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

Утечки паролей и безопасность учётных данных

Подбор учётных данных, утечки данных, алгоритмы хеширования, многофакторная аутентификация и безопасность паролей.

ОБЗОР ОБУЧЕНИЯ: УТЕЧКИ ПАРОЛЕЙ

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 утечки паролей и безопасность учётных данных. Вы изучите подстановку учётных данных (credential stuffing), утечки данных, алгоритмы хеширования, многофакторную аутентификацию и менеджеры паролей.

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/utechka-parolej/

Ваша дорожная карта обучения: безопасность паролей

- Разберитесь в рисках раскрытия учётных данных на форумах даркнета.
- Внедрите многофакторную аутентификацию (MFA) и мониторинг скомпрометированных учётных данных.
- Разработайте корпоративную защиту от целевых мошеннических схем социальной инженерии.

ИНСТРУКЦИИ К РУКОВОДСТВУ ПО УТЕЧКАМ ПАРОЛЕЙ

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: защите учётных данных. Завершите работу дополнительным заданием «Думай быстро».

УТЕЧКИ ПАРОЛЕЙ И БЕЗОПАСНОСТЬ УЧЁТНЫХ ДАННЫХ (ВВЕДЕНИЕ)

Утечки паролей раскрывают учётные данные пользователей на общедоступных сайтах и в даркнете. Уникальные пароли из менеджера паролей, проверка на скомпрометированные пароли и многофакторная аутентификация (MFA) снижают риск подбора учётных данных, а хеширование паролей с солью и замедлением ограничивает ущерб при краже базы паролей.

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

Контрольная точка 1: Задание с выбором ответа

1. Что такое подстановка учётных данных (credential stuffing)?

- A. Использование автоматизации для проверки утёкших сочетаний логина и пароля на нескольких сайтах
- B. Шифрование локальных файлов хранилища баз данных
- C. Перегрузка веб-серверов запросами сетевого трафика
- D. Скрытое отслеживание ввода с клавиатуры

2. Какой алгоритм OWASP сегодня указывает первым выбором для хранения паролей?

- A. Argon2id
- B. MD5
- C. SHA-1
- D. ROT13

3. Как многофакторная аутентификация (MFA) снижает риск утечки паролей?

- A. Она требует дополнительного фактора проверки, поэтому одного украденного пароля недостаточно
- B. Она автоматически меняет пароль каждый час
- C. Она шифрует имя пользователя при передаче
- D. Она оповещает кредитное бюро о мошеннических запросах

4. Что такое дамп данных утечки?

- A. Набор утёкших учётных данных пользователей, опубликованный в сети или продаваемый на хакерских форумах
- B. Резервная копия файлов базы данных, хранящаяся вне площадки
- C. Временный кэш журналов веб-сервера
- D. Административный инструмент для сброса паролей пользователей

5. Какова роль менеджера паролей?

- A. Создание и хранение уникальных надёжных паролей для каждого аккаунта
- B. Мониторинг сетевого трафика на предмет утечек паролей
- C. Блокировка автоматических атак методом подбора на шлюзе
- D. Сканирование блоков хранения базы данных на наличие незашифрованных паролей

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Повторное использование паролей в нескольких аккаунтах повышает риск подстановки учётных данных.

○ Верно ○ Неверно

7 Вопрос 7

7. SHA-1 — рекомендуемая хеш-функция для хранения паролей в современных системах.

○ Верно ○ Неверно

8 Вопрос 8

8. Одни лишь требования к сложности пароля (без MFA) полностью останавливают подстановку учётных данных.

○ Верно ○ Неверно

9 Вопрос 9

9. Инструменты мониторинга тёмного веба сканируют интернет в поисках скомпрометированных корпоративных учётных данных.

○ Верно ○ Неверно

10 Вопрос 10

10. Хеши с солью добавляют к паролям уникальные случайные данные перед хешированием, что противодействует атакам с радужными таблицами.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Проверка утёкших учётных данных во многих веб-приложениях — это _____ учётных данных.

2. Медленный адаптивный алгоритм хеширования паролей, который по-прежнему допускает OWASP, — это _____ .

3. Раскрытие конфиденциальных файлов баз данных в интернете — это _____ .

4. Добавление случайных значений к паролям перед хешированием называется _____ .

5. Защищённая локальная база данных учётных данных пользователя — это парольный _____ .

6. Добавление второго шага проверки при входе — это _____ аутентификация.

СЛОВАРНЫЙ БАНК СЛОВ

БИКРИПТ МЕНЕДЖЕР МНОГОФАКТОРНАЯ ПОДСТАНОВКА РАДУЖНАЯ СОЛЕНИЕ УТЕЧКА ДАННЫХ ФИШИНГ

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление понятий о безопасности

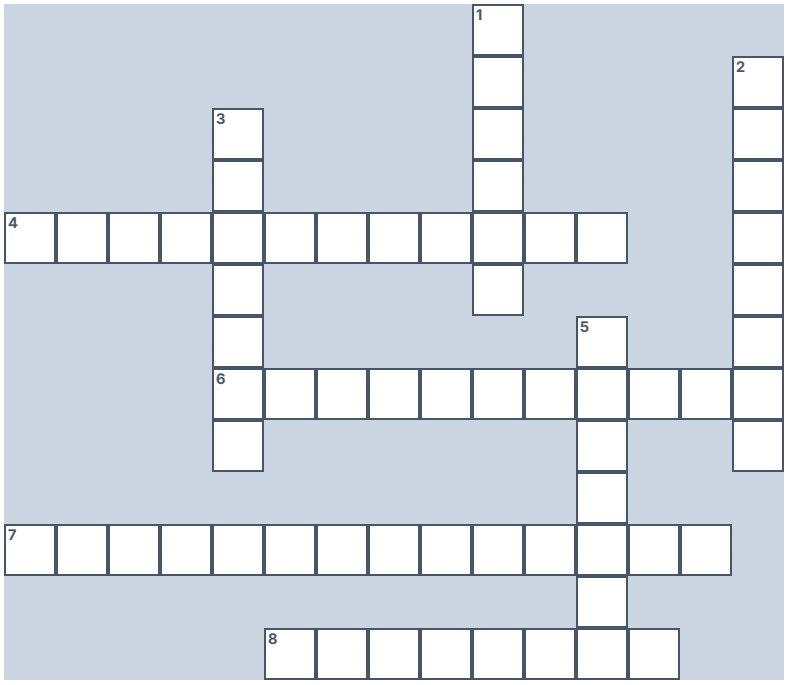
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. ПОДСТАНОВКА	A	Заранее вычисленная таблица хешей паролей.
☐	2. BCRYPT	B	Многофакторная проверка входа.
☐	3. УТЕЧКА	C	Инструмент хранения учётных данных.
☐	4. ДОБАВЛЕНИЕ СОЛИ	D	Несанкционированное раскрытие базы данных.
☐	5. МЕНЕДЖЕР	E	Социальная инженерия с целью кражи учётных данных.
☐	6. MFA	F	Проверка утёкших учётных данных.
☐	7. РАДУЖНАЯ ТАБЛИЦА	G	Добавление случайной соли к хешу пароля.
☐	8. ФИШИНГ	H	Медленный алгоритм хеширования паролей.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

4. Несанкционированное раскрытие базы данных. (12)

6. Проверка утёкших учётных данных. (11)

7. Многофакторная проверка при входе. (14)

8. Инструмент хранения учётных данных. (8)

ПО ВЕРТИКАЛИ

1. Социальная инженерия для кражи логинов. (6)

2. Заранее рассчитанная таблица хешей паролей. (8)

3. Медленный алгоритм хеширования паролей. (7)

5. Добавление случайной соли к хешу пароля. (7)

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

4 по горизонтали: Несанкционированное раскрытие базы данных. (12 букв):

6 по горизонтали: Проверка утёкших учётных данных. (11 букв):

7 по горизонтали: Многофакторная проверка при входе. (14 букв):

8 по горизонтали: Инструмент хранения учётных данных. (8 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Социальная инженерия для кражи логинов. (6 букв):

2 по вертикали: Заранее рассчитанная таблица хешей паролей. (8 букв):

3 по вертикали: Медленный алгоритм хеширования паролей. (7 букв):

5 по вертикали: Добавление случайной соли к хешу пароля. (7 букв):

Контрольная точка 6: Поиск скрытых слов

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

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

СПИСОК СЛОВ СЛОВАРЯ

ПОДСТАНОВКА · БИКРИПТ · УТЕЧКАДАННЫХ · СОЛЕНИЕ · МЕНЕДЖЕР · МНОГОФАКТОРНАЯ · РАДУЖНАЯ · ФИШИНГ

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. ПОДСТАНОВКА**
- **B. БИКРИПТ**
- **C. УТЕЧКАДАННЫХ**
- **D. СОЛЕНИЕ**
- **E. МЕНЕДЖЕР**
- **F. МНОГОФАКТОРНАЯ**
- **G. РАДУЖНАЯ**
- **H. ФИШИНГ**

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

1. Социальная инженерия для кражи логинов.
2. Несанкционированное раскрытие базы данных.
3. Медленный алгоритм хеширования паролей.
4. Заранее рассчитанная таблица хешей паролей.
5. Проверка утёкших учётных данных.
6. Добавление случайной соли к хешу пароля.
7. Инструмент хранения учётных данных.
8. Многофакторная проверка при входе.

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. ТНКОАОПВДАС _____

2. ХТКАУНЫЕАНДЧ _____

3. ЕЕМДЖРЕН _____

4. УАЯНЖРАД _____

5. ИТРКБПИ _____

6. ИЛНСЕЕО _____

7. РАОМТНОЯФНКГАО _____

8. ШГФНИИ _____

Дополнительное задание: Думай быстро

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

1	Безопасные привычки, которые можно начать уже сегодня			
2	Правила надёжного пароля			
3	Известные вам менеджеры паролей			
4	Известные вам инструменты безопасности			
5	Тревожные признаки в электронном письме			
6	Забавные слова для длинной парольной фразы			
7	Способы входа без пароля			
8	Информация, которой нельзя делиться			
9	Причины обновлять программы			
10	Что делать, когда пароль утёк			
11	Аккаунты, которым нужна MFA			
12	Места, где пароли нельзя хранить ни в коем случае			
13	Признаки заражения компьютера			
14	Плохие пароли, которые используют люди			
15	То, для чего вы делаете резервные копии			

Контрольная точка 8: Кейсы по кибербезопасности

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: УСТРАНЕНИЕ УТЕЧКИ КОРПОРАТИВНЫХ УЧЁТНЫХ ДАННЫХ

👷

Ситуация: Служба мониторинга даркнета предупреждает организацию, что в интернете опубликован дамп базы данных с паролями корпоративных системных администраторов.

Вопрос для обсуждения: Проанализируйте риски утечки учётных данных и предложите административную стратегию сброса.

КЕЙС 2: ВНЕДРЕНИЕ СТАНДАРТОВ ХЕШИРОВАНИЯ ПАРОЛЕЙ

👷

Ситуация: В корпоративной базе данных пароли пользователей пока хранятся в виде устаревших хешей MD5 без криптографической соли, что делает их уязвимыми для быстрого извлечения.

Вопрос для обсуждения: Разработайте стратегию миграции для перехода базы данных на более современный алгоритм хеширования.

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		21	20	6	12	26	10	6

17	1	18	16	13	10

14	15	16	4	16	22	1	12	20	16	18	15	29	14

3	23	16	5	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 утечка пароля?

Утечка паролей происходит, когда учётные данные пользователей раскрываются из-за утечек данных или неправильной настройки серверов.

Q2: Как хакеры находят утёкшие пароли?

Хакеры просматривают форумы даркнета, публичные дампы баз данных и сайты вставки текста (paste-сайты), где публикуются данные утечек [8].

Q3: Опасно ли использовать один пароль повторно?

Да, потому что, если один сайт взломан, хакеры могут проверить те же учётные данные на тысячах других платформ [3].

Q4: Что такое криптографическая соль?

Соль — это случайные данные, добавляемые к паролю перед хешированием, что делает атаки по заранее вычисленным таблицам неэффективными [2].

Q5: Почему MD5 устарел?

MD5 — это быстрый устаревший хеш общего назначения, поэтому злоумышленники могут проверять догадки о паролях крайне быстро, особенно если хеши не посолены [2].

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

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q6: Как менеджер паролей защищает пользователей?

Автоматически генерирует сложные уникальные учётные данные для каждого сайта, снижая количество человеческих ошибок памяти и повторное использование паролей.

Q7: Что такое атака полным перебором?

Атака, систематически перебирающая все возможные сочетания символов, пока не будет найден верный пароль [4].

Q8: Чем помогает блокировка учётной записи?

Блокировка или ограничение частоты замедляет повторный подбор онлайн и в сочетании с мониторингом и MFA снижает риск перебора [4].

Q9: Надёжны ли мастер-пароли?

Они безопасны, если это парольные фразы с высокой энтропией, которые никогда не используются повторно в других веб-системах.

Q10: Нужно ли регулярно менять пароли?

NIST советует не требовать периодической смены; меняйте пароли при признаках компрометации и отдавайте приоритет длине, спискам блокировки и MFA [1].

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

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

Q1: Чем Argon2 отличается от bcrypt?

OWASP называет Argon2id первым выбором: его настройки с интенсивным использованием памяти лучше противостоят взлому на GPU и ASIC, чем bcrypt [2].

Q2: Что такое растяжение ключа (key stretching)?

Приём, при котором алгоритм хеширования выполняется в цикле тысячи раз, чтобы замедлить проверку пароля и сделать взлом дорогостоящим [2].

Q3: Как работают радужные таблицы?

Это заранее вычисленные таблицы поиска, связывающие открытые пароли с их хешами; их используют для быстрого обращения хешей без соли [2].

Q4: Что такое повторное использование учётных данных?

Повторное использование украденных пар имени пользователя и пароля из одной утечки для попыток доступа к другим сервисам, особенно там, где люди повторно использовали пароли [3].

Q5: Можно ли взломать менеджеры паролей?

Да. Многие используют шифрование с нулевым разглашением, поэтому при взломе сервера раскрываются только зашифрованные хранилища, но слабые мастер-пароли всё равно можно подобрать офлайн.

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 атака по словарю?

Вариант подбора паролей, который проверяет распространённые слова, фразы и ранее утёкшие пароли, а не случайные буквы.

Q7: Почему парольные фразы предпочтительнее?

Парольные фразы состоят из нескольких случайных слов, что создаёт высокую энтропию: людям их легко запомнить, а подобрать вычислительно дорого [1].

Q8: Как единый вход (SSO) влияет на утечки паролей?

SSO сокращает разрастание паролей, но поставщик удостоверений становится ценной целью и нуждается в надёжной, желательно устойчивой к фишингу MFA [6].

Q9: Что такое перехват сеанса?

Злоумышленник получает или злоупотребляет действующим токеном сеанса, чтобы выдавать себя за вошедшего в систему пользователя, не вводя пароль повторно [5].

Q10: Как обнаружить подбор паролей (password spraying)?

Выявляя одни и те же немногие пароли, перебираемые во многих учётных записях, часто медленно, чтобы не превысить пороги блокировки [7].

Часть 11: 10 реальных фактов и выводов о кибербезопасности

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

1. АНАЛИЗ БЕЗОПАСНОСТИ

NIST SP 800-63B требует проверять новые пароли по спискам блокировки распространённых и скомпрометированных паролей [1].

2. АНАЛИЗ БЕЗОПАСНОСТИ

Дамп «Collection #1» 2019 года объединил данные из многих более ранних утечек в один огромный файл с парами «адрес электронной почты — пароль» [8].

3. АНАЛИЗ БЕЗОПАСНОСТИ

NIST теперь требует, чтобы пароли, используемые как единственный фактор аутентификации, были не короче 15 символов [1].

4. АНАЛИЗ БЕЗОПАСНОСТИ

ASIC-оборудование способно вычислять миллиарды хешей SHA-256 в секунду, поэтому необработанное хеширование SHA небезопасно для паролей пользователей [2].

5. АНАЛИЗ БЕЗОПАСНОСТИ

Уникальная соль означает, что у двух пользователей с одинаковым паролем в базе данных будут разные хеши [2].

6. АНАЛИЗ БЕЗОПАСНОСТИ

Многие менеджеры паролей локально шифруют данные хранилища стойкой криптографией, ключ для которой получают из мастер-пароля пользователя.

7. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Подбор учётных данных работает потому, что многие люди используют один и тот же пароль в интернет-магазинах, банках и почтовых аккаунтах [3].

8. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

NIST SP 800-63B говорит, что верификаторы не должны требовать периодической смены паролей, а только их смену при наличии признаков компрометации [1].

9. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Добавление одной заглавной буквы и символа в короткий пароль не защищает от современных автоматизированных атак по словарю на GPU [1].

10. АНАЛИЗ БЕЗОПАСНОСТИ

MFA может блокировать многие попытки подстановки учётных данных, даже если пароль утёк; MFA, устойчивая к фишингу, надёжнее SMS-кодов [3].

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. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[2] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

[3] OWASP. (n.d.). Credential Stuffing Prevention Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Credential_Stuffing_Prevention_Cheat_Sheet.html

[4] OWASP. (n.d.). Authentication Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[5] OWASP. (n.d.). Session Management Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[6] CISA. (2022). Implementing Phishing-Resistant MFA (fact sheet).

https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[7] CISA. (2018). Brute Force Attacks Conducted by Cyber Actors (Alert TA18-086A).

https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors

[8] Hunt, T. (2019). The 773 Million Record "Collection #1" Data Breach. Troy Hunt.

https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 Вопрос 1

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Подстановка учётных данных использует автоматизацию, чтобы пробовать утёкшие пары «имя пользователя/пароль» на других сайтах [3].

2 Вопрос 2

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

OWASP рекомендует в первую очередь Argon2id; bcrypt нужен главным образом для устаревших систем, где Argon2id или scrypt недоступны [2].

3 Вопрос 3

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

MFA требует дополнительного фактора, поэтому одного украденного пароля недостаточно, чтобы разблокировать аккаунт [3].

4 Вопрос 4

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Дампы утечек — это коллекции утёкших учётных данных, например сборник Collection #1 2019 года [8].

5 Вопрос 5

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Менеджер паролей создаёт и хранит уникальный надёжный пароль для каждого аккаунта, предотвращая повторное использование [3].

Ответы: контрольная точка 2 – верно или неверно

6 Вопрос 6

Правильный ответ: Верно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Верно: повторно используемые пароли позволяют злоумышленникам применять учётные данные, утёкшие с одного сайта, на других сайтах [3].

7 Вопрос 7

Правильный ответ: Неверно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: SHA-1 — быстрая хеш-функция; OWASP рекомендует вместо неё Argon2id, scrypt, bcrypt или PBKDF2 [2].

8 Вопрос 8

Правильный ответ: Неверно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: одних правил сложности недостаточно, чтобы остановить подстановку утёкших повторно используемых паролей; нужна MFA [3].

9 Вопрос 9

Правильный ответ: Верно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Верно: сервисы мониторинга ищут в дампах утечек и источниках даркнета раскрытые учётные данные [8].

10 Вопрос 10

Правильный ответ: Верно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Верно: уникальная соль для каждого пароля делает предвычисленные радужные таблицы неэффективными [2].

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

F 1. ПОДСТАНОВКА	H 2. BCRYPT	D 3. УТЕЧКА	G 4. ДОБАВЛЕНИЕ СОЛИ
C 5. МЕНЕДЖЕР	B 6. MFA	A 7. РАДУЖНАЯ ТАБЛИЦА	E 8. ФИШИНГ

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 ПОДСТАНОВКА	2 БИКРИПТ	3 УТЕЧКА ДАННЫХ	4 СОЛЕНИЕ
5 МЕНЕДЖЕР	6 МНОГОФАКТОРНАЯ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 H – ФИШИНГ	2 C – УТЕЧКАДАННЫХ	3 B – БИКРИПТ	4 G – РАДУЖНАЯ
5 A – ПОДСТАНОВКА	6 D – СОЛЕНИЕ	7 E – МЕНЕДЖЕР	8 F – МНОГОФАКТОРНАЯ

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить ПОДСТАНОВКА, BCRYPT и УТЕЧКА и привести пример для каждого термина.

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

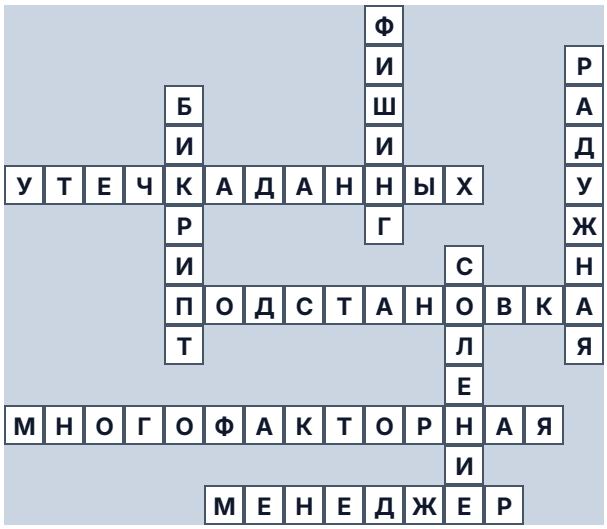
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

4 по горизонтали: УТЕЧКАДАННЫХ
Несанкционированное раскрытие базы данных. (12 букв)

6 по горизонтали: ПОДСТАНОВКА Проверка утёкших учётных данных. (11 букв)

7 по горизонтали: МНОГОФАКТОРНАЯ Многофакторная проверка при входе. (14 букв)

8 по горизонтали: МЕНЕДЖЕР Инструмент хранения учётных данных. (8 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: ФИШИНГ Социальная инженерия для кражи логинов. (6 букв)

2 по вертикали: РАДУЖНАЯ Заранее рассчитанная таблица хешей паролей. (8 букв)

3 по вертикали: БИКРИПТ Медленный алгоритм хеширования паролей. (7 букв)

5 по вертикали: СОЛЕНИЕ Добавление случайной соли к хешу пароля. (7 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. ТНКОАОПВДАС — **ПОДСТАНОВКА**
2. ХТКАУНЫЕАНДЧ — **УТЕЧКАДАННЫХ**
3. ЕЕМДЖРЕН — **МЕНЕДЖЕР**
4. УАЯНЖРАД — **РАДУЖНАЯ**
5. ИТРКБПИ — **БИКРИПТ**
6. ИЛНСЕЕО — **СОЛЕНИЕ**
7. РАОМТНОЯФНКГАО — **МНОГОФАКТОРНАЯ**
8. ШГФНИИ — **ФИШИНГ**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ЗАЩИТИТЕ УТЕКШИЕ ПАРОЛИ МНОГОФАКТОРНЫМ ВХОДОМ"

Ответы к кейсам

A Кейс 1: Устранение утечки корпоративных учётных данных

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: сервис мониторинга даркнета предупреждает организацию, что в сети опубликован дамп базы данных с паролями системных администраторов компании.
- Рекомендуемая стратегия и решение: Отзовите все активные сеансы администраторов и сбросьте учётные данные с помощью генератора высокой энтропии. Включите устойчивую к фишингу MFA на порталах администрирования [6], смените затронутые ключи API, просмотрите журналы входа, найдите первоначальную точку утечки и проверьте другие привилегированные аккаунты.

B Кейс 2: Внедрение стандартов хеширования паролей

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: корпоративная база данных хранит пароли пользователей в виде устаревших хешей MD5 без криптографической соли, что делает их уязвимыми для быстрого извлечения.
- Рекомендуемая стратегия и решение: перейдите на Argon2id (или bcrypt в устаревших системах) с уникальной солью для каждого пользователя [2]. Сразу оберните существующие хеши MD5 в новый алгоритм, пересчитывайте хеш напрямую при следующем входе каждого пользователя и принудительно сбрасывайте пароли у давно неактивных учётных записей.