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

Основы кибербезопасности и онлайн-угрозы Предотвращение

Киберугрозы, сетевые межсетевые экраны, многофакторная аутентификация, системы безопасности

ОБЗОР ОБУЧЕНИЯ: ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

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 основные принципы кибербезопасности и предотвращения онлайн-угроз. Вы изучите вредоносное ПО, многофакторную аутентификацию, сетевые межсетевые экраны и фреймворки реагирования на инциденты.

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/

Ваша дорожная карта обучения: основы кибербезопасности

- Определите распространённые векторы вредоносного ПО, фишинга и вторжения в корпоративную сеть.
- Внедрите стандартные меры кибербезопасности, включая MFA, брандмауэры и защиту конечных точек.
- Оцените процедуры реагирования на инциденты для смягчения последствий утечек данных.
- Проанализируйте организационные факторы риска и соответствие требованиям безопасности по рекомендациям NIST.
- Настройте практики цифровой гигиены, снижающие риск автоматизированного подбора учётных данных.

ИНСТРУКЦИИ ПО КИБЕРБЕЗОПАСНОСТИ

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: предотвращению угроз. Завершите работу дополнительным заданием «Думай быстро».

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ И ПРЕДОТВРАЩЕНИЕ УГРОЗ (ВВЕДЕНИЕ)

Кибербезопасность защищает сети, системы и данные от несанкционированных цифровых атак. Формирование надёжных привычек безопасности, настройка межсетевых экранов, требование многофакторной аутентификации и обучение сотрудников распознаванию угроз — важнейшие составляющие защиты корпоративной сети.

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

Контрольная точка 1: Задание с выбором ответа

1. Какова главная цель фишинговой атаки?

- A. Кража учётных данных и конфиденциальных данных пользователей
- B. Повышение видимости сайта в поисковых системах
- C. Увеличение пропускной способности сети
- D. Управление репликацией резервного центра обработки данных

2. Какой механизм обеспечивает самую надёжную защиту аккаунта?

- A. Многофакторная аутентификация с аппаратными ключами
- B. Сложные пароли, обновляемые каждые тридцать дней
- C. Ограничение входа в аккаунт рабочими часами
- D. Скрытие имени пользователя аккаунта из публичных каталогов

3. Что определяет полезную нагрузку заражения программой-вымогателем?

- A. Шифрование системных файлов и требование оплаты
- B. Скрытая запись нажатий клавиш и отправка на удалённые серверы
- C. Внедрение несанкционированной рекламы в браузеры
- D. Использование ресурсов локального процессора для майнинга криптовалюты

4. Как эксплойт нулевого дня влияет на защитные механизмы?

- A. Нацелена на неисправленные, неизвестные уязвимости
- B. Он автоматически отключает корпоративный межсетевой экран
- C. Заставляет систему выполнить жёсткую перезагрузку
- D. Для устранения не требуется никакого бюджета

5. Какая система стандартов регулирует корпоративные меры безопасности?

- A. Рекомендации NIST Cybersecurity Framework
- B. Спецификации схемы документов W3C HTML5
- C. Руководства по установке драйверов принтера
- D. Определения протоколов маршрутизации IETF

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос «верно/неверно» 6

6. Фишинговые атаки нацелены только на личные адреса электронной почты.

○ Верно ○ Неверно

7 Вопрос «верно/неверно» 7

7. Многофакторная аутентификация помогает блокировать атаки подстановки учётных данных.

○ Верно ○ Неверно

8 Вопрос «верно/неверно» 8

8. Брандмауэры проверяют сетевой трафик, чтобы блокировать несанкционированный доступ к портам.

○ Верно ○ Неверно

9 Вопрос «верно/неверно» 9

9. Устранение эксплойтов нулевого дня требует стандартных обновлений определений антивируса.

○ Верно ○ Неверно

10 Вопрос «верно/неверно» 10

10. Honeypot — это сервер-приманка, используемый для привлечения киберпреступников.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Сетевые администраторы устанавливают _____ для фильтрации входящего трафика.

2. Атакующий применяет _____ нулевого дня, чтобы обойти исправления в системе.

3. Злоумышленники рассылают поддельные письма сотрудникам, проводя атаки типа « _____ ».

4. Программа-вымогатель блокирует данные пользователя и относится к разрушительной категории — _____ .

5. Строгая парольная _____ снижает риски кражи учётных данных.

6. Для защиты конфиденциальных сообщений пользователи применяют защитные протоколы, основанные на технологии, называемой: _____ .

СЛОВАРНЫЙ БАНК СЛОВ

БРАНДМАУЭР ВРЕДОНОСНОЕ ПО ГИГИЕНА МНОГОФАКТОРНАЯ РЕАГИРОВАНИЕ ФИШИНГ ШИФРОВАНИЕ ЭКСПЛОЙТ

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление понятий о безопасности

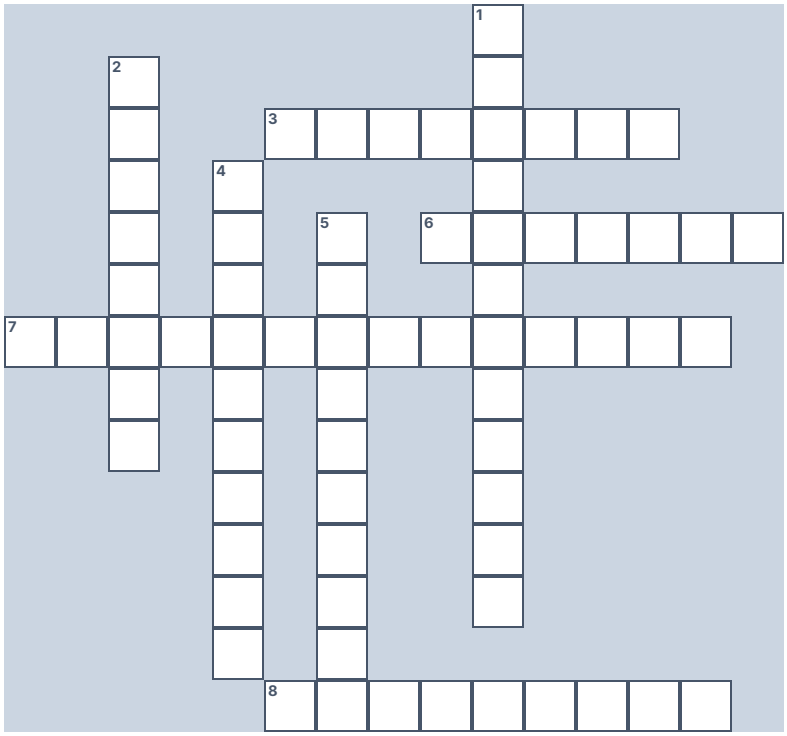
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. Угроза программ-вымогателей	A	Структурированные рекомендации, например NIST, используемые для управления киберрисками.
☐	2. Многофакторная аутентификация	B	Структурированный план обработки и смягчения последствий нарушений безопасности.
☐	3. Эксплойт нулевого дня	C	Сетевой барьер, фильтрующий трафик по правилам безопасности.
☐	4. Ловушка-приманка	D	Вредоносное ПО, шифрующее данные и требующее денежную выплату за расшифровку.
☐	5. Межсетевой экран защиты от вторжений	E	Эксплойт уязвимости, используемый до выхода исправления от разработчика.
☐	6. Реагирование на инциденты	F	Лучшие практики управления учётными данными и ключами аутентификации.
☐	7. Гигиена паролей	G	Проверка безопасности, требующая двух или более факторов аутентификации.
☐	8. Фреймворк безопасности	H	Система-приманка, созданная для заманивания и изучения злоумышленников.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

3. Система-ловушка, созданная, чтобы привлекать и изучать злоумышленников (8)

6. Лучшие практики управления учётными данными и ключами аутентификации (7)

7. Проверка безопасности, требующая двух или более факторов аутентификации (14)

8. Структурированные рекомендации вроде NIST для управления киберрисками (9)

ПО ВЕРТИКАЛИ

1. Структурированный план обработки и смягчения последствий нарушений безопасности (12)

2. Использование уязвимости до выпуска исправления вендором (8)

4. Вредоносная программа, шифрующая данные и требующая денежную оплату за расшифровку (10)

5. Сетевой барьер, фильтрующий трафик по правилам безопасности (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

3 по горизонтали: Система-ловушка, созданная, чтобы привлекать и изучать злоумышленников (8 букв):

6 по горизонтали: Лучшие практики управления учётными данными и ключами аутентификации (7 букв):

7 по горизонтали: Проверка безопасности, требующая двух или более факторов аутентификации (14 букв):

8 по горизонтали: Структурированные рекомендации вроде NIST для управления киберрисками (9 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Структурированный план обработки и смягчения последствий нарушений безопасности (12 букв):

2 по вертикали: Использование уязвимости до выпуска исправления вендором (8 букв):

4 по вертикали: Вредоносная программа, шифрующая данные и требующая денежную оплату за расшифровку (10 букв):

5 по вертикали: Сетевой барьер, фильтрующий трафик по правилам безопасности (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.

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

СПИСОК СЛОВ СЛОВАРЯ

ВЫМОГАТЕЛЬ · МНОГОФАКТОРНАЯ · ЭКСПЛОЙТ · ПРИМАНКА · БРАНДМАУЭР · РЕАГИРОВАНИЕ · ГИГИЕНА · ФРЕЙМВОРК

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. ВЫМОГАТЕЛЬ**
- **B. МНОГОФАКТОРНАЯ**
- **C. ЭКСПЛОЙТ**
- **D. ПРИМАНКА**
- **E. БРАНДМАУЭР**
- **F. РЕАГИРОВАНИЕ**
- **G. ГИГИЕНА**
- **H. ФРЕЙМВОРК**

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Сетевой барьер, фильтрующий трафик по правилам безопасности.

_____ 2. Структурированный план обработки и смягчения последствий нарушений безопасности.

_____ 3. Вредоносная программа, шифрующая данные и требующая денежную оплату за расшифровку.

_____ 4. Проверка безопасности, требующая двух или более факторов аутентификации.

_____ 5. Лучшие практики управления учётными данными и ключами аутентификации.

_____ 6. Структурированные рекомендации вроде NIST для управления киберрисками.

_____ 7. Использование уязвимости до выпуска исправления вендором.

_____ 8. Система-ловушка, созданная, чтобы привлекать и изучать злоумышленников.

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. ЛТАГЫВЕЬОМ
2. ПЭТКЙОЛС
3. БМЭАРДРНУА
4. АИЕИНГГ
5. ООННКТОЯФРАМАГ
6. КАМНПАРИ
7. ВАИРЕОЕНИАРГ
8. КМРФЙРВОЕ

Дополнительное задание: Думай быстро

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

1	Профессии в кибербезопасности			
2	Причины обновлять программы			
3	То, что может блокировать межсетевой экран			
4	Тревожные признаки в электронном письме			
5	То, для чего вы делаете резервные копии			
6	Известные виды кибератак			
7	То, что может привлечь ханипот			
8	Информация, которой нельзя делиться			
9	Признаки заражения компьютера			
10	Фильмы или сериалы о хакерах			
11	Уровни защиты, которые можно выстроить			
12	То, что отрабатывают на учениях по безопасности			
13	Известные вам инструменты безопасности			
14	Люди, у которых можно попросить помощи по ИТ			
15	Слова, которые начинаются на «кибер»			

Контрольная точка 8: Кейсы по кибербезопасности

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: СТРАТЕГИЯ ВОССТАНОВЛЕНИЯ ПОСЛЕ ПРОГРАММЫ-ВЫМОГАТЕЛЯ



Ситуация: Корпоративная сеть заражена программой-вымогателем, которая заблокировала критически важные базы данных. Злоумышленники требуют выкуп в криптовалюте в размере $100,000. У компании есть офлайн-резервные копии 24-часовой давности.

Вопрос для обсуждения: проанализируйте риски выплаты выкупа и оцените стратегию восстановления.

КЕЙС 2: ЗАЩИТА ОТ ПОДБОРА УЧЁТНЫХ ДАННЫХ



Ситуация: Онлайн-сервис подвергается атаке подстановки учётных данных: хакеры проверяют миллионы пар «имя пользователя — пароль», украденных на других сайтах.

Вопрос для обсуждения: Опишите механизм этой атаки и перечислите две системы защиты.

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

9	1	27	10	20	10	20	6		19	10	19	20	6	14	21

14	15	16	4	16	22	1	12	20	16	18	15	16	11

1	21	20	6	15	20	10	22	10	12	1	24	10	6	11

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: Какова главная цель кибербезопасности?

Главная цель — защита сетей, устройств и данных от несанкционированного доступа, атак и случайного ущерба.

Q2: Чем фишинг отличается от целевого фишинга (spear phishing)?

Фишинг — это массовая рассылка писем случайным пользователям, а целевой фишинг (spear phishing) нацелен на конкретных людей с использованием персонализированных данных.

Q3: Что такое сетевой межсетевой экран?

Межсетевой экран — это система сетевой безопасности, которая отслеживает и фильтрует входящий и исходящий трафик по заранее заданным правилам безопасности.

Q4: Почему необходима многофакторная аутентификация (MFA)?

MFA добавляет важный уровень защиты и не даёт получить доступ, даже если злоумышленники украдут или взломают основные учётные данные с паролем.

Q5: Что определяет компьютерный вирус?

Вирус — это самовоспроизводящееся вредоносное ПО, которое прикрепляется к чистым файлам и распространяется по системам после запуска.

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

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q6: Как программа-вымогатель блокирует локальные данные?

Программа-вымогатель использует криптографические алгоритмы для шифрования пользовательских файлов, делая их нечитаемыми, пока не будет применён ключ расшифровки.

Q7: Что такое уязвимость нулевого дня?

Уязвимость нулевого дня — это изъян безопасности в программе, неизвестный разработчику, поэтому до эксплуатации нет времени на создание исправления.

Q8: Какую роль играет фреймворк NIST?

Рамочная программа NIST предлагает добровольные рекомендации и стандарты, помогающие организациям управлять рисками кибербезопасности и снижать их.

Q9: Что такое план реагирования на инциденты безопасности?

Это документированный набор процедур для обнаружения, локализации и восстановления после нарушений безопасности и компрометации сети.

Q10: Как социальная инженерия использует пользователей?

Социальная инженерия использует психологическое манипулирование, чтобы обманом заставить сотрудников раскрыть пароли или скачать вредоносные файлы.

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 DDoS-атака перегружает веб-серверы?

DDoS-атака координирует миллионы заражённых устройств ботнета, чтобы завалить сервер трафиком и исчерпать пропускную способность и ресурсы процессора.

Q2: В чём разница между симметричным и асимметричным шифрованием?

Симметричное шифрование использует один ключ для шифрования и расшифровки, а асимметричное — пару из открытого и закрытого ключей.

Q3: Как хакеры проводят атаки с SQL-инъекциями?

Злоумышленники вводят вредоносные SQL-команды в поля форм, заставляя серверную базу данных выдавать несанкционированные записи пользователей.

Q4: Что такое боковое перемещение при вторжениях в сеть?

Это приём, при котором злоумышленники используют первоначальный доступ к серверу, чтобы скомпрометировать другие связанные системы во внутренней сети.

Q5: Как подмена DNS перенаправляет веб-трафик?

Подмена DNS изменяет записи кеша сервера имён и направляет обычных пользователей на вредоносные сайты-двойники вместо нужных доменов.

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 аппаратный токен безопасности?

Это физическое устройство (например, YubiKey), генерирующее криптографические подтверждения аутентификации и обеспечивающее максимальную защиту от удалённого фишинга.

Q7: Как специалисты по безопасности используют ловушки-приманки (honeypot)?

Команды развёртывают непроизводственные серверы-приманки, чтобы на ранней стадии обнаруживать вторжения и анализировать модели атак несанкционированных лиц.

Q8: Что такое принцип наименьших привилегий?

Это стандарт безопасности, ограничивающий права доступа пользователей абсолютным минимумом, необходимым для выполнения их рабочих ролей.

Q9: Как атака «человек посередине» использует соединения?

Злоумышленник перехватывает и изменяет связь между двумя устройствами в незашифрованных сетях, похищая токены сеансов и учётные данные.

Q10: Что такое индикаторы компрометации (IOC)?

IOC — это криминалистические улики в данных, например необычные изменения реестра или подозрительный IP-трафик, показывающие, что систему взломали.

Часть 11: 10 реальных фактов и выводов о кибербезопасности

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

1. АНАЛИЗ БЕЗОПАСНОСТИ

Злоумышленники постоянно сканируют интернет в поисках уязвимых серверов и рассылают фишинговые письма на почтовые ящики сотрудников.

2. АНАЛИЗ БЕЗОПАСНОСТИ

Человеческая ошибка, например переход по фишинговым ссылкам, — частый фактор утечек данных, поэтому обучение важно.

3. АНАЛИЗ БЕЗОПАСНОСТИ

Затраты на утечку данных включают юридические штрафы, отток клиентов, расследование и устранение последствий и могут достигать миллионов долларов.

4. АНАЛИЗ БЕЗОПАСНОСТИ

Устойчивая к фишингу MFA, например аппаратные ключи безопасности, — самый надёжный тип MFA и стандарт, к которому призывает CISA. [2]

5. АНАЛИЗ БЕЗОПАСНОСТИ

Программы-вымогатели остаются серьёзной угрозой для корпоративных сетей, а CISA рекомендует автономные зашифрованные резервные копии как ключевую защиту. [4]

6. АНАЛИЗ БЕЗОПАСНОСТИ

В NIST Cybersecurity Framework 2.0 (2024) шесть основных функций: Govern (управление), Identify (выявление), Protect (защита), Detect (обнаружение), Respond (реагирование), Recover (восстановление). [1]

7. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Боты для подбора учётных данных в массовом порядке проверяют утёкшие пары имени пользователя и пароля на порталах входа банков и интернет-магазинов.

8. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Рынки эксплойтов нулевого дня существуют по всему миру: уязвимости высокой степени опасности могут продаваться за крупные суммы до выпуска исправлений.

9. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Система-приманка honeypot сразу сообщает о вторжении, поскольку у обычных пользователей нет причин обращаться к ней.

10. АНАЛИЗ БЕЗОПАСНОСТИ

Transport Layer Security (TLS) шифрует сеансы браузера и предотвращает перехват пакетов в общедоступных сетях Wi-Fi.

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. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] 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

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

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

[6] 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

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

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 **Фишинговые атаки** ФИШИНГ — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Фишинговые кампании пытаются украсть учётные данные и конфиденциальные данные пользователей с помощью поддельных писем. Источник: OWASP Secure Configuration.

2 **Защита аккаунта** КЛЮЧ MFA — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Многофакторная аутентификация (MFA) с аппаратными токенами обеспечивает самую надёжную защиту доступа к аккаунту. Источник: NIST Digital Identity.

3 **Угроза программ-вымогателей** ПРОГРАММА-ВЫМОГАТЕЛЬ — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Программа-вымогатель шифрует критически важные системы и данные и требует оплаты в криптовалюте за ключи расшифровки. Источник: Center for Internet Security (CIS).

4 **Уязвимость нулевого дня** НУЛЕВОГО ДНЯ — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Угрозы нулевого дня используют неисправленные, неизвестные уязвимости безопасности до выпуска производителем исправления. Источник: OWASP Secure Configuration.

5 **Модели безопасности** ФРЕЙМВОРКИ — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Такие стандарты, как NIST, содержат структурированные рекомендации, которые помогают организациям управлять киберрисками и снижать их. Источник: NIST Digital Identity.

Ответы: контрольная точка 2 – верно или неверно

6 **Целевой фишинг** ФИШИНГ — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Фишинговые атаки нацелены как на корпоративные сети, так и на личные учётные записи, расширяя векторы эксплуатации. Источник: OWASP Secure Configuration.

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

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

MFA требует второго фактора, поэтому одного украденного пароля обычно недостаточно для входа.

8 **Межсетевой экран трафика** БРАНДМАУЭР — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Брандмауэры проверяют трафик на определённых сетевых портах и блокируют его, отсеивая несанкционированные подключения. Источник: Center for Internet Security (CIS).

9 **Реагирование на уязвимости нулевого дня** НУЛЕВОГО ДНЯ — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Устранение уязвимостей нулевого дня требует исправлений кода и фильтрации WAF, так как сигнатур для них ещё нет. Источник: OWASP Secure Configuration.

10 **Ловушки-приманки** ХАНИПОТ — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Honeypot — это обманные серверы, которые команды безопасности используют, чтобы заманивать, оповещать и изучать злоумышленников. Источник: Center for Internet Security (CIS).

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. Угроза программ-вымогателей	G 2. Многофакторная аутентификация	E 3. Эксплойт нулевого дня	H 4. Ловушка-приманка
C 5. Межсетевой экран защиты от вторжений	B 6. Реагирование на инциденты	F 7. Гигиена паролей	A 8. Фреймворк безопасности

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 БРАНДМАУЭР	2 ЭКСПЛОЙТ	3 ФИШИНГ	4 ВРЕДОНОСНОЕ ПО
5 ГИГИЕНА	6 ШИФРОВАНИЕ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 E – БРАНДМАУЭР	2 F – РЕАГИРОВАНИЕ	3 A – ВЫМОГАТЕЛЬ	4 B – МНОГОФАКТОРНАЯ
5 G – ГИГИЕНА	6 H – ФРЕЙМВОРК	7 C – ЭКСПЛОЙТ	8 D – ПРИМАНКА

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить Угроза программ-вымогателей, Многофакторная аутентификация и Эксплойт нулевого дня и привести пример для каждого термина.

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

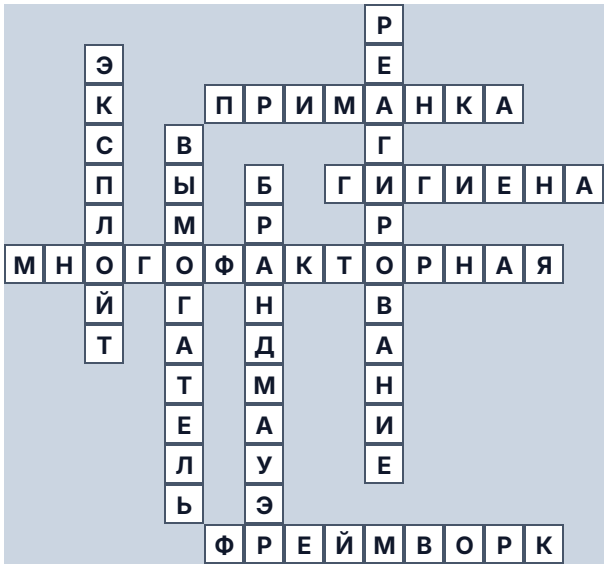
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

3 по горизонтали: ПРИМАНКА Система-ловушка, созданная, чтобы привлекать и изучать злоумышленников (8 букв)

6 по горизонтали: ГИГИЕНА Лучшие практики управления учётными данными и ключами аутентификации (7 букв)

7 по горизонтали: МНОГОФАКТОРНАЯ Проверка безопасности, требующая двух или более факторов аутентификации (14 букв)

8 по горизонтали: ФРЕЙМВОРК Структурированные рекомендации вроде NIST для управления киберрисками (9 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: РЕАГИРОВАНИЕ Структурированный план обработки и смягчения последствий нарушений безопасности (12 букв)

2 по вертикали: ЭКСПЛОЙТ Использование уязвимости до выпуска исправления вендором (8 букв)

4 по вертикали: ВЫМОГАТЕЛЬ Вредоносная программа, шифрующая данные и требующая денежную оплату за расшифровку (10 букв)

5 по вертикали: БРАНДМАУЭР Сетевой барьер, фильтрующий трафик по правилам безопасности (10 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. ЛТАГЫВЕЬОМ — **ВЫМОГАТЕЛЬ**
2. ПЭТКЙОЛС — **ЭКСПЛОЙТ**
3. БМЭАРДРНУА — **БРАНДМАУЭР**
4. АИЕИНГГ — **ГИГИЕНА**
5. ООННКТОЯФРАМАГ — **МНОГОФАКТОРНАЯ**
6. КАМНПАРИ — **ПРИМАНКА**
7. ВАИРЕОЕНИАРГ — **РЕАГИРОВАНИЕ**
8. КМРФЙРВОЕ — **ФРЕЙМВОРК**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ЗАЩИТИТЕ СИСТЕМУ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИЕЙ"

Ответы к кейсам

A Кейс 1: Стратегия восстановления после программы-вымогателя

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: корпоративная сеть заражена программой-вымогателем, заблокированы критические базы данных. Злоумышленники требуют выкуп в криптовалюте на сумму $100,000. У компании есть автономные резервные копии 24-часовой давности.
- Рекомендуемая стратегия и решение: Риски выплаты: выплата не гарантирует расшифровку файлов, помечает компанию как платящую цель и финансирует преступную деятельность. Стратегия восстановления: команде следует изолировать заражённые узлы, очистить скомпрометированные серверы и восстановить данные из автономных резервных копий. Необходимо закрыть первоначальный вектор проникновения (фишинг или эксплойт), чтобы предотвратить немедленное повторное заражение.

B Кейс 2: Защита от подбора учётных данных

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: онлайн-сервис подвергается атаке методом подстановки учётных данных: хакеры проверяют миллионы пар «имя пользователя — пароль», украденных с других сайтов.
- Рекомендуемая стратегия и решение: Механизм: злоумышленники используют повторное применение паролей на разных сайтах и с помощью автоматических ботов входят в аккаунты пользователей. Защита: 1. Многофакторная аутентификация (MFA) блокирует попытки входа, даже если пароль верный. 2. Ограничение частоты запросов и CAPTCHA блокируют автоматический трафик ботов, засыпающий конечные точки входа.