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

# Предотвращение кражи личных данных и защита активов Руководство по безопасности

**Утечки учётных данных, MFA, мониторинг даркнета, оповещения о заморозке кредитной истории, социальная инженерия**

## ОБЗОР ЦЕЛЕЙ ОБУЧЕНИЯ: ПРЕДОТВРАЩЕНИЕ КРАЖИ ЛИЧНЫХ ДАННЫХ

**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 предотвращение кражи личных данных и снижение её последствий. Вы изучите утечки учётных данных, многофакторную аутентификацию, мониторинг даркнета, оповещения о заморозке кредита и защиту от социальной инженерии.

### 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/krazha-lichnosti/

# Ваша дорожная карта обучения: защита личности

- Разберитесь в рисках раскрытия учётных данных на форумах даркнета.
- Внедрите многофакторную аутентификацию (MFA) и оповещения о заморозке кредитной истории.
- Разработайте корпоративную защиту от целевых мошеннических схем социальной инженерии.

## ИНСТРУКЦИИ К РУКОВОДСТВУ ПО КРАЖЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

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 личности. Завершите работу дополнительным заданием «Думай быстро».

## ПРЕДОТВРАЩЕНИЕ КРАЖИ ЛИЧНЫХ ДАННЫХ И ЗАЩИТА АКТИВОВ (ВВЕДЕНИЕ)

Кража личных данных использует утёкшие учётные данные и слабые логины для перехвата личных и корпоративных аккаунтов. Использование MFA, заморозки кредитной истории, сканеров даркнета и систем SPF/DKIM/DMARC образует важнейшую защиту от цифровой подмены личности.

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

## Контрольная точка 1: Задание с выбором ответа

**1. Какой способ чаще всего используют похитители личных данных, чтобы украсть логины и пароли?**

- A. Рассылка поддельных уведомлений по электронной почте, чтобы обманом заставить пользователей вводить пароли на подменённых порталах
- B. Прослушивание радиопередач рядом с корпоративным офисом пользователя
- C. Дефрагментация локального диска хранилища пользовательского сервера
- D. Отключение внешних конфигураций резервного копирования по сети

**2. Какая мера безопасности обеспечивает самую надёжную защиту от утечек учётных данных?**

- A. Многофакторная аутентификация с аппаратными ключами
- B. Создание длинных паролей в форматах браузера по умолчанию
- C. Смена имён пользователей электронной почты каждые шесть месяцев
- D. Удаление сохранённых историй браузера с отслеживанием cookie

**3. Что представляет собой заморозка кредитной истории?**

- A. Блокировка кредитных отчётов, чтобы злоумышленники не могли оформлять несанкционированные займы
- B. Удаление истории банковских транзакций из баз данных
- C. Отключение магнитных считывателей кредитных карт на сканерах
- D. Шифрование локальных жёстких дисков с базами данных при хранении

**4. Чем полезен мониторинг даркнета?**

- A. Предупреждает пользователей, если их утёкшие учётные данные появляются в нелегальных базах данных
- B. Он не позволяет активному вредоносному ПО запускаться в виртуальных песочницах
- C. Ускоряет маршрутизацию в браузере в виртуальных сетях
- D. Блокирует попытки доступа к серверной базе данных через SQL-инъекции

**5. Что означает социальная инженерия?**

- A. Манипулирование людьми, чтобы они добровольно раскрыли конфиденциальные учётные данные
- B. Сканирование портов корпоративных серверов на наличие активных эксплойтов безопасности
- C. Резервное копирование файлов системных баз данных на автономные жёсткие диски
- D. Маршрутизация сетевых пакетов через три зашифрованных узла onion

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

**6 Вопрос 6**

6. Кража личных данных затрагивает только цифровые онлайн-аккаунты, но не физическую почтовую корреспонденцию.

○ Верно ○ Неверно

**7 Вопрос 7**

7. Обязательная MFA для всех личных аккаунтов блокирует большинство ботов-атак подстановки учётных данных.

○ Верно ○ Неверно

**8 Вопрос 8**

8. Заморозка кредитной истории блокирует кредитные проверки, но не даёт вам получить доступ к собственному банковскому счёту.

○ Верно ○ Неверно

**9 Вопрос 9**

9. Менеджеры паролей защищают пользователей от фишинга, отказываясь автоматически подставлять пароли на поддельных доменах.

○ Верно ○ Неверно

**10 Вопрос 10**

10. Фишинговые письма часто используют срочные формулировки, чтобы вызвать эмоциональную и быструю реакцию.

○ Верно ○ Неверно

## Контрольная точка 3: Вставьте ключевые термины

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

**1. Похитители личности нацелены на пользовательские пароли и другие сведения для входа — _____ .**

**2. Уведомления о взломах баз данных обнаруживают частные _____ аккаунтов.**

**3. Требование временного кода для входа — это _____ аутентификация.**

**4. Поиск украденных данных на хакерских форумах в даркнете — это _____ .**

**5. Чтобы заблокировать несанкционированные запросы кредитной истории, нужна кредитная _____ .**

**6. В организации, где сотрудников учат распознавать фишинг, формируется активная _____ безопасности.**

**СЛОВАРНЫЙ БАНК СЛОВ**

ЗАМОРОЗКА ЗАЩИТА УТЕЧКИ МНОГОФАКТОРНАЯ УЧЁТНЫЕ ДАННЫЕ МОНИТОРИНГ ФИШИНГ СПУФИНГ

**Напишите свои ответы здесь:**

**1.** 

**2.** 

**3.** 

**4.** 

**5.** 

**6.** 

# Контрольная точка 4: Сопоставление понятий о безопасности

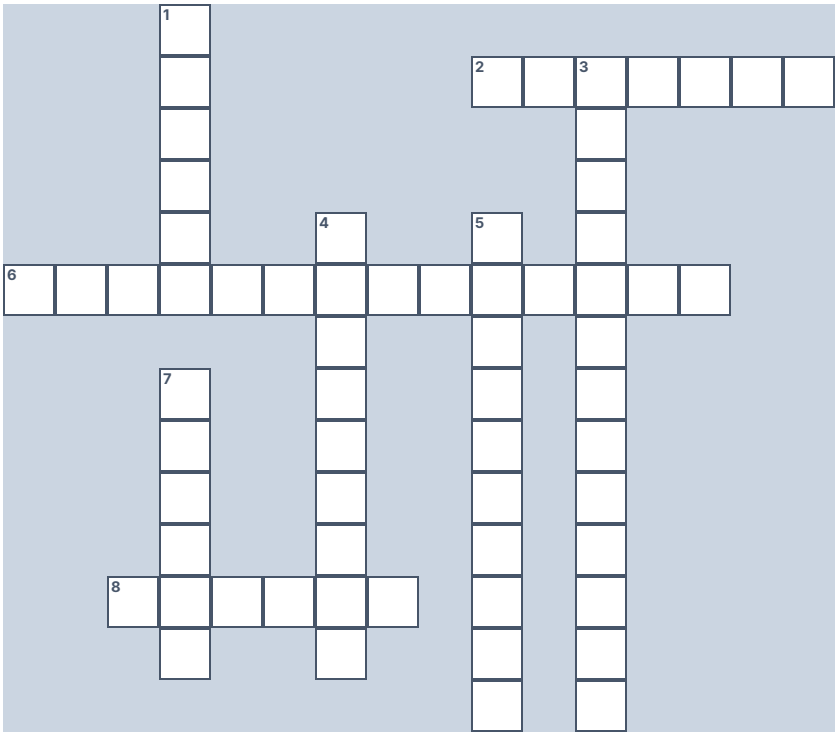
## СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

| | | | |
|---|---|---|---|
| ☐ | 1. УЧЁТНЫЕ ДАННЫЕ | **A** | Дополнительный шаг проверки (например, аппаратные ключи), защищающий вход в учётную запись. |
| ☐ | 2. УТЕЧКИ | **B** | Создание поддельного сайта или письма, имитирующего настоящую организацию. |
| ☐ | 3. MFA | **C** | Ограничение доступа к кредитным файлам для предотвращения мошеннических заявок на кредит. |
| ☐ | 4. МОНИТОРИНГ | **D** | Несанкционированное раскрытие частных баз данных с персональными записями пользователей. |
| ☐ | 5. ЗАМОРОЗКА | **E** | Обучение и технические меры, используемые для защиты от кражи личных данных. |
| ☐ | 6. ЗАЩИТА | **F** | Отправка мошеннических сообщений, чтобы обманом заставить пользователей выдать учётные данные. |
| ☐ | 7. ПОДМЕНА | **G** | Сканирование онлайн-форумов и хакерских каналов в поисках украденных корпоративных данных. |
| ☐ | 8. ФИШИНГ | **H** | Имена пользователей, пароли и закрытые токены, используемые для аутентификации цифровых личностей. |

## Контрольная точка 5: Кроссворд

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




### ПО ГОРИЗОНТАЛИ

**2. Создание поддельного сайта или письма, имитирующего настоящую организацию. (7)**

**6. Дополнительный этап проверки (например, аппаратные ключи), защищающий вход в аккаунты. (14)**

**8. Несанкционированное раскрытие закрытых баз данных с персональными записями пользователей. (6)**

### ПО ВЕРТИКАЛИ

**1. Рассылка мошеннических сообщений, чтобы обманом получить учётные данные. (6)**

**3. Имена пользователей, пароли и закрытые токены для аутентификации цифровых личностей. (13)**

**4. Ограничение доступа к кредитным файлам для предотвращения мошеннических заявок на кредит. (9)**

**5. Сканирование онлайн-форумов и хакерских каналов в поисках украденных корпоративных данных. (10)**

**7. Обучение и технические меры, используемые для защиты от кражи личности. (6)**

# 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: Создание поддельного сайта или письма, имитирующего настоящую организацию. (7 букв):**

**6 по горизонтали: Дополнительный этап проверки (например, аппаратные ключи), защищающий вход в аккаунты. (14 букв):**

**8 по горизонтали: Несанкционированное раскрытие закрытых баз данных с персональными записями пользователей. (6 букв):**

## ПО ВЕРТИКАЛИ

**1 по вертикали: Рассылка мошеннических сообщений, чтобы обманом получить учётные данные. (6 букв):**

**3 по вертикали: Имена пользователей, пароли и закрытые токены для аутентификации цифровых личностей. (13 букв):**

**4 по вертикали: Ограничение доступа к кредитным файлам для предотвращения мошеннических заявок на кредит. (9 букв):**

**5 по вертикали: Сканирование онлайн-форумов и хакерских каналов в поисках украденных корпоративных данных. (10 букв):**

**7 по вертикали: Обучение и технические меры, используемые для защиты от кражи личности. (6 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 | А | Д | Ж | Г | И | К | Д | Х | Ф | П | Е | К | Ц | Я |
| Ы | К | Ч | Ж | Ф | Н | А | Т | И | Щ | А | З | Ъ | Ж | А |
| Н | З | А | Ф | Т | Р | И | У | Ф | И | Ш | И | Н | Г | Ш |
| Н | О | Э | Ф | М | Х | Ш | Р | Ц | Г | Р | Ю | В | З | Г |
| А | Р | Ц | Ь | Ы | Л | А | Х | О | Я | Ю | Ю | Н | Н | З |
| Д | О | К | П | Х | М | О | О | Ч | Т | Т | И | И | У | Ф |
| Е | М | И | Я | А | С | Ъ | З | Щ | В | И | Ф | Ю | Ц | Ю |
| Ы | А | Б | И | О | Я | И | М | С | У | У | Н | Р | Ь | В |
| Н | З | О | Я | Ю | З | Э | Т | Ы | П | Щ | Н | О | Щ | У |
| Т | Б | С | Ъ | Ш | О | И | Ъ | С | Г | Э | Щ | М | М | Х |
| Е | М | Н | О | Г | О | Ф | А | К | Т | О | Р | Н | А | Я |
| Ч | Б | Ь | Я | Э | П | Ц | Ф | Ь | К | Т | Д | А | Г | М |
| У | Ф | У | Т | Е | Ч | К | И | Ы | Ь | Ь | Н | Л | Й | Ш |
| Й | З | Б | Ж | К | Н | Ч | Ц | Ы | Х | Я | Е | Й | Ж | Ц |
| Г | А | О | У | В | Я | П | М | Ъ | Х | Щ | А | Ц | Ь | М |

**СПИСОК СЛОВ СЛОВАРЯ**

УЧЕТНЫЕДАННЫЕ УТЕЧКИ МНОГОФАКТОРНАЯ МОНИТОРИНГ ЗАМОРОЗКА
ЗАЩИТА СПУФИНГ 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. УЧЕТНЫЕДАННЫЕ**

**B. УТЕЧКИ**

**C. МНОГОФАКТОРНАЯ**

**D. МОНИТОРИНГ**

**E. ЗАМОРОЗКА**

**F. ЗАЩИТА**

**G. СПУФИНГ**

**H. ФИШИНГ**

**ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ**

1. Рассылка мошеннических сообщений, чтобы обманом получить учётные данные.

2. Имена пользователей, пароли и закрытые токены для аутентификации цифровых личностей.

3. Создание поддельного сайта или письма, имитирующего настоящую организацию.

4. Обучение и технические меры, используемые для защиты от кражи личности.

5. Сканирование онлайн-форумов и хакерских каналов в поисках украденных корпоративных данных.

6. Ограничение доступа к кредитным файлам для предотвращения мошеннических заявок на кредит.

7. Несанкционированное раскрытие закрытых баз данных с персональными записями пользователей.

8. Дополнительный этап проверки (например, аппаратные ключи), защищающий вход в аккаунты.

## 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. ЕЕАЫЫЧДНУНЕНТ _____
2. ОНФОААМНКЯОРТГ _____
3. ЗОРАЗАОКМ _____
4. ГПИФНСУ _____
5. ЧЕИУКТ _____
6. НТИРИМООГН _____
7. ТЗИАЩА _____
8. ШГФНИИ _____

# Дополнительное задание: Думай быстро

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

| | | | | |
|---|---|---|---|---|
| 1 | Что делать, если ваши личные данные украдены | | | |
| 2 | То, чем не стоит делиться в социальных сетях | | | |
| 3 | То, для чего вы делаете резервные копии | | | |
| 4 | Карты или удостоверения в вашем кошельке | | | |
| 5 | Документы, которые нужно защищать | | | |
| 6 | Что делать после утечки данных | | | |
| 7 | Причины обновлять программы | | | |
| 8 | Информация, которая нужна похитителю личных данных | | | |
| 9 | Устройства, которые могут быть взломаны | | | |
| 10 | Места, откуда могут утечь ваши данные | | | |
| 11 | Безопасные привычки, которые можно начать уже сегодня | | | |
| 12 | Признаки заражения компьютера | | | |
| 13 | Способы подтвердить свою личность | | | |
| 14 | Признаки кражи личных данных | | | |
| 15 | Тревожные признаки в электронном письме | | | |

# Контрольная точка 8: Кейсы по кибербезопасности

Примените изученные понятия к реальным ситуациям ниже.

## КЕЙС 1: ЗАЩИТА ОТ ПОДМЕНЫ ЛИЧНОСТИ РУКОВОДИТЕЛЯ



**Ситуация:** Известный руководитель высшего звена стал целью доменных имён с опечатками, имитирующих его личную электронную почту, чтобы обманывать клиентов. Разработайте план защиты бренда.

**Вопрос для обсуждения:** Проанализируйте риски подмены бренда и опишите SPF/DKIM/DMARC и средства контроля аутентификации.

## КЕЙС 2: ПОЯВЛЕНИЕ КОРПОРАТИВНЫХ УЧЁТНЫХ ДАННЫХ В ДАРКНЕТЕ



**Ситуация:** Дамп базы данных из даркнета содержит несколько сотен корпоративных учётных данных системных администраторов компании. Разработайте стратегию снижения рисков.

**Вопрос для обсуждения:** Опишите процесс очистки учётных данных и спланируйте внедрение менеджера паролей.

## 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 | | 13 | 10 | 25 | 15 | 16 | 19 | 20 | 30 | | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | |

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

| 17 | 18 | 16 | 3 | 6 | 18 | 12 | 16 | 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: Что такое кража личных данных?

Преступление, при котором злоумышленник похищает личные данные (например, пароли или номера социального страхования), чтобы выдать себя за другого человека ради финансовой выгоды.

### Q2: Какова самая частая причина кражи личных данных?

Фишинг — один из основных способов, которыми злоумышленники получают пароли: он заманивает пользователей на поддельные, подменённые сайты.

### Q3: Как многофакторная аутентификация (MFA) защищает учётные данные?

MFA требует дополнительного подтверждения (например, аппаратного ключа) для входа и не пускает злоумышленников, даже если они украдут ваш пароль.

### Q4: Что такое заморозка кредитной истории?

Бесплатная услуга, не позволяющая бюро кредитных историй передавать вашу кредитную историю и мешающая злоумышленникам оформлять новые займы на ваше имя. [2]

### Q5: Что такое мониторинг даркнета?

Программа, которая проверяет хакерские форумы на наличие утёкших адресов электронной почты, паролей и персональных данных и предупреждает вас, если ваши данные раскрыты.

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

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

### Q6: Что означает подстановка учётных данных (credential stuffing)?

Автоматические боты проверяют утёкшие списки паролей на сотнях сайтов, чтобы захватить действующие учётные записи.

### Q7: Чем опасна подмена адреса электронной почты?

Позволяет злоумышленникам подделывать имя отправителя в письмах, из-за чего фишинговые сообщения выглядят так, будто их прислали доверенные коллеги.

### Q8: Как менеджеры паролей предотвращают кражу личных данных?

Они хранят сложные уникальные пароли для каждой учётной записи и отказываются автоматически подставлять учётные данные на поддельных фишинговых доменах.

### Q9: Что такое целевой фишинг (spear phishing)?

Высоконаправленная фишинговая атака, подстроенная под имя и данные жертвы, чтобы повысить вероятность обмана.

### Q10: Чем оповещение о кредитной истории отличается от заморозки?

Оповещение требует от кредиторов проверять вашу личность перед открытием счетов, а заморозка полностью блокирует доступ к вашей кредитной истории. [2]

# 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 подмена SIM-карты (SIM swapping) приводит к краже личных данных?

Злоумышленники убеждают сотрудников оператора связи перенести номер телефона жертвы на новую SIM-карту и перехватывают коды 2FA, приходящие по SMS.

### Q2: Какую роль играет DMARC в предотвращении кражи личных данных?

DMARC позволяет владельцам доменов блокировать поддельные письма, не давая им попасть во входящие, и мешает выдавать фальшивые письма за корпоративные домены.

### Q3: Почему кражу синтетической личности трудно обнаружить?

Воры сочетают настоящие номера SSN с вымышленными именами и датами рождения, создавая новые кредитные профили в обход базовых оповещений о мошенничестве.

### Q4: Как брокеры данных используют персональные данные?

Брокеры данных собирают публичные записи, данные о поведении в сети и историю покупок, чтобы составлять досье на профили, которые могут быть утечены или проданы.

### Q5: Почему MFA на основе SMS считается уязвимой?

SMS-трафик уязвим для перехвата, фишинга и атак с подменой SIM-карты на уровне оператора.

# 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 блокировка кредитного файла?

Коммерческая услуга, похожая на заморозку, позволяющая мгновенно разблокировать или заблокировать кредитную историю через мобильное приложение.

### Q7: Как утечки корпоративных данных способствуют краже личности?

Утёкшие базы данных раскрывают миллионы учётных данных в открытом виде и дают злоумышленникам сырые данные для целевого мошенничества с личными данными.

### Q8: Чем опасно чрезмерное раскрытие информации в социальных сетях?

Публичное разглашение кличек питомцев, мест рождения и девичьих фамилий матерей даёт злоумышленникам ответы на типичные вопросы для восстановления учётных записей.

### Q9: Как биометрический вход защищает профили личных данных?

Биометрия привязывает вход к таким признакам, как отпечатки пальцев или лица; при хранении на устройстве её трудно украсть, но сохранённые биометрические данные могут утечь.

### Q10: Как правило Red Flags Rule борется с кражей личных данных?

Федеральное правило, требующее от финансовых учреждений разработать письменные программы для выявления признаков кражи личных данных и реагирования на них.

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

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

**1. АНАЛИЗ БЕЗОПАСНОСТИ**

IdentityTheft.gov, которым управляет FTC, позволяет жертвам в США сообщить о краже личных данных и получить персональный план восстановления. [1]

**2. АНАЛИЗ БЕЗОПАСНОСТИ**

Аппаратные ключи безопасности — это устойчивая к фишингу MFA, самый надёжный вид MFA, к использованию которого призывает CISA. [4]

**3. АНАЛИЗ БЕЗОПАСНОСТИ**

Скомпрометированные пароли — частая точка входа при утечках данных, способствующая последующему мошенничеству с личными данными.

**4. АНАЛИЗ БЕЗОПАСНОСТИ**

Заморозка кредитной истории бесплатна по федеральному закону и не позволяет кредиторам проверять кредитные файлы, пока она не снята. [2]

**5. АНАЛИЗ БЕЗОПАСНОСТИ**

DMARC позволяет владельцам доменов указать почтовым серверам отклонять или помещать в карантин поддельные письма, не прошедшие проверки. [7]

**6. АНАЛИЗ БЕЗОПАСНОСТИ**

Подмена SIM-карты позволяет хакерам обходить двухфакторную аутентификацию по SMS на банковских порталах.

**7. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ**

Мошенничество с синтетической личностью смешивает реальные и поддельные данные, из-за чего кредиторам трудно его обнаружить.

**8. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ**

Многие люди используют один и тот же пароль для разных онлайн-аккаунтов, поэтому одна утечка может раскрыть сразу несколько из них.

**9. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ**

Брокеры данных собирают подробные досье на большое число потребителей, что создаёт сконцентрированный риск для конфиденциальности.

**10. АНАЛИЗ БЕЗОПАСНОСТИ**

Восстановление после кражи личных данных может занять месяцы работы, например оспаривание списаний и исправление кредитных отчётов.

# 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] Federal Trade Commission. (n.d.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

[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

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

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

[7] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

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

### 1 Вопрос 1

**Правильный ответ: A**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Какой способ чаще всего используют похитители личных данных, чтобы украсть логины и пароли? → Рассылка поддельных уведомлений по электронной почте, чтобы обманом заставить пользователей вводить пароли на подменённых порталах

### 2 Вопрос 2

**Правильный ответ: A**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Какая мера безопасности обеспечивает самую надёжную защиту от утечек учётных данных? → Многофакторная аутентификация с аппаратными ключами

### 3 Вопрос 3

**Правильный ответ: A**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что представляет собой заморозка кредитной истории? → Блокировка кредитных отчётов, чтобы злоумышленники не могли оформлять несанкционированные займы

### 4 Вопрос 4

**Правильный ответ: A**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Чем полезен мониторинг даркнета? → Предупреждает пользователей, если их утёкшие учётные данные появляются в нелегальных базах данных

### 5 Вопрос 5

**Правильный ответ: A**

#### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что означает социальная инженерия? → Манипулирование людьми, чтобы они добровольно раскрыли конфиденциальные учётные данные

## Ответы: контрольная точка 2 – верно или неверно

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

### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Кража личных данных может начаться и офлайн, например с украденной почты или документов.

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

### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Обязательная MFA для всех личных аккаунтов блокирует большинство ботов-атак подстановки учётных данных.

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

### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Заморозка кредитной истории останавливает новые проверки кредитоспособности, но не влияет на ваши существующие счета.

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

### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Менеджеры паролей защищают пользователей от фишинга, отказываясь автоматически подставлять пароли на поддельных доменах.

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

### ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Фишинговые письма часто используют срочные формулировки, чтобы вызвать эмоциональную и быструю реакцию.

# 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

| | | | |
|---|---|---|---|
| H 1. УЧЁТНЫЕ ДАННЫЕ | D 2. УТЕЧКИ | A 3. MFA | G 4. МОНИТОРИНГ |
| C 5. ЗАМОРОЗКА | E 6. ЗАЩИТА | B 7. ПОДМЕНА | F 8. ФИШИНГ |

## КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

| | | | |
|---|---|---|---|
| 1 УЧЁТНЫЕ ДАННЫЕ | 2 УТЕЧКИ | 3 МНОГОФАКТОРНАЯ | 4 МОНИТОРИНГ |
| 5 ЗАМОРОЗКА | 6 ЗАЩИТА | | |

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

| | | | |
|---|---|---|---|
| 1 H – ФИШИНГ | 2 A – УЧЕТНЫЕДАННЫЕ | 3 G – СПУФИНГ | 4 F – ЗАЩИТА |
| 5 D – МОНИТОРИНГ | 6 E – ЗАМОРОЗКА | 7 B – УТЕЧКИ | 8 C – МНОГОФАКТОРНАЯ |

## ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

**Ключевые термины:**
Проверьте, могут ли учащиеся своими словами объяснить УЧЁТНЫЕ ДАННЫЕ, УТЕЧКИ и MFA и привести пример для каждого термина.

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

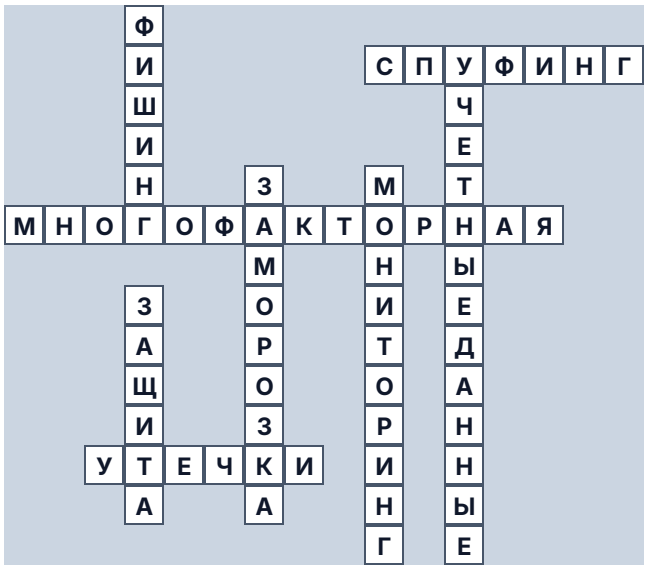
**Оценка источников:**
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

# Ключи к головоломкам и примечания для преподавателя

## РЕШЕНИЕ К ПОИСКУ СЛОВ

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

## РЕШЕНИЕ КРОССВОРДА




## РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

### ПО ГОРИЗОНТАЛИ

**2 по горизонтали: СПУФИНГ** Создание поддельного сайта или письма, имитирующего настоящую организацию. (7 букв)

**6 по горизонтали: МНОГОФАКТОРНАЯ** Дополнительный этап проверки (например, аппаратные ключи), защищающий вход в аккаунты. (14 букв)

**8 по горизонтали: УТЕЧКИ** Несанкционированное раскрытие закрытых баз данных с персональными записями пользователей. (6 букв)

### ПО ВЕРТИКАЛИ

**1 по вертикали: ФИШИНГ** Рассылка мошеннических сообщений, чтобы обманом получить учётные данные. (6 букв)

**3 по вертикали: УЧЕТНЫЕДАННЫЕ** Имена пользователей, пароли и закрытые токены для аутентификации цифровых личностей. (13 букв)

**4 по вертикали: ЗАМОРОЗКА** Ограничение доступа к кредитным файлам для предотвращения мошеннических заявок на кредит. (9 букв)

**5 по вертикали: МОНИТОРИНГ** Сканирование онлайн-форумов и хакерских каналов в поисках украденных корпоративных данных. (10 букв)

**7 по вертикали: ЗАЩИТА** Обучение и технические меры, используемые для защиты от кражи личности. (6 букв)

# Ключ к словам-перевёртышам и шифру

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

### КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. ЕЕАЫЫЧДНУНЕНТ — **УЧЕТНЫЕДАННЫЕ**
2. ОНФОААМНКЯОРТГ — **МНОГОФАКТОРНАЯ**
3. ЗОРАЗАОКМ — **ЗАМОРОЗКА**
4. ГПИФНСУ — **СПУФИНГ**
5. ЧЕИУКТ — **УТЕЧКИ**
6. НТИРИМООГН — **МОНИТОРИНГ**
7. ТЗИАЩА — **ЗАЩИТА**
8. ШГФНИИ — **ФИШИНГ**

### КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

**"ЗАЩИТИТЕ ЛИЧНОСТЬ С МНОГОФАКТОРНОЙ ПРОВЕРКОЙ"**

# Ответы к кейсам

## A Кейс 1: Защита от подмены личности руководителя

Решение для преподавателя

### РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

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

- Анализ ситуации: известный топ-менеджер стал целью доменных имён с опечатками, имитирующих его личную почту, с помощью которых обманывают клиентов. Разработайте план защиты бренда.
- Рекомендуемая стратегия и решение: Зарегистрируйте все распространённые варианты написания имени руководителя. Внедрите протоколы аутентификации почты (DMARC, DKIM, SPF), чтобы предотвратить подмену домена. Включите аппаратную MFA для всех корпоративных входов топ-менеджеров.

## B Кейс 2: Появление корпоративных учётных данных в даркнете

Решение для преподавателя

### РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

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

- Анализ ситуации: дамп базы данных даркнета содержит несколько сотен корпоративных учётных записей системных администраторов предприятия. Разработайте стратегию снижения рисков.
- Рекомендуемая стратегия и решение: проведите сброс паролей во всей компании. Обяжите использовать корпоративный менеджер паролей. Включите MFA на всех порталах системы и настройте непрерывные автоматические оповещения мониторинга даркнета.