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

Атаки программ-вымогателей и бизнес Восстановление

Выполнение вредоносной нагрузки, криптографическое шифрование файлов, офлайн-резервные копии, меры локализации и аварийное восстановление.

АТАКИ ПРОГРАММ-ВЫМОГАТЕЛЕЙ: ОБЗОР ТЕМЫ

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 атаки программ-вымогателей и восстановление бизнеса. Вы изучите выполнение вредоносной нагрузки, шифрование файлов, автономные резервные копии, сдерживание угроз, платежи в криптовалюте и планы аварийного восстановления.

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/ataka-ransomware/

Ваша дорожная карта обучения: восстановление после программы-вымогателя

- Различайте полезную нагрузку троянов, программ-вымогателей и шпионского ПО.
- Проанализируйте вредоносные файлы в защищённых изолированных средах-песочницах.
- Разработайте процедуры быстрой изоляции и локализации сети.

АТАКИ ПРОГРАММ-ВЫМОГАТЕЛЕЙ: ИНСТРУКЦИИ

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: восстановлению после атаки программы-вымогателя. Завершите работу дополнительным заданием «Думай быстро».

АТАКИ ПРОГРАММ-ВЫМОГАТЕЛЕЙ И АВАРИЙНОЕ ВОССТАНОВЛЕНИЕ (ВВЕДЕНИЕ)

Вредоносная нагрузка программ-вымогателей криптографически блокирует хранилище системы и требует выплат в криптовалюте за ключи расшифровки. Снизить эту угрозу помогают правила сетевой изоляции, анализ вредоносного ПО в песочнице и надёжные изолированные «холодные» резервные копии.

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

Контрольная точка 1: Задание с выбором ответа

1. **1. Каков основной механизм атаки программы-вымогателя?**
   - A. Криптографическое шифрование файлов пользователя, чтобы закрыть доступ к системе
   - B. Внедрение вредоносных SQL-команд в поля форм
   - C. Перехват сетевых пакетов в общедоступном соединении Wi-Fi
   - D. Подделка заголовков писем для обхода проверки SPF

2. **2. Что такое автономная (холодная) резервная копия?**
   - A. Копия данных, отключённая от сети для защиты от распространения вредоносного ПО
   - B. Резервная копия на жёстком диске основного веб-сервера
   - C. Временный кэш журналов реестра системы
   - D. Административный инструмент для сброса паролей пользователей

3. **3. Как командам безопасности следует изолировать заражённые системы во время атаки программы-вымогателя?**
   - A. Немедленно отключить сетевые кабели и выключить беспроводные интерфейсы
   - B. Обновить базу сигнатур антивируса
   - C. Отключить основной DNS-сервер
   - D. Переименовать расширения скомпрометированных файлов

4. **4. Почему спецслужбы советуют не платить выкуп вымогателям?**
   - A. Выплата денег поощряет злоумышленников и не гарантирует получение ключа расшифровки
   - B. Он автоматически аннулирует все корпоративные страховые полисы
   - C. Автоматически уведомляет каждого клиента по электронной почте
   - D. Повреждает оставшиеся файлы резервных копий системы

5. **5. Что такое план аварийного восстановления (DRP)?**
   - A. Структурированный процесс восстановления работы и данных после компрометации системы
   - B. Конфигурация межсетевого экрана, сопоставляющая входящие сетевые порты
   - C. Схема базы данных со списком административных привилегий пользователей
   - D. Протокол аутентификации электронной почты, отклоняющий подменённые домены

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Вредоносная нагрузка программ-вымогателей может легко распространиться на сетевые онлайн-резервные копии.

○ Верно ○ Неверно

7 Вопрос 7

7. Выплата выкупа в криптовалюте гарантирует успешную расшифровку файлов.

○ Верно ○ Неверно

8 Вопрос 8

8. Отключение зараженных систем от сети помогает остановить распространение программы-вымогателя на соседние системы.

○ Верно ○ Неверно

9 Вопрос 9

9. Симметричная криптография никогда не используется программами-вымогателями для шифрования системных хранилищ.

○ Верно ○ Неверно

10 Вопрос 10

10. Регулярная проверка процедур восстановления данных — важная часть аварийного восстановления.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. **Блокировка доступа к локальным файлам использует криптографическое** _____ .

2. **Активный вредоносный код, выполняемый в системе, — это** _____ .

3. **Отключённые от сети копии хранилища вне площадки — это надёжная** _____ .

4. **Чтобы остановить распространение вредоносной программы, необходима** _____ **конечных узлов в сети.**

5. **Криптовалютный платёж, которого требуют киберпреступники, — это** _____ .

6. **Возврат рабочих файлов данных в строй — это аварийное** _____ .

СЛОВАРНЫЙ БАНК СЛОВ

ВОССТАНОВЛЕНИЕ ВЫКУП ИЗОЛЯЦИЯ КАТАСТРОФА НАГРУЗКА ТРОЯН ХОЛОДНАЯ КОПИЯ ШИФРОВАНИЕ

Напишите свои ответы здесь:

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

Контрольная точка 4: Сопоставление понятий о безопасности

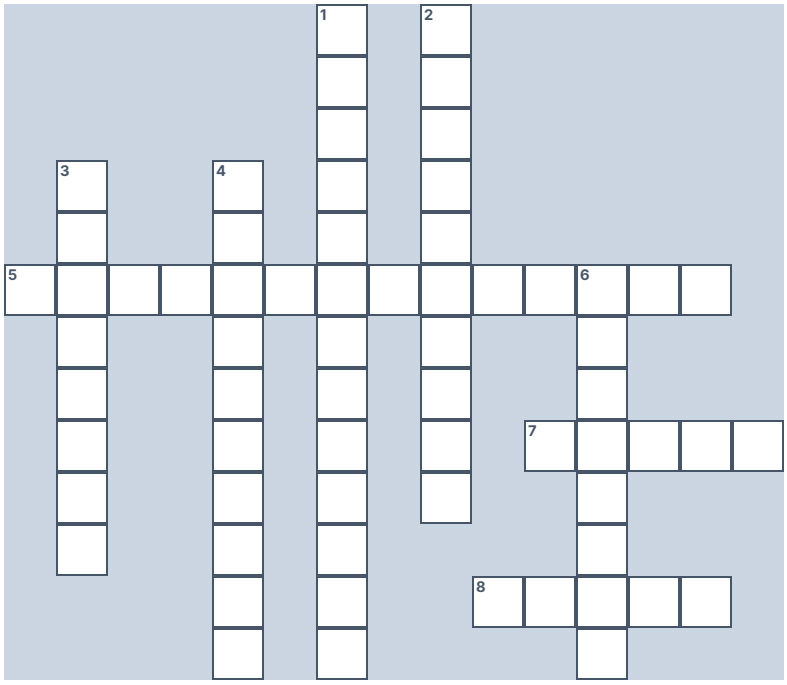
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. ШИФРОВАНИЕ	A	Отключение заражённых сетевых систем.
☐	2. ПОЛЕЗНАЯ НАГРУЗКА	B	Вредоносный файл, замаскированный под безопасный.
☐	3. ХОЛОДНАЯ КОПИЯ	C	Криптографическая блокировка файлов.
☐	4. ИЗОЛЯЦИЯ	D	Крупный сбой в работе системы.
☐	5. ВЫКУП	E	Запуск вредоносного ПО.
☐	6. ВОССТАНОВЛЕНИЕ	F	Отключённая автономная копия.
☐	7. АВАРИЯ	G	Восстановление базы данных из резервной копии.
☐	8. ТРОЯН	H	Запрос на выплату по криптографическому ключу.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

5. Возврат базы данных из резервной копии. (14)

7. Вредоносный файл, замаскированный под безопасный. (5)

8. Требование выплаты за криптографический ключ. (5)

ПО ВЕРТИКАЛИ

1. Отключённая автономная копия. (13)

2. Криптографическая блокировка файлов. (10)

3. Отключение зараженных сетевых систем. (8)

4. Событие серьёзного нарушения работы системы. (10)

6. Запуск вредоносного ПО. (8)

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

5 по горизонтали: Возврат базы данных из резервной копии. (14 букв):

7 по горизонтали: Вредоносный файл, замаскированный под безопасный. (5 букв):

8 по горизонтали: Требование выплаты за криптографический ключ. (5 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Отключённая автономная копия. (13 букв):

2 по вертикали: Криптографическая блокировка файлов. (10 букв):

3 по вертикали: Отключение зараженных сетевых систем. (8 букв):

4 по вертикали: Событие серьёзного нарушения работы системы. (10 букв):

6 по вертикали: Запуск вредоносного ПО. (8 букв):

Контрольная точка 6: Поиск скрытых слов

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

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

СПИСОК СЛОВ СЛОВАРЯ

ШИФРОВАНИЕ НАГРУЗКА ХОЛОДНАЯКОПИЯ ИЗОЛЯЦИЯ ВЫКУП
ВОССТАНОВЛЕНИЕ КАТАСТРОФА ТРОЯН

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. ШИФРОВАНИЕ**
- **B. НАГРУЗКА**
- **C. ХОЛОДНАЯКОПИЯ**
- **D. ИЗОЛЯЦИЯ**
- **E. ВЫКУП**
- **F. ВОССТАНОВЛЕНИЕ**
- **G. КАТАСТРОФА**
- **H. ТРОЯН**

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

1. Отключённая автономная копия. ____
2. Вредоносный файл, замаскированный под безопасный. ____
3. Криптографическая блокировка файлов. ____
4. Требование выплаты за криптографический ключ. ____
5. Отключение зараженных сетевых систем. ____
6. Событие серьёзного нарушения работы системы. ____
7. Запуск вредоносного ПО. ____
8. Возврат базы данных из резервной копии. ____

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. **ИАВОИШНЕРФ** _____
2. **ИДОНЛХПАЯ КОЯО** _____
3. **КВПУЫ** _____
4. **ТФСАААОРКАТ** _____
5. **УЗААРНКГ** _____
6. **ИЯЛЦИЯЗО** _____
7. **ЕИЛВВОСЕАН ОСНТ** _____
8. **НТОЯР** _____

Дополнительное задание: Думай быстро

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

1	Информация, которой нельзя делиться			
2	Устройства, которые могут быть взломаны			
3	Причины не платить выкуп			
4	Безопасные привычки, которые можно начать уже сегодня			
5	Известные вам инструменты безопасности			
6	Способы защитить свои аккаунты			
7	Признаки заражения компьютера			
8	Места для хранения резервной копии			
9	Файлы, которые вы никогда не хотите потерять			
10	Способы распространения программ-вымогателей			
11	Что делать в первый час атаки			
12	Люди, к которым нужно обратиться во время атаки			
13	То, что может заблокировать программа-вымогатель			
14	Слова, связанные с кибербезопасностью			
15	Организации, которые часто становятся целью			

Контрольная точка 8: Кейсы по кибербезопасности

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: СДЕРЖИВАНИЕ ВРЕДОНОСНОЙ НАГРУЗКИ ПРОГРАММЫ-ВЫМОГАТЕЛЯ В КОМПАНИИ



Ситуация: корпоративная локальная сеть заражена активной программой-вымогателем. На ключевых файловых серверах начали появляться файлы с расширением .locked.

Вопрос для обсуждения: Опишите шаги по локализации и протокол восстановления данных.

КЕЙС 2: ОЦЕНКА АВТОНОМНЫХ АРХИТЕКТУР РЕЗЕРВНОГО КОПИРОВАНИЯ



Ситуация: Компания хочет разработать стратегию резервного копирования данных, которая снижает риск компрометации резервных копий, даже если основная локальная сеть полностью захвачена программой-вымогателем.

Вопрос для обсуждения: разработайте защищённое автономное хранилище резервных копий.

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	16	19	19	20	1	15	16	3	10	20	6		5	1	15	15	29	6

10	9		23	16	13	16	5	15	16	11		12	16	17	10	10

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 программа-вымогатель?

Программа-вымогатель — это вредоносное ПО, которое блокирует доступ к компьютерным системам или файлам, пока не будет выплачен выкуп.

Q2: Как распространяется программа-вымогатель?

Через вложения фишинговых писем, неустранённые уязвимости ПО и скомпрометированные системы удалённого доступа. [1]

Q3: Почему просят оплатить в криптовалюте?

Криптовалюты, такие как биткоин, обеспечивают относительную анонимность, из-за чего правоохранительным органам трудно отслеживать средства.

Q4: Блокирует ли антивирус программы-вымогатели?

Да, но антивирус на основе сигнатур может не справиться с только что созданными вредоносными нагрузками программ-вымогателей нулевого дня.

Q5: Что такое изолированная резервная копия (air-gapped)?

Резервная копия, не имеющая физической или логической связи с основной сетью, что защищает её от распространения угроз.

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

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q6: Что такое двойное вымогательство?

Когда злоумышленники не только шифруют файлы, но и крадут конфиденциальные данные, угрожая публичной утечкой в случае неоплаты.

Q7: Что такое дешифратор?

Программная утилита, содержащая криптографический ключ, необходимый для восстановления заблокированных файлов в открытом виде.

Q8: Как рано обнаружить программу-вымогатель?

Отслеживая в файловых системах внезапную массовую модификацию и переименование файлов.

Q9: Какую роль играет страхование?

Киберстрахование может помочь покрыть расходы на восстановление, но условия покрытия и правила выплаты выкупа зависят от полиса.

Q10: Нужно ли перезагружать заражённую систему?

Нет, перезагрузка может уничтожить улики в энергозависимой памяти; вместо этого изолируйте устройство от сети. [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: Как программы-вымогатели используют асимметричное шифрование?

Использует открытый ключ, встроенный в вредоносное ПО, для шифрования файлов, и для расшифровки требуется закрытый ключ злоумышленника.

Q2: Почему также используется симметричное шифрование?

Симметричное шифрование (например, AES) быстрое и может заблокировать огромные базы данных за минуты, а асимметричные ключи защищают ключ AES.

Q3: Что такое логическая сегментация?

Разделение сетей на изолированные зоны, не позволяющее вредоносному ПО распространяться в стороны с рабочих станций на основные серверы.

Q4: Что такое хранилище WORM?

Носители с однократной записью и многократным чтением (WORM), не позволяющие вредоносным нагрузкам программ-вымогателей изменять, перезаписывать или удалять данные резервных копий.

Q5: Что такое теневые копии?

Локальные резервные снимки, создаваемые Windows; программы-вымогатели обычно удаляют их первыми с помощью административных инструментов.

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 кража учётных данных помогает вымогателям?

Злоумышленники покупают утёкшие учётные данные администраторов, чтобы входить через удалённые рабочие столы и вручную запускать программу-вымогатель по всей сети.

Q7: Что такое тестовое восстановление (dry-run)?

Регулярное восстановление резервных баз данных в изолированных тестовых средах, чтобы убедиться, что скорость восстановления и целостность данных соответствуют показателям аварийного восстановления.

Q8: Как обнаружение и реагирование на конечных точках (EDR) останавливает программы-вымогатели?

Анализируя поведение процессов (например, быстрое шифрование) и быстро приостанавливая подозрительное приложение.

Q9: Что такое модель «программа-вымогатель как услуга» (RaaS)?

Франшизная модель, при которой разработчики вредоносного ПО сдают партнёрам в аренду конструкторы программ-вымогателей в обмен на процент от выплат.

Q10: Как непропатченный RDP приводит к заражению программами-вымогателями?

Открытые шлюзы Remote Desktop Protocol без обновлений позволяют злоумышленникам подбирать пароли для входа и вручную запускать вредоносное ПО.

Часть 11: 10 реальных фактов и выводов о кибербезопасности

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

1. АНАЛИЗ БЕЗОПАСНОСТИ

Операторы программ-вымогателей часто используют такие инструменты, как vssadmin.exe, чтобы удалять теневые копии Windows и блокировать локальное восстановление. [1]

2. АНАЛИЗ БЕЗОПАСНОСТИ

Симметричные ключи AES-256 обычно используются для шифрования содержимого файлов, которые затем блокируются с помощью открытых ключей RSA.

3. АНАЛИЗ БЕЗОПАСНОСТИ

Восстановление после успешной атаки программы-вымогателя может занять недели, поэтому важны проверенные автономные резервные копии.

4. АНАЛИЗ БЕЗОПАСНОСТИ

ФБР не поддерживает выплату выкупа и предупреждает, что выплата не гарантирует возврата данных. [2]

5. АНАЛИЗ БЕЗОПАСНОСТИ

Планы аварийного восстановления (DRP) должны определять целевое время восстановления (RTO) и целевую точку восстановления (RPO).

6. АНАЛИЗ БЕЗОПАСНОСТИ

ФБР рекомендует зашифрованные и неизменяемые резервные копии, то есть такие, которые нельзя изменить или удалить. [3]

7. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Разработчики программ-вымогателей используют сложные методы обфускации, чтобы обходить традиционные антивирусные сканеры на основе сигнатур.

8. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Сегментация сети ограничивает перемещение внутри сети, помогая не допустить распространения программы-вымогателя дальше первого заражённого узла. [3]

9. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Открытые, плохо защищённые удалённые службы, такие как Remote Desktop Protocol (RDP), — распространённая точка проникновения программ-вымогателей. [1]

10. АНАЛИЗ БЕЗОПАСНОСТИ

CISA рекомендует хранить зашифрованные резервные копии офлайн, поскольку многие вариации программ-вымогателей ищут и удаляют доступные резервные копии. [1]

Технические ссылки и источники

Учебное пособие и интерактивные головоломки составлены на основе мировых стандартов NIST, OWASP и требований к соблюдению правил конфиденциальности данных.

НАУЧНЫЕ И ОТРАСЛЕВЫЕ ИСТОЧНИКИ

[1] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.

https://www.ic3.gov/CrimeInfo/Ransomware

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

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

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

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

[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

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 Вопрос 1

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Каков основной механизм атаки программы-вымогателя? → Криптографическое шифрование файлов пользователя, чтобы закрыть доступ к системе

2 Вопрос 2

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что такое автономная (холодная) резервная копия? → Копия данных, отключённая от сети для защиты от распространения вредоносного ПО

3 Вопрос 3

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Как командам безопасности следует изолировать заражённые системы во время атаки программы-вымогателя? → Немедленно отключить сетевые кабели и выключить беспроводные интерфейсы

4 Вопрос 4

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Почему спецслужбы советуют не платить выкуп вымогателям? → Выплата денег поощряет злоумышленников и не гарантирует получение ключа расшифровки

5 Вопрос 5

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что такое план аварийного восстановления (DRP)? → Структурированный процесс восстановления работы и данных после компрометации системы

Ответы: контрольная точка 2 – верно или неверно

6 **Вопрос 6** — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Вредоносная нагрузка программ-вымогателей может легко распространиться на сетевые онлайн-резервные копии.

7 **Вопрос 7** — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: ФБР предупреждает, что оплата не гарантирует возврата каких-либо данных.

8 **Вопрос 8** — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Верно: CISA советует отключать зараженные узлы или переводить сеть в офлайн, чтобы сдержать распространение.

9 **Вопрос 9** — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: программы-вымогатели обычно шифруют файлы быстрыми симметричными шифрами, такими как AES.

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

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Регулярная проверка процедур восстановления данных — важная часть аварийного восстановления.

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

C 1. ШИФРОВАНИЕ	E 2. ПОЛЕЗНАЯ НАГРУЗКА	F 3. ХОЛОДНАЯ КОПИЯ	A 4. ИЗОЛЯЦИЯ
H 5. ВЫКУП	G 6. ВОССТАНОВЛЕНИЕ	D 7. АВАРИЯ	B 8. ТРОЯН

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 ШИФРОВАНИЕ	2 НАГРУЗКА	3 ХОЛОДНАЯ КОПИЯ	4 ИЗОЛЯЦИЯ
5 ВЫКУП	6 ВОССТАНОВЛЕНИЕ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 C – ХОЛОДНАЯКОПИЯ	2 H – ТРОЯН	3 A – ШИФРОВАНИЕ	4 E – ВЫКУП
5 D – ИЗОЛЯЦИЯ	6 G – КАТАСТРОФА	7 B – НАГРУЗКА	8 F – ВОССТАНОВЛЕНИЕ

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить ШИФРОВАНИЕ, ПОЛЕЗНАЯ НАГРУЗКА и ХОЛОДНАЯ КОПИЯ и привести пример для каждого термина.

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

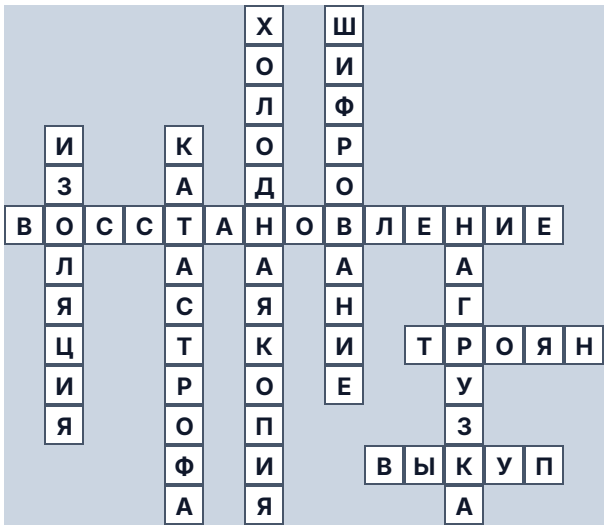
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

5 по горизонтали: ВОССТАНОВЛЕНИЕ Возврат базы данных из резервной копии. (14 букв)

7 по горизонтали: ТРОЯН Вредоносный файл, замаскированный под безопасный. (5 букв)

8 по горизонтали: ВЫКУП Требование выплаты за криптографический ключ. (5 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: ХОЛОДНАЯКОПИЯ Отключённая автономная копия. (13 букв)

2 по вертикали: ШИФРОВАНИЕ Криптографическая блокировка файлов. (10 букв)

3 по вертикали: ИЗОЛЯЦИЯ Отключение зараженных сетевых систем. (8 букв)

4 по вертикали: КАТАСТРОФА Событие серьёзного нарушения работы системы. (10 букв)

6 по вертикали: НАГРУЗКА Запуск вредоносного ПО. (8 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. ИАВОИШНЕРФ — **ШИФРОВАНИЕ**
2. ИДОНЛХПАЯКОЯО — **ХОЛОДНАЯКОПИЯ**
3. КВПУЫ — **ВЫКУП**
4. ТФСАААОРКАТ — **КАТАСТРОФА**
5. УЗААРНКГ — **НАГРУЗКА**
6. ИЯЛЦИЯЗО — **ИЗОЛЯЦИЯ**
7. ЕИЛВВОСЕАНОСНТ — **ВОССТАНОВЛЕНИЕ**
8. НТОЯР — **ТРОЯН**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ВОССТАНОВИТЕ ДАННЫЕ ИЗ ХОЛОДНОЙ КОПИИ"

Ответы к кейсам

A Кейс 1: Сдерживание вредоносной нагрузки программы-вымогателя в компании

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: корпоративная локальная сеть взломана активной программой-вымогателем. На ключевых файловых серверах у файлов появились расширения .locked.
- Рекомендуемая стратегия и решение: отключите все затронутые серверы от локальной сети. Завершите активные административные сеансы. Восстановите неповреждённые файлы из защищённой от записи автономной системы резервного копирования.

B Кейс 2: Оценка автономных архитектур резервного копирования

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: компания хочет разработать стратегию резервного копирования данных, которая снижает риск компрометации резервных копий, даже если основная локальная сеть полностью захвачена программой-вымогателем.
- Рекомендуемая стратегия и решение: Внедрите хранилище WORM (однократная запись, многократное чтение). Создайте логический воздушный зазор, отключив систему резервного копирования от всех сетей, и ежедневно меняйте физические носители.