLS

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Нулевое доверие предполагает, что весь трафик внутри корпоративного межсетевого экрана безопасен.

○ Верно ○ Неверно

7 Вопрос 7

7. Микросегментация ограничивает возможность злоумышленников перемещаться по внутренним серверам.

○ Верно ○ Неверно

8 Вопрос 8

8. Принцип наименьших привилегий по умолчанию даёт доступ ко всем файлам базы данных.

○ Верно ○ Неверно

9 Вопрос 9

9. Непрерывная проверка подтверждает исправность устройства и учётные данные на протяжении всего сеанса входа.

○ Верно ○ Неверно

10 Вопрос 10

10. Внедрение нулевого доверия снижает последствия компрометации корпоративных логинов.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Требование учётных данных в каждой точке доступа — это непрерывная _____ .

2. Разделение корпоративной сети на мелкие зоны — это микро- _____ .

3. Настройка цифровых идентичностей и контроля доступа — это система « _____ доступом».

4. Принцип минимального доступа ограничивает права пользователей; такие права называются так: _____ .

5. Проверка исправности подключённых устройств сканирует _____ устройства.

6. Ведение и просмотр журналов активных сеансов — это проверка безопасности, или _____ .

СЛОВАРНЫЙ БАНК СЛОВ

АУДИТ БРАНДМАУЭР ВЕРИФИКАЦИЯ ПРИВИЛЕГИИ РОУТЕР
СЕГМЕНТАЦИЯ СОСТОЯНИЕ УПРАВЛЕНИЕ

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление понятий о безопасности

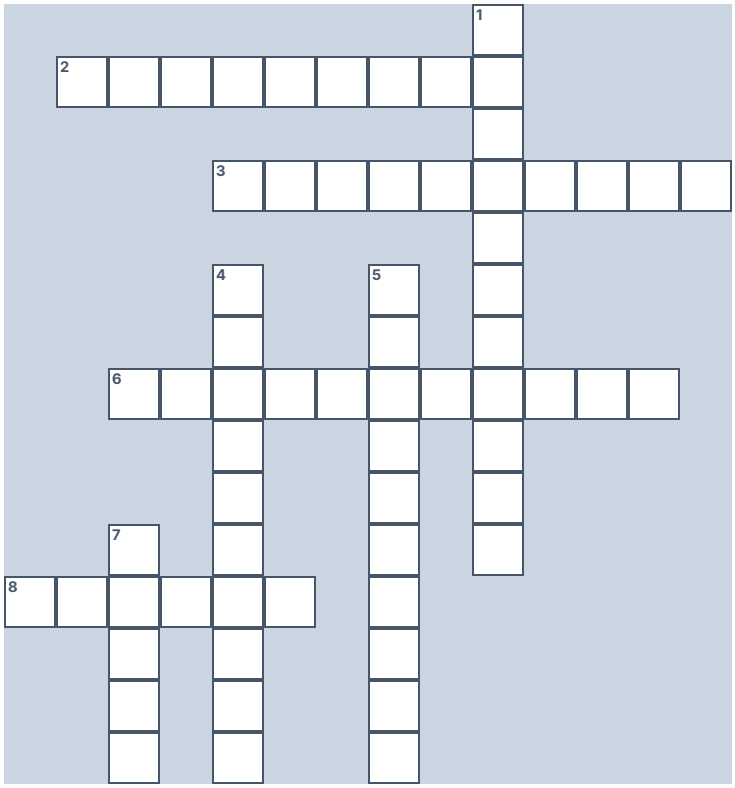
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. ПРОВЕРКА	A	Управление доступом к учётным данным пользователей.
☐	2. СЕГМЕНТАЦИЯ	B	Принцип наименьших прав доступа.
☐	3. IAM	C	Маршрутизация сетевых пакетов.
☐	4. ПРИВИЛЕГИЯ	D	Защита внешнего сетевого периметра.
☐	5. СОСТОЯНИЕ	E	Просмотр журналов сеансов доступа.
☐	6. АУДИТ	F	Разделение внутренних сетевых зон.
☐	7. БРАНДМАУЭР	G	Всегда проверяет учётные данные пользователя.
☐	8. МАРШРУТИЗАТОР	H	Оценка состояния устройства.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

2. Оценка исправности устройств. (9)

3. Защита внешнего периметра сети. (10)

6. Постоянная проверка учётных данных пользователей. (11)

8. Маршрутизация сетевых пакетов. (6)

ПО ВЕРТИКАЛИ

1. Разделение внутренних сетевых зон. (11)

4. Управление учётными данными и доступом пользователей. (10)

5. Принцип наименьших прав доступа. (10)

7. Просмотр журналов сеансов доступа. (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: Оценка исправности устройств. (9 букв):

3 по горизонтали: Защита внешнего периметра сети. (10 букв):

6 по горизонтали: Постоянная проверка учётных данных пользователей. (11 букв):

8 по горизонтали: Маршрутизация сетевых пакетов. (6 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Разделение внутренних сетевых зон. (11 букв):

4 по вертикали: Управление учётными данными и доступом пользователей. (10 букв):

5 по вертикали: Принцип наименьших прав доступа. (10 букв):

7 по вертикали: Просмотр журналов сеансов доступа. (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.

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

СПИСОК СЛОВ СЛОВАРЯ

ВЕРИФИКАЦИЯ СЕГМЕНТАЦИЯ УПРАВЛЕНИЕ ПРИВИЛЕГИИ СОСТОЯНИЕ
АУДИТ БРАНДМАУЭР РОУТЕР

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. ВЕРИФИКАЦИЯ

B. СЕГМЕНТАЦИЯ

C. УПРАВЛЕНИЕ

D. ПРИВИЛЕГИИ

E. СОСТОЯНИЕ

F. АУДИТ

G. БРАНДМАУЭР

H. РОУТЕР

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Защита внешнего периметра сети.

_____ 2. Просмотр журналов сеансов доступа.

_____ 3. Принцип наименьших прав доступа.

_____ 4. Разделение внутренних сетевых зон.

_____ 5. Маршрутизация сетевых пакетов.

_____ 6. Оценка исправности устройств.

_____ 7. Управление учётными данными и доступом пользователей.

_____ 8. Постоянная проверка учётных данных пользователей.

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. **ФКИЕИАВЦРЯИ** _____
2. **ИАУПВЕЕНЛР** _____
3. **СЯООНЕТИС** _____
4. **МЭДРНУАБРА** _____
5. **ЦЕАТГЯЕНСИМ** _____
6. **ИИВЕГПРЛИИ** _____
7. **ИТАДУ** _____
8. **УРРЕТО** _____

Дополнительное задание: Думай быстро

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

1	Информация, которой нельзя делиться			
2	Безопасные привычки, которые можно начать уже сегодня			
3	То, что проверяют на устройстве			
4	То, что записывается в журнал			
5	Слова, связанные с кибербезопасностью			
6	То, что проверяет Zero Trust			
7	Места, где в повседневной жизни показывают удостоверение личности			
8	Способы доказать, что это действительно вы			
9	Что делать после утечки данных			
10	Признаки заражения компьютера			
11	Причины обновлять программы			
12	Уровни доступа в компании			
13	Известные вам инструменты безопасности			
14	Зоны, на которые можно разделить сеть			
15	Поговорки о доверии			

Контрольная точка 8: Кейсы по кибербезопасности

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: ПЕРЕХОД НА СЕТЕВУЮ АРХИТЕКТУРУ НУЛЕВОГО ДОВЕРИЯ

👷

Ситуация: Крупная компания сейчас использует плоскую внутреннюю сеть, где любое устройство в локальной сети может получить доступ ко всем корпоративным серверам и базам данных.

Вопрос для обсуждения: Разработайте стратегию микросегментации сети, чтобы ограничить боковое перемещение.

КЕЙС 2: ВНЕДРЕНИЕ СРЕДСТВ КОНТРОЛЯ ДОСТУПА С МИНИМАЛЬНЫМИ ПРИВИЛЕГИЯМИ

👷

Ситуация: Журналы аудита показывают, что временные пользователи баз данных и сотрудники низкого уровня имеют глобальные права на чтение и запись в критически важных бухгалтерских базах данных.

Вопрос для обсуждения: Проведите аудит и ограничьте привилегии IAM базы данных, чтобы обеспечить принцип наименьших привилегий.

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

3	19	6	4	5	1		17	18	16	3	6	18	33	11	20	6		17	16

14	16	5	6	13	10		15	21	13	6	3	16	4	16

5	16	3	6	18	10	33

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 Zero Trust?

Нулевое доверие — концепция безопасности, предполагающая, что угрозы существуют как за пределами сети, так и внутри неё, и требующая проверки каждого запроса. [1]

Q2: Каково основное правило Zero Trust?

Никогда не доверяй, всегда проверяй.

Q3: Что такое микросегментация?

Разделение сети на небольшие защищённые логические сегменты для управления трафиком и локализации взломов.

Q4: Что такое принцип наименьших привилегий?

Предоставление пользователям только минимальных прав доступа, необходимых для выполнения их конкретных рабочих задач. [2]

Q5: Что означает IAM?

Управление идентификацией и доступом.

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

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q6: Чем помогает проверка состояния устройства?

Проверяет, что на устройстве установлены исправления, работает активный антивирус и оно безопасно, прежде чем разрешить доступ.

Q7: Что такое боковое перемещение?

Процесс, с помощью которого злоумышленники перемещаются по сети от первого взломанного узла к более ценным системам.

Q8: Заменяет ли модель нулевого доверия межсетевые экраны?

Нет, она усиливает их, добавляя проверки на основе идентичности и внутренние сегментирующие брандмауэры.

Q9: Что такое непрерывная аутентификация?

Постоянная проверка личности пользователя на протяжении всего активного сеанса входа, а не только при первом входе.

Q10: Почему плоская сеть опасна?

В плоских сетях один скомпрометированный узел позволяет злоумышленникам легко получить доступ к любой базе данных в сети.

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 Zero Trust решает проблему периметровой модели?

Заменяет устаревшую модель «замка с рвом», смещая защиту с периметра сети на конкретные идентичности пользователей и ресурсы.

Q2: Что такое точка принятия решений о политике (PDP)?

Компонент системы, который проверяет запросы авторизации по правилам безопасности и решает, предоставлять ли доступ.

Q3: Что такое точка применения политик (PEP)?

Системный узел (например, шлюз или прокси), который физически разрешает или блокирует запросы на подключение на основе решения PDP.

Q4: Как ролевое управление доступом (RBAC) поддерживает модель нулевого доверия?

RBAC группирует разрешения по определённым ролям, что помогает не допустить получения пользователями избыточных административных привилегий.

Q5: Что такое контекстное управление доступом?

Оценка запросов на вход с помощью дополнительных признаков, таких как географическое положение, состояние устройства и время входа, чтобы определить риск.

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

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

Q6: Чем микросегментация отличается от обычных VLAN?

VLAN делят сети на широкие логические сегменты на уровне 2, а микросегментация использует программные политики для изоляции отдельных рабочих нагрузок.

Q7: Что такое доступ точно в срок (JIT)?

Временное предоставление повышенных административных прав и их автоматический отзыв после завершения задачи.

Q8: Как защитить API в модели нулевого доверия?

Требуя криптографически подписанные токены OAuth и проверяя подписи запросов на каждом шлюзе API.

Q9: Что такое клиент доступа к сети с нулевым доверием (ZTNA)?

Программный агент, устанавливающий защищённые зашифрованные исходящие соединения с определёнными приложениями, а не с необработанными сетевыми подсетями.

Q10: Как аудит журналов помогает Zero Trust?

Непрерывное журналирование позволяет автоматизированным инструментам аналитики безопасности выявлять аномалии и немедленно приостанавливать подозрительные входы.

Часть 11: 10 реальных фактов и выводов о кибербезопасности

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

1. АНАЛИЗ БЕЗОПАСНОСТИ

Архитектуры нулевого доверия заменяют устаревшую модель «замок и ров» правилами проверки, ориентированными на идентификацию.

2. АНАЛИЗ БЕЗОПАСНОСТИ

Микросегментация сети уменьшает область, до которой может добраться вредоносное ПО, изолируя рабочие нагрузки в небольших защищённых зонах.

3. АНАЛИЗ БЕЗОПАСНОСТИ

Нулевое доверие направлено на защиту ресурсов, таких как активы, службы и учётные записи, а не сегментов сети. [1]

4. АНАЛИЗ БЕЗОПАСНОСТИ

Политики доступа по принципу наименьших привилегий снижают риск утечки данных из основных баз данных по вине внутренних нарушителей.

5. АНАЛИЗ БЕЗОПАСНОСТИ

Проверка состояния устройства в реальном времени проверяет уровень обновлений операционной системы и состояние активного антивируса.

6. АНАЛИЗ БЕЗОПАСНОСТИ

Брокеры доступа к сети с нулевым доверием (ZTNA) могут заменять или дополнять корпоративные VPN, чтобы ограничивать область доступа пользователей.

7. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Делегирование административных привилегий «точно в срок» (JIT) снижает риск кражи учётных данных на контроллерах домена.

8. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Непрерывная проверка журналирует и проверяет поведение сеанса, приостанавливая работу пользователей с аномальными шаблонами выполнения скриптов.

9. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Традиционная защита периметра не блокирует боковые атаки после утечки административных учётных данных.

10. АНАЛИЗ БЕЗОПАСНОСТИ

Специальная публикация NIST 800-207 (2020) даёт абстрактное определение архитектуры Zero Trust с моделями развёртывания. [1]

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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

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

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

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 Вопрос 1

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

В чём основной принцип безопасности Zero Trust? → Никогда не доверять, всегда проверять каждый запрос доступа независимо от источника

2 Вопрос 2

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что такое микросегментация сети? → Разделение сетей на небольшие изолированные зоны для сдерживания горизонтального перемещения

3 Вопрос 3

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что такое принцип наименьших привилегий? → Ограничение прав доступа пользователя только тем, что необходимо для его работы

4 Вопрос 4

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что такое управление идентификацией и доступом (IAM)? → Фреймворки для управления цифровыми идентификаторами и контроля системных привилегий

5 Вопрос 5

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что означает непрерывная аутентификация? → Многократная проверка личности пользователя и состояния устройства во время активного сеанса

Ответы: контрольная точка 2 – верно или неверно

6 **Вопрос 6** — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: Zero Trust не предоставляет неявного доверия на основе местоположения в сети, внутри или снаружи.

7 **Вопрос 7** — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Верно: небольшие изолированные зоны ограничивают, насколько далеко злоумышленник может продвинуться между серверами.

8 **Вопрос 8** — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: принцип наименьших привилегий даёт только минимальный доступ, необходимый каждой роли.

9 **Вопрос 9** — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Непрерывная проверка подтверждает исправность устройства и учётные данные на протяжении всего сеанса входа.

10 **Вопрос 10** — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Внедрение нулевого доверия снижает последствия компрометации корпоративных логинов.

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

G 1. ПРОВЕРКА	F 2. СЕГМЕНТАЦИЯ	A 3. IAM	B 4. ПРИВИЛЕГИЯ
H 5. СОСТОЯНИЕ	E 6. АУДИТ	D 7. БРАНДМАУЭР	C 8. МАРШРУТИЗАТОР

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 ВЕРИФИКАЦИЯ	2 СЕГМЕНТАЦИЯ	3 УПРАВЛЕНИЕ	4 ПРИВИЛЕГИИ
5 СОСТОЯНИЕ	6 АУДИТ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 G – БРАНДМАУЭР	2 F – АУДИТ	3 D – ПРИВИЛЕГИИ	4 B – СЕГМЕНТАЦИЯ
5 H – РОУТЕР	6 E – СОСТОЯНИЕ	7 C – УПРАВЛЕНИЕ	8 A – ВЕРИФИКАЦИЯ

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить ПРОВЕРКА, СЕГМЕНТАЦИЯ и IAM и привести пример для каждого термина.

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

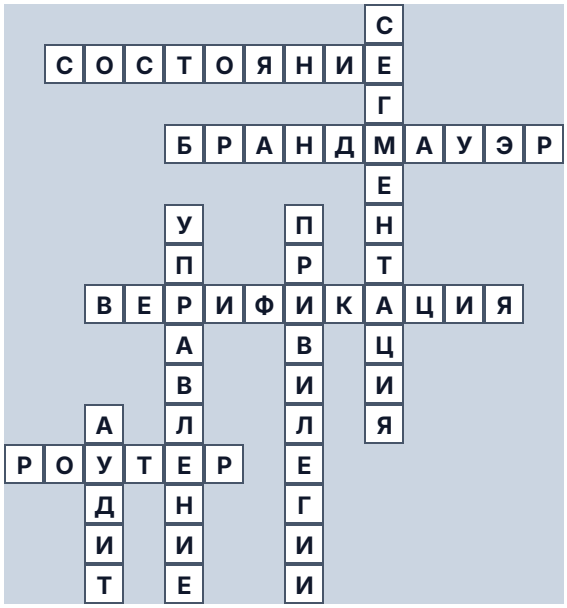
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

2 по горизонтали: СОСТОЯНИЕ Оценка исправности устройств. (9 букв)

3 по горизонтали: БРАНДМАУЭР Защита внешнего периметра сети. (10 букв)

6 по горизонтали: ВЕРИФИКАЦИЯ Постоянная проверка учётных данных пользователей. (11 букв)

8 по горизонтали: РОУТЕР Маршрутизация сетевых пакетов. (6 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: СЕГМЕНТАЦИЯ Разделение внутренних сетевых зон. (11 букв)

4 по вертикали: УПРАВЛЕНИЕ Управление учётными данными и доступом пользователей. (10 букв)

5 по вертикали: ПРИВИЛЕГИИ Принцип наименьших прав доступа. (10 букв)

7 по вертикали: АУДИТ Просмотр журналов сеансов доступа. (5 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. ФКИЕИАВЦРЯИ — **ВЕРИФИКАЦИЯ**
2. ИАУПВЕЕНЛР — **УПРАВЛЕНИЕ**
3. СЯООНЕТИС — **СОСТОЯНИЕ**
4. МЭДРНУАБРА — **БРАНДМАУЭР**
5. ЦЕАТГЯЕНСИМ — **СЕГМЕНТАЦИЯ**
6. ИИВЕГПРЛИИ — **ПРИВИЛЕГИИ**
7. ИТАДУ — **АУДИТ**
8. УРРЕТО — **РОУТЕР**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ВСЕГДА ПРОВЕРЯЙТЕ ПО МОДЕЛИ НУЛЕВОГО ДОВЕРИЯ"

Ответы к кейсам

A Кейс 1: Переход на сетевую архитектуру нулевого доверия

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: крупное предприятие сейчас использует плоскую внутреннюю сеть, где любое устройство локальной сети может получить доступ ко всем корпоративным серверам и базам данных.
- Рекомендуемая стратегия и решение: Разделите плоскую сеть на изолированные зоны подразделений. Установите внутренние межсетевые экраны для контроля трафика между зонами и обязательную проверку токена соединения при любом доступе.

B Кейс 2: Внедрение средств контроля доступа с минимальными привилегиями

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: журналы аудита показывают, что временные пользователи базы данных и рядовые сотрудники имеют глобальные права на чтение и запись в критически важных бухгалтерских базах данных.
- Рекомендуемая стратегия и решение: Отзовите все глобальные административные привилегии. Внедрите управление доступом на основе ролей (RBAC), соответствующее конкретным должностям, и настройте еженедельные автоматические проверки разрешений.