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

Фишинговые атаки и социальная инженерия

Целевой фишинг, мошенничество против топ-менеджеров (whaling), протоколы SPF/DKIM/DMARC, подмена отправителя и обучение сотрудников безопасности.

ОБЗОР ОБУЧЕНИЯ: ФИШИНГОВЫЕ АТАКИ

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 фишинговые атаки и социальную инженерию. Вы изучите целевой фишинг, фишинг руководителей, подмену доменов, протоколы SPF/DKIM/DMARC, безопасность ссылок и обучение сотрудников.

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/fishing-ataki/

Ваша дорожная карта обучения: снижение угрозы фишинга

- Определите распространённые формы фишинга, вишинга и мошенничества с всплывающими окнами поддержки.
- Внедрите внеполосные процедуры подтверждения транзакций.
- Настройте правила SPF, DKIM и DMARC для блокировки подменённых доменов.

ИНСТРУКЦИИ К РУКОВОДСТВУ ПО ФИШИНГОВЫМ АТАКАМ

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: аутентификации электронной почты. Завершите работу дополнительным заданием «Думай быстро».

ФИШИНГОВЫЕ АТАКИ И СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ (ВВЕДЕНИЕ)

Фишинговые атаки используют целевые сообщения, мошенничество с «китами» (whaling) и подмену доменов для сбора учётных данных пользователей. Защита корпоративных систем требует развёртывания правил SPF, DKIM и DMARC на шлюзе наряду с внеполосными шагами подтверждения.

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

Контрольная точка 1: Задание с выбором ответа

1. Что такое целевой фишинг (spear phishing)?

- A. Целевое фишинговое письмо, адаптированное под конкретного человека или организацию
- B. Массовая рассылка электронных писем миллионам случайных адресов
- C. Сетевая атака, при которой веб-серверы заливаются потоком трафика
- D. Метод извлечения из базы данных записей пользователей

2. Какой протокол позволяет домену перечислить в DNS разрешённые IP-адреса отправки для борьбы с подменой?

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3. Что такое атака типа «вейлинг»?

- A. Фишинговая кампания, нацеленная на высокопоставленных корпоративных руководителей
- B. Атака с SQL-инъекцией, нацеленная на резервные копии баз данных
- C. Физическая кража оборудования маршрутизаторов локальной сети
- D. Автоматическое сканирование подбором учётных данных

4. Что делает DKIM?

- A. Добавляет к письмам криптографическую подпись для подтверждения подлинности отправителя
- B. Блокирует входящий сетевой трафик пакетов на межсетевом экране
- C. Шифрует тома хранилища баз данных в состоянии покоя
- D. Сканирует вложения электронной почты на вредоносное ПО по сигнатурам

5. Какова роль DMARC?

- A. Указание принимающим почтовым серверам, как обрабатывать письма, не прошедшие проверки SPF/DKIM
- B. Расшифровка системных паролей с помощью заранее вычисленных радужных таблиц
- C. Сжатие вложений электронной почты перед доставкой
- D. Настройка привилегий доступа к сетевой маршрутизации

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Целевой фишинг (spear phishing) основан на типовых массовых письмах, рассылаемых миллионам случайных адресов.

○ Верно ○ Неверно

7 Вопрос 7

7. Политики DMARC могут предписывать почтовым серверам отклонять неавторизованные поддельные сообщения.

○ Верно ○ Неверно

8 Вопрос 8

8. Проверка SPF работает путём проверки криптографической подписи тела письма.

○ Верно ○ Неверно

9 Вопрос 9

9. Атаки типа «вейлинг» нацелены на рядовых корпоративных администраторов, чтобы получить доступ к файлам баз данных.

○ Верно ○ Неверно

10 Вопрос 10

10. Внеполосная проверка платёжных запросов помогает остановить мошенничество с банковскими переводами.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Нацеливание на конкретного сотрудника с персонализированными сведениями — это _____ фишинг.

2. Подделка заголовка письма, чтобы сообщения выглядели легитимно, — это _____ отправителя.

3. DNS-запись со списком IP-адресов авторизованных почтовых серверов называется _____ .

4. Стандарт подписи электронной почты, подтверждающий отправителя, — это _____ .

5. Политики отклонения писем, не прошедших проверки SPF/DKIM, задаёт стандарт _____ .

6. Фишинговая кампания, нацеленная на руководителей высшего звена, называется _____ .

СЛОВАРНЫЙ БАНК СЛОВ

ВЕЙЛИНГ ВИШИНГ ДКИМ ДМАРК ЗАПИСЬ СПФ СПУФИНГ ЦЕЛЕВОЙ ШИФРОВАНИЕ

Напишите свои ответы здесь:

1.
2.
3.
4.
5.
6.

Контрольная точка 4: Сопоставление понятий о безопасности

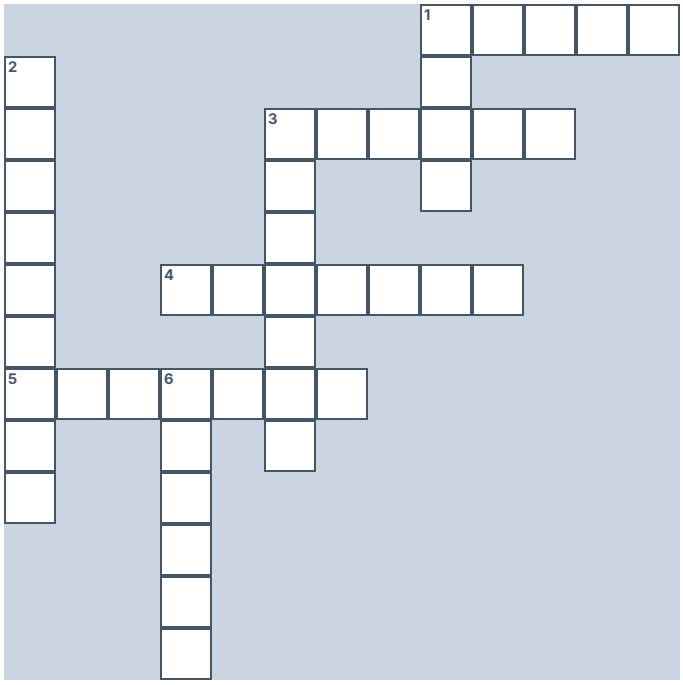
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. ЦЕЛЕВОЙ ФИШИНГ	A	Мошеннические голосовые звонки.
☐	2. ПОДМЕНА	B	Мишень — топ-менеджеры уровня C.
☐	3. SPF	C	Инструкции политики на отклонение.
☐	4. DKIM	D	Авторизованные IP-адреса отправителей DNS.
☐	5. DMARC	E	Письмо с социальной инженерией.
☐	6. ВЕЙЛИНГ	F	Персонализированное целевое письмо.
☐	7. ФИШИНГ	G	Подделка адреса электронной почты отправителя.
☐	8. ВИШИНГ	H	Криптографическая подпись в электронном письме.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

1. Политика отклонения писем. (5)

3. Голосовые мошеннические звонки. (6)

4. Персонализированное целевое письмо. (7)

5. Подделка адреса отправителя письма. (7)

ПО ВЕРТИКАЛИ

1. Криптографическая подпись в письме. (4)

2. Авторизованные IP-адреса отправителей в DNS. (9)

3. Атака на руководителей высшего звена. (7)

6. Письмо социальной инженерии. (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

1 по горизонтали: Политика отклонения писем. (5 букв):

3 по горизонтали: Голосовые мошеннические звонки. (6 букв):

4 по горизонтали: Персонализированное целевое письмо. (7 букв):

5 по горизонтали: Подделка адреса отправителя письма. (7 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Криптографическая подпись в письме. (4 букв):

2 по вертикали: Авторизованные IP-адреса отправителей в DNS. (9 букв):

3 по вертикали: Атака на руководителей высшего звена. (7 букв):

6 по вертикали: Письмо социальной инженерии. (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.

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

СПИСОК СЛОВ СЛОВАРЯ

ЦЕЛЕВОЙ СПУФИНГ ЗАПИСЬСПФ ДКИМ ДМАРК ВЕЙЛИНГ ФИШИНГ ВИШИНГ

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. ЦЕЛЕВОЙ**
- **B. СПУФИНГ**
- **C. ЗАПИСЬСПФ**
- **D. ДКИМ**
- **E. ДМАРК**
- **F. ВЕЙЛИНГ**
- **G. ФИШИНГ**
- **H. ВИШИНГ**

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

1. _____ Подделка адреса отправителя письма.
2. _____ Персонализированное целевое письмо.
3. _____ Голосовые мошеннические звонки.
4. _____ Авторизованные IP-адреса отправителей в DNS.
5. _____ Письмо социальной инженерии.
6. _____ Политика отклонения писем.
7. _____ Криптографическая подпись в письме.
8. _____ Атака на руководителей высшего звена.

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. **ЕОЦВЙЛЕ** _____
2. **ФЗПИАЬССП** _____
3. **АДКРМ** _____
4. **ГИШНФИ** _____
5. **ИГФУСНП** _____
6. **ИМДК** _____
7. **ВНИГЕЛЙ** _____
8. **ШГВНИИ** _____

Дополнительное задание: Думай быстро

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

1	Устройства, которые могут быть взломаны			
2	Признаки фишингового письма			
3	Признаки заражения компьютера			
4	Слова, создающие ложную срочность			
5	Способы проверить отправителя			
6	Люди, у которых можно попросить помощи по ИТ			
7	То, для чего вы делаете резервные копии			
8	Известные вам рыбы или морские животные			
9	Компании, под которые маскируются мошенники			
10	Безопасные привычки, которые можно начать уже сегодня			
11	Что делать после перехода по поддельной ссылке			
12	Что делать после утечки данных			
13	Каналы, по которым происходит фишинг			
14	То, что никогда нельзя отправлять по электронной почте			
15	Способы защитить свои аккаунты			

Контрольная точка 8: Кейсы по кибербезопасности

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: УСТРАНЕНИЕ ПОСЛЕДСТВИЙ АТАКИ «КИТОБОЙ» НА ТОП-МЕНЕДЖМЕНТ



Ситуация: Финансовый директор получает высокоперсонализированное письмо, якобы от генерального директора, с просьбой срочно перевести $50,000 для закрытия конфиденциальной покупки домена.

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

КЕЙС 2: ВНЕДРЕНИЕ ПОЛИТИК ШЛЮЗА SPF/DKIM/DMARC



Ситуация: Компания не проходит аудиты безопасности, потому что исходящие маркетинговые письма часто помечаются как спам, а хакеры активно подделывают домен её бренда.

Вопрос для обсуждения: Определите технические и административные средства контроля для проверки подлинности электронной почты.

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	29	33	3	13	33	11	20	6

19	16	24	10	15	8	6	15	6	18	10	32		1	21	5	10	20	16	14

17	16	25	20	16	3	16	4	16		26	13	32	9	1

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 фишинг?

Фишинг — это атака с использованием социальной инженерии, при которой преступники рассылают мошеннические сообщения, чтобы обманом получить конфиденциальные данные.

Q2: В чём разница между фишингом и целевым фишингом (spear phishing)?

Фишинг нацелен на широкие группы с типовым содержимым, а целевой фишинг (spear phishing) — на конкретных жертв с использованием индивидуальных деталей.

Q3: Что такое вейлинг?

Вейлинг — это узконаправленная фишинговая атака на высокопоставленных руководителей, обладающих административной властью.

Q4: Что такое подмена адреса электронной почты?

Подмена электронной почты — это создание писем с поддельным адресом отправителя, чтобы обманом заставить получателя доверять источнику.

Q5: Как SPF предотвращает подмену?

Публикует в DNS список разрешённых IP-адресов отправителей, позволяя принимающим серверам проверять источник письма. [1]

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

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q6: Что такое DKIM?

DomainKeys Identified Mail добавляет к заголовкам письма криптографическую подпись, подтверждающую, что домен взял на себя ответственность и что сообщение не было изменено.

Q7: Что означает DMARC?

Domain-based Message Authentication, Reporting, and Conformance. [2]

Q8: Что такое политика DMARC?

Политика, определяющая, как почтовые серверы должны обращаться с письмами, не прошедшими проверку SPF/DKIM (none, quarantine или reject). [2]

Q9: Что такое вишинг?

Голосовой фишинг, при котором злоумышленники с помощью мошеннических телефонных звонков выманивают административные или финансовые данные.

Q10: Чем помогают сканеры ссылок?

Они сканируют и переписывают ссылки во входящих письмах, чтобы проверить безопасность целевых веб-страниц в момент перехода.

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 работает гомографическая атака?

Злоумышленники регистрируют доменные имена с похожими на настоящие символами Unicode, не входящими в ASCII, чтобы визуально имитировать легитимное доменное имя.

Q2: Что такое представление Punycode?

Кодировка, преобразующая доменные имена в Unicode в ASCII-совместимые строки, начинающиеся с «xn--», чтобы DNS мог их обрабатывать.

Q3: Почему «p=reject» — самое безопасное состояние DMARC?

Просит принимающие серверы отклонять почту, не прошедшую проверку DMARC (согласованные SPF/DKIM), во время SMTP-сеанса, блокируя прямую подмену отправителя. [2]

Q4: Как злоумышленники обходят правила SPF?

Используя похожие домены (тайпсквоттинг) или взломанные учётные записи в легитимных сторонних почтовых сервисах.

Q5: Что такое компрометация деловой электронной почты (BEC)?

Корпоративное мошенничество, при котором злоумышленники взламывают деловые электронные ящики или выдают себя за их владельцев, чтобы санкционировать мошеннические платежи.

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

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

Q6: Как многофакторная аутентификация останавливает фишинг?

Требует вторичные токены (например, аппаратные ключи), которые нельзя украсть одними лишь поддельными страницами входа.

Q7: Что такое целевая страница для кражи учётных данных?

Поддельный портал входа, предназначенный для перехвата вводимых имён пользователей, паролей и MFA-токенов в реальном времени.

Q8: Что такое захват поддомена?

Злоумышленник захватывает неиспользуемый указатель поддомена DNS, чтобы размещать вредоносные фишинговые страницы под доверенным родительским доменом.

Q9: Как работает проверка выравнивания DKIM?

Проверяет, что домен в заголовке «From» совпадает с доменом, который криптографически подписал сообщение в заголовке DKIM.

Q10: Какова роль шлюза электронной почты?

Фильтрация входящей электронной почты, проверка ссылок, изоляция вложений в песочнице и проверка соответствия SPF/DKIM/DMARC.

Часть 11: 10 реальных фактов и выводов о кибербезопасности

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

1. АНАЛИЗ БЕЗОПАСНОСТИ

Фишинг и подмена были самым часто регистрируемым видом преступлений в IC3 ФБР в 2025 году: 191,561 жалобы. [4]

2. АНАЛИЗ БЕЗОПАСНОСТИ

Компрометация деловой электронной почты (BEC) привела к потерям свыше 3 млрд долларов, о которых сообщили в IC3 ФБР в 2025 году. [4]

3. АНАЛИЗ БЕЗОПАСНОСТИ

Гомографические атаки используют похожие на латиницу кириллические буквы, чтобы визуально продублировать в браузерах домены брендов с точным соответствием.

4. АНАЛИЗ БЕЗОПАСНОСТИ

При «p=reject» домен просит получателей отклонять письма, не прошедшие проверку, на этапе доставки, а не помещать их в спам. [2]

5. АНАЛИЗ БЕЗОПАСНОСТИ

Атаки типа «вейлинг» на директоров часто содержат срочные требования оплатить конфиденциальные слияния или покупку доменов.

6. АНАЛИЗ БЕЗОПАСНОСТИ

Порталы кражи учётных данных копируют настоящие страницы входа, чтобы жертвы вводили пароли прямо в форму злоумышленника.

7. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Совместные рекомендации CISA по борьбе с фишингом советуют обучение пользователей наряду с DMARC, SPF, DKIM и устойчивой к фишингу MFA. [3]

8. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Проверка SPF ограничена 10 терминами с DNS-запросами; превышение лимита возвращает результат 'permerror'. [1]

9. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Аппаратные ключи безопасности FIDO2 обеспечивают криптографически подкреплённую защиту от удалённого сбора учётных данных.

10. АНАЛИЗ БЕЗОПАСНОСТИ

Фишинг — один из самых распространённых способов, которыми злоумышленники впервые проникают в организацию, поэтому регулярное обучение осведомлённости является эффективной защитой.

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] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

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

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

[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] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 Вопрос 1 — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что такое целевой фишинг (spear phishing)? → Целевое фишинговое письмо, адаптированное под конкретного человека или организацию

2 Вопрос 2 — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

SPF публикует в DNS список разрешённых узлов отправки домена, чтобы получатели могли проверять отправителя конверта.

3 Вопрос 3 — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что такое атака типа «вейлинг»? → Фишинговая кампания, нацеленная на высокопоставленных корпоративных руководителей

4 Вопрос 4 — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что делает DKIM? → Добавляет к письмам криптографическую подпись для подтверждения подлинности отправителя

5 Вопрос 5 — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Какова роль DMARC? → Указание принимающим почтовым серверам, как обрабатывать письма, не прошедшие проверки SPF/DKIM

Ответы: контрольная точка 2 – верно или неверно

6 Вопрос 6

Правильный ответ: Неверно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: целевой фишинг (spear phishing) направлен на конкретных людей, в отличие от обычного массового фишинга.

7 Вопрос 7

Правильный ответ: Верно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Политики DMARC могут предписывать почтовым серверам отклонять неавторизованные поддельные сообщения.

8 Вопрос 8

Правильный ответ: Неверно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: SPF сверяет IP-адрес отправителя с DNS; именно DKIM проверяет криптографическую подпись.

9 Вопрос 9

Правильный ответ: Неверно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: вейлинг нацелен на высшее руководство, которое может одобрять платежи и имеет доступ к конфиденциальным данным.

10 Вопрос 10

Правильный ответ: Верно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Верно: подтверждение платёжных запросов по отдельному, известному каналу помогает остановить мошенничество с переводами.

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. ЦЕЛЕВОЙ ФИШИНГ	G 2. ПОДМЕНА	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. ВЕЙЛИНГ	E 7. ФИШИНГ	A 8. ВИШИНГ

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 ЦЕЛЕВОЙ	2 СПУФИНГ	3 ЗАПИСЬ СПФ	4 ДКИМ
5 ДМАРК	6 ВЕЙЛИНГ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 B – СПУФИНГ	2 A – ЦЕЛЕВОЙ	3 H – ВИШИНГ	4 C – ЗАПИСЬСПФ
5 G – ФИШИНГ	6 E – ДМАРК	7 D – ДКИМ	8 F – ВЕЙЛИНГ

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить ЦЕЛЕВОЙ ФИШИНГ, ПОДМЕНА и SPF и привести пример для каждого термина.

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

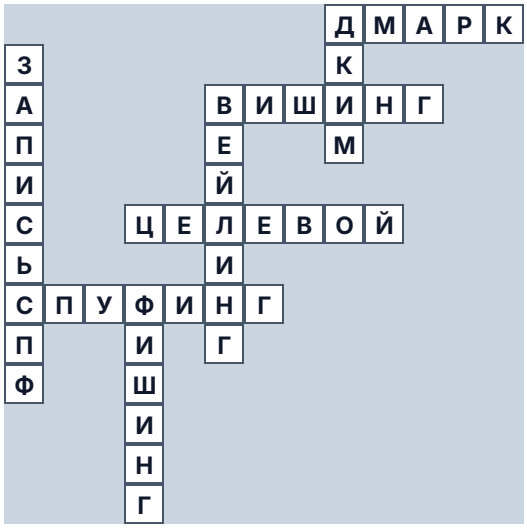
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

1 по горизонтали: ДМАРК Политика отклонения писем. (5 букв)

3 по горизонтали: ВИШИНГ Голосовые мошеннические звонки. (6 букв)

4 по горизонтали: ЦЕЛЕВОЙ Персонализированное целевое письмо. (7 букв)

5 по горизонтали: СПУФИНГ Подделка адреса отправителя письма. (7 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: ДКИМ Криптографическая подпись в письме. (4 букв)

2 по вертикали: ЗАПИСЬСПФ Авторизованные IP-адреса отправителей в DNS. (9 букв)

3 по вертикали: ВЕЙЛИНГ Атака на руководителей высшего звена. (7 букв)

6 по вертикали: ФИШИНГ Письмо социальной инженерии. (6 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. ЕОЦВЙЛЕ — **ЦЕЛЕВОЙ**
2. ФЗПИАЬССП — **ЗАПИСЬСПФ**
3. АДКРМ — **ДМАРК**
4. ГИШНФИ — **ФИШИНГ**
5. ИГФУСНП — **СПУФИНГ**
6. ИМДК — **ДКИМ**
7. ВНИГЕЛЙ — **ВЕЙЛИНГ**
8. ШГВНИИ — **ВИШИНГ**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ВЫЯВЛЯЙТЕ СОЦИНЖЕНЕРИЮ АУДИТОМ ПОЧТОВОГО ШЛЮЗА"

Ответы к кейсам

A Кейс 1: Устранение последствий атаки «китобой» на топ-менеджмент

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: финансовый директор получает очень персонализированное письмо якобы от генерального директора с просьбой срочно перевести $50,000 для закрытия конфиденциальной покупки домена.
- Рекомендуемая стратегия и решение: настройте DMARC с политикой «p=reject», чтобы блокировать поддельные домены отправителей. Добавьте на шлюзе предупреждающие баннеры о внешнем отправителе и требуйте устного подтверждения по другому каналу для всех финансовых операций.

B Кейс 2: Внедрение политик шлюза SPF/DKIM/DMARC

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: компания не проходит аудиты безопасности, потому что её исходящие маркетинговые письма часто попадают в спам, а хакеры активно подделывают домен её бренда.
- Рекомендуемая стратегия и решение: Опубликуйте TXT-запись SPF с перечнем разрешённых IP-адресов отправителей. Настройте ключи подписи DKIM на серверах исходящей почты и анализируйте входящие XML-отчёты DMARC, чтобы выявлять злоупотребления.