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

Защита данных и корпоративные хранилища Руководство по безопасности

Маскирование данных, токенизация, шифрование неактивных и передаваемых данных, автономные резервные копии

ОБЗОР ОБУЧЕНИЯ: ЗАЩИТА 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 стандарты и средства защиты данных. Вы изучите полнодисковое шифрование, защищённый контроль доступа, аппаратные резервные копии, состояние облачной безопасности и методы маскирования данных.

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/zashchita-dannykh/

Ваша дорожная карта обучения: стратегия защиты данных

- Различайте методы маскирования данных и токенизации.
- Внедрите шифрование накопителей при хранении и шифрование при передаче с помощью TLS.
- Разработайте автономные, изолированные от сети системы резервного копирования для защиты от программ-вымогателей.

ИНСТРУКЦИИ ПО ЗАЩИТЕ 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 данных. Завершите работу дополнительным заданием «Думай быстро».

ЗАЩИТА ДАННЫХ И БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ ХРАНИЛИЩ (ВВЕДЕНИЕ)

Защита данных охраняет корпоративные информационные активы с помощью маскирования, токенизации, шифрования баз данных в состоянии покоя и защищённых протоколов передачи. Создание изолированных от сети резервных копий помогает восстановить ключевые базы данных в случае активного вторжения.

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

Контрольная точка 1: Задание с выбором ответа

1. Для чего в основном нужно маскирование данных?

- A. Замена конфиденциальных идентификаторов вымышленными, но реалистичными символами для защиты конфиденциальности
- B. Сжатие больших файлов базы данных для экономии физического места на сервере
- C. Удаление старых писем с контактами клиентов из архивных систем резервного копирования
- D. Скрытие публичного IP-адреса сервера базы данных от интернет-сканирования

2. Какой механизм шифрует файлы, хранящиеся на жёстком диске сервера баз данных?

- A. Полнодисковое шифрование в состоянии покоя
- B. Протоколы рукопожатия сеансов TLS при передаче
- C. Правила пересылки серверов имён с динамическим DNS
- D. Многофакторная аутентификация с аппаратными ключами

3. Что представляют собой данные при передаче?

- A. Пакеты данных, перемещающиеся через сетевые роутеры и коммутаторы
- B. Журналы транзакций базы данных, хранящиеся на холодном резервном диске
- C. Архивные пользовательские файлы в изолированном облачном хранилище
- D. Статические системные файлы конфигурации в локальном хранилище настольного компьютера

4. Почему регулярная автономная резервная копия критически важна для защиты от программ-вымогателей?

- A. Даёт чистую автономную копию для восстановления файлов без выплаты выкупа
- B. Он не даёт хакерам сканировать конфигурации открытых портов
- C. Увеличивает скорость передачи данных в локальной сети
- D. Автоматизирует журналы согласия на cookie в браузерах

5. Что делает токенизация данных?

- A. Заменяет конфиденциальные номера карт неконфиденциальными случайными токенами
- B. Он направляет веб-трафик через несколько защищённых луковых узлов
- C. Сканирует системные каталоги на наличие вредоносного ПО по сигнатурам
- D. Проверяет время сеансов входа администраторов базы данных

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Маскирование данных необратимо изменяет записи базы данных в рабочих средах.

○ Верно ○ Неверно

7 Вопрос 7

7. Резервные копии вне площадки должны быть изолированы от основной корпоративной сети, чтобы предотвратить распространение программ-вымогателей.

○ Верно ○ Неверно

8 Вопрос 8

8. Сертификаты SSL/TLS защищают базы данных, шифруя данные, хранящиеся на физических носителях.

○ Верно ○ Неверно

9 Вопрос 9

9. Доступ к сети с нулевым доверием (ZTNA) проверяет личность каждого пользователя перед предоставлением доступа к базе данных.

○ Верно ○ Неверно

10 Вопрос 10

10. Токенизация на основе хранилища сохраняет исходные значения карт в защищённом центральном хранилище токенов.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Замена личных имён реалистичными заполнителями называется _____ данных.

2. Шифрование физических блоков хранилища защищает активы базы данных, когда они находятся _____ .

3. Протоколы TLS шифруют активные пакеты данных, находящиеся _____ .

4. Права на основе ролей ограничивают, какие пользователи могут получить _____ к базе данных.

5. Для восстановления чистых корпоративных файлов после инцидента нужна защищённая автономная _____ .

6. Аудит облачных конфигураций оценивает общее _____ безопасности организации.

СЛОВАРНЫЙ БАНК СЛОВ

В ПРОЦЕССЕ ПЕРЕДАЧИ | В СОСТОЯНИИ ПОКОЯ | ДОСТУП | ИНЦИДЕНТ
МАСКИРОВАНИЕ | МИНИМИЗАЦИЯ | РЕЗЕРВНАЯ КОПИЯ | СОСТОЯНИЕ

Напишите свои ответы здесь:

1. | **2.**

3. | **4.**

5. | **6.**

Контрольная точка 4: Сопоставление понятий о безопасности

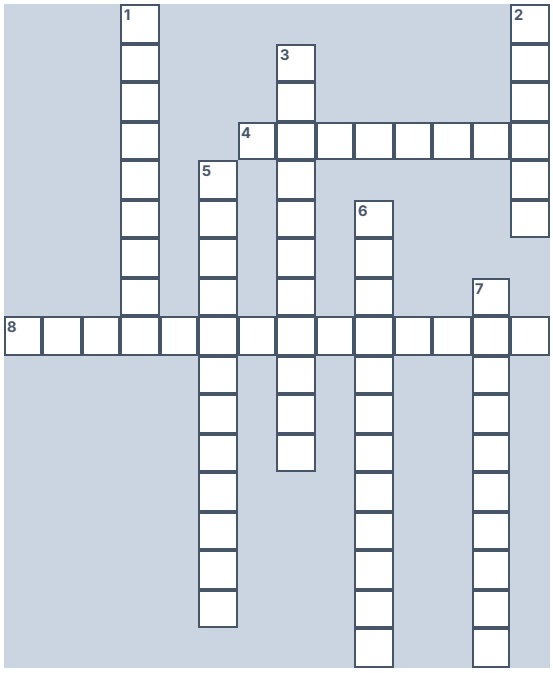
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. ШИФРОВАНИЕ	A	Создание защищённых внешних копий данных для восстановления при сбоях системы.
☐	2. РЕЗЕРВНАЯ КОПИЯ	B	Преобразование открытого текста в нечитаемый шифртекст, чтобы перехваченные данные оставались конфиденциальными.
☐	3. МИНИМИЗАЦИЯ	C	Совокупное состояние безопасности и готовность к защите облака организации.
☐	4. ДОСТУП	D	Соблюдение нормативных стандартов, таких как GDPR или CCPA, при управлении частной информацией пользователей.
☐	5. СОСТОЯНИЕ	E	Инцидент безопасности, при котором защищённые данные получают или раскрывают без разрешения.
☐	6. УТЕЧКА	F	Ограничение прав чтения и записи в базе данных ролями аутентифицированных пользователей.
☐	7. СООТВЕТСТВИЕ ТРЕБОВАНИЯМ	G	Замена конфиденциальных символов в полях базы данных для защиты личных данных.
☐	8. МАСКИРОВКА	H	Ограничение сбора персональных данных абсолютным минимумом, необходимым для работы.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

4. Событие безопасности, при котором защищённые данные становятся доступны или раскрываются без разрешения (8)

8. Создание защищённых внешних копий данных для восстановления при сбоях системы (14)

ПО ВЕРТИКАЛИ

1. Совокупный статус безопасности и готовность организации к защите в облаке (9)

2. Ограничение прав чтения и записи в базе данных ролями аутентифицированных пользователей (6)

3. Ограничение сбора персональных данных абсолютным минимумом, необходимым для работы (11)

5. Выполнение нормативных требований, таких как GDPR или CCPA, при обращении с частной информацией пользователей (12)

6. Замена конфиденциальных символов в полях базы данных для защиты личностей (12)

7. Преобразование открытого текста в нечитаемый шифртекст, чтобы перехваченные данные оставались конфиденциальными (10)

Контрольная точка 5, альтернативный вариант: Доступные подсказки к кроссворду

Пользователи программ чтения с экрана и клавиатуры могут вводить ответы на кроссворд прямо в текстовые поля ниже.

ПО ГОРИЗОНТАЛИ

4 по горизонтали: Событие безопасности, при котором защищённые данные становятся доступны или раскрываются без разрешения (8 букв):

8 по горизонтали: Создание защищённых внешних копий данных для восстановления при сбоях системы (14 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Совокупный статус безопасности и готовность организации к защите в облаке (9 букв):

2 по вертикали: Ограничение прав чтения и записи в базе данных ролями аутентифицированных пользователей (6 букв):

3 по вертикали: Ограничение сбора персональных данных абсолютным минимумом, необходимым для работы (11 букв):

5 по вертикали: Выполнение нормативных требований, таких как GDPR или CCPA, при обращении с частной информацией пользователей (12 букв):

6 по вертикали: Замена конфиденциальных символов в полях базы данных для защиты личностей (12 букв):

7 по вертикали: Преобразование открытого текста в нечитаемый шифртекст, чтобы перехваченные данные оставались конфиденциальными (10 букв):

Контрольная точка 6: Поиск скрытых слов

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

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

СПИСОК СЛОВ СЛОВАРЯ

ШИФРОВАНИЕ РЕЗЕРВНАЯКОПИЯ МИНИМИЗАЦИЯ ДОСТУП СОСТОЯНИЕ ИНЦИДЕНТ СООТВЕТСТВИЕ МАСКИРОВАНИЕ

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. РЕЗЕРВНАЯКОПИЯ**
- **C. МИНИМИЗАЦИЯ**
- **D. ДОСТУП**
- **E. СОСТОЯНИЕ**
- **F. ИНЦИДЕНТ**
- **G. СООТВЕТСТВИЕ**
- **H. МАСКИРОВАНИЕ**

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Событие безопасности, при котором защищённые данные становятся доступны или раскрываются без разрешения.

_____ 2. Замена конфиденциальных символов в полях базы данных для защиты личностей.

_____ 3. Ограничение прав чтения и записи в базе данных ролями аутентифицированных пользователей.

_____ 4. Совокупный статус безопасности и готовность организации к защите в облаке.

_____ 5. Выполнение нормативных требований, таких как GDPR или CCPA, при обращении с частной информацией пользователей.

_____ 6. Ограничение сбора персональных данных абсолютным минимумом, необходимым для работы.

_____ 7. Преобразование открытого текста в нечитаемый шифртекст, чтобы перехваченные данные оставались конфиденциальными.

_____ 8. Создание защищённых внешних копий данных для восстановления при сбоях системы.

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. **МЯИМИИНЦАЗИ** _____

3. **СЯООНЕТИС** _____

4. **ИСВОТЕЕВТСОТ** _____

5. **КЗПЕАЯРЯВОНРИЕ** _____

6. **УТДСПО** _____

7. **ИТДЕННИЦ** _____

8. **ВСИНОЕМРАИАК** _____

Дополнительное задание: Думай быстро

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

1	То, для чего вы делаете резервные копии			
2	Слова, связанные с кибербезопасностью			
3	Люди, которым разрешено видеть конфиденциальные данные			
4	Способы безопасного удаления данных			
5	Места, где хранятся данные			
6	То, что следует шифровать			
7	Данные, которые должна защищать больница			
8	Виды резервного копирования			
9	Информация, которой нельзя делиться			
10	Тревожные признаки в электронном письме			
11	Безопасные привычки, которые можно начать уже сегодня			
12	Люди, у которых можно попросить помощи по ИТ			
13	Устройства, которые могут быть взломаны			
14	Способы защиты данных			
15	То, что может уничтожить данные			

Контрольная точка 8: Кейсы по кибербезопасности

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: ПЕРЕХОД КОРПОРАТИВНОЙ БАЗЫ ДАННЫХ НА ШИФРОВАНИЕ ПРИ ХРАНЕНИИ



Ситуация: Интернет-магазин хранит базы данных транзакций в облачном хранилище без полного шифрования диска. Недавний аудит соответствия выявил в этом серьёзный риск безопасности данных по CCPA. Разработайте архитектуру восстановления.

Вопрос для обсуждения: Проанализируйте риски соответствия CCPA и предложите стратегию шифрования данных в состоянии покоя.

КЕЙС 2: СДЕРЖИВАНИЕ ПРОГРАММЫ-ВЫМОГАТЕЛЯ И ВОССТАНОВЛЕНИЕ ДАННЫХ



Ситуация: Активная атака программы-вымогателя шифрует сетевые диски в корпоративной локальной сети. Администратор обнаружил заражение на ранней стадии. Спланируйте шаги по локализации и восстановлению.

Вопрос для обсуждения: Опишите немедленные действия по локализации и спланируйте безопасный процесс восстановления.

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	27	1	11	20	6		13	10	25	15	29	6

5	1	15	15	29	6		15	1	5	6	8	15	29	14

12	16	15	20	18	16	13	6	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 защита данных?

Это процесс защиты личных и бизнес-данных от несанкционированного доступа, потери или повреждения с помощью технических средств контроля.

Q2: Почему важно полнодисковое шифрование?

Защищает сохранённые блоки данных на физических дисках, не позволяя никому прочитать данные при физической краже жёсткого диска.

Q3: Чем отличается шифрование данных при хранении от шифрования при передаче?

Шифрование неактивных данных защищает файлы, хранящиеся на дисках, а шифрование передаваемых данных защищает активные сетевые пакеты, проходящие через маршрутизаторы.

Q4: Что такое маскирование данных?

Заменяет чувствительные сведения (например, номера кредитных карт) вымышленными, но реалистичными данными для тестирования без раскрытия реальных записей.

Q5: Почему важна автономная резервная копия?

Хранит чистую копию ваших файлов в изоляции от сети, что помогает защитить резервные копии от шифрования программой-вымогателем.

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

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q6: Что такое хранилище токенизации данных?

Защищённая изолированная база данных, сопоставляющая случайные токены с исходными конфиденциальными значениями (например, номерами банковских карт).

Q7: Что означает доступ к базе данных по принципу нулевого доверия?

Это означает проверку личности каждого пользователя и состояния устройства при каждом входе вместо доверия любому, кто находится внутри сети.

Q8: Как TLS защищает данные при передаче?

TLS шифрует полезные данные сеанса TCP, не позволяя злоумышленникам в общедоступных сетях перехватывать или изменять передаваемые пакеты.

Q9: Что такое аудит доступа к базе данных?

Непрерывная запись запросов к базе данных и входов в систему для выявления шаблонов несанкционированного доступа или аномалий безопасности.

Q10: Что такое аудит состояния облачной безопасности?

Процесс анализа облачных конфигураций для выявления открытых портов, неверно настроенных правил доступа и пробелов в соответствии требованиям безопасности.

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 конвертное шифрование?

Шифрует данные ключом данных, а затем шифрует этот ключ данных мастер-ключом, упрощая хранение и ротацию ключей.

Q2: Что такое гомоморфное шифрование?

Продвинутый метод шифрования, позволяющий выполнять операции прямо над зашифрованными данными без предварительной расшифровки.

Q3: Зачем используется шифрование столбцов базы данных?

Шифрует отдельные чувствительные столбцы (например, номера соцстрахования) по отдельности, защищая их, даже если администраторы получают общий доступ на чтение таблицы.

Q4: Что такое предотвращение утечки данных (DLP)?

Программа, отслеживающая точки выхода из сети, чтобы обнаруживать и блокировать несанкционированную исходящую передачу конфиденциальных файлов.

Q5: Как резервные копии WORM (однократная запись, многократное чтение) защищают от программ-вымогателей?

Резервные копии WORM не позволяют удалять или изменять файлы в течение заданного срока, что мешает программам-вымогателям зашифровать существующие копии.

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

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

Q6: Чем опасно повторное использование ключей?

Использование одного и того же криптографического ключа в разных базах данных означает, что компрометация одного ключа раскрывает все базы данных.

Q7: Как токенизация базы данных помогает соблюдать CCPA?

Токены псевдонимизируют записи в нерабочих системах и ограничивают последствия утечки, но токенизированные данные всё равно могут быть персональной информацией.

Q8: Почему классификация данных так важна?

Классифицирует файлы по уровню чувствительности, помогая организациям применять самое сильное шифрование и средства контроля доступа к данным высокого риска.

Q9: Какую роль играет смена ключей?

Регулярное обновление ключей шифрования ограничивает объём исторических данных, которые окажутся доступны, если один из ключей в итоге будет взломан.

Q10: Как защищённые анклавы защищают запросы к базе данных в памяти?

Защищённые анклавы изолируют операции с запросами в блоках памяти, защищённых процессором, не позволяя администраторам хоста видеть открытый текст в ОЗУ.

Часть 11: 10 реальных фактов и выводов о кибербезопасности

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

1. АНАЛИЗ БЕЗОПАСНОСТИ

Положения GDPR вступили в силу в мае 2018 года и изменили то, как сайты по всему миру управляют согласием на cookie и реестрами персональных данных.

2. АНАЛИЗ БЕЗОПАСНОСТИ

Штраф за нарушение GDPR может достигать 20 миллионов евро или 4% глобального оборота, что означает существенные юридические риски. [4]

3. АНАЛИЗ БЕЗОПАСНОСТИ

CCPA вступил в силу в январе 2020 года и закрепил в США новаторские права потребителей на цифровую конфиденциальность.

4. АНАЛИЗ БЕЗОПАСНОСТИ

Минимизация данных уменьшает объём хранимых в базе данных данных, снижая эксплуатационные расходы на серверы и масштаб последствий утечки.

5. АНАЛИЗ БЕЗОПАСНОСТИ

Криптографическое уничтожение решает проблему удаления резервных копий путём удаления ключей, а не редактирования файлов исторических резервных копий на лентах.

6. АНАЛИЗ БЕЗОПАСНОСТИ

Сейчас в большинстве стран мира приняты законы о защите персональных данных для защиты прав потребителей на конфиденциальность.

7. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Формы согласия с заранее отмеченными флажками прямо запрещены определениями европейских нормативных актов о конфиденциальности данных.

8. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

GDPR требует сообщать о нарушениях защиты персональных данных надзорному органу в течение 72 часов с момента, как стало о них известно, если это возможно. [3]

9. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Хеширование паролей медленными алгоритмами, такими как bcrypt или Argon2, значительно затрудняет офлайн-подбор украденных хешей. [6]

10. АНАЛИЗ БЕЗОПАСНОСТИ

Неактивные данные — это сохранённые файлы баз данных, а передаваемые данные — это пакеты, которые в данный момент движутся через сетевые маршрутизаторы.

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 800-88 Rev. 2, Guidelines for Media Sanitization.

https://csrc.nist.gov/pubs/sp/800/88/r2/final

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

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

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.

https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.

https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).

https://cppa.ca.gov/faq.html

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

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

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 Вопрос 1

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Для чего в основном нужно маскирование данных? → Замена конфиденциальных идентификаторов вымышленными, но реалистичными символами для защиты конфиденциальности

2 Вопрос 2

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Какой механизм шифрует файлы, хранящиеся на жёстком диске сервера баз данных? → Полнодисковое шифрование в состоянии покоя

3 Вопрос 3

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что представляют собой данные при передаче? → Пакеты данных, перемещающиеся через сетевые роутеры и коммутаторы

4 Вопрос 4

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Почему регулярная автономная резервная копия критически важна для защиты от программ-вымогателей? → Даёт чистую автономную копию для восстановления файлов без выплаты выкупа

5 Вопрос 5

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что делает токенизация данных? → Заменяет конфиденциальные номера карт неконфиденциальными случайными токенами

Ответы: контрольная точка 2 – верно или неверно

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

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Маскирование изменяет тестовые копии или скрывает значения во время запроса; рабочие записи остаются без изменений.

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

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Резервные копии вне площадки должны быть изолированы от основной корпоративной сети, чтобы предотвратить распространение программ-вымогателей.

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

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Сертификаты TLS защищают данные при передаче; данные в состоянии покоя требуют шифрования диска, файлов или базы данных.

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

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Доступ к сети с нулевым доверием (ZTNA) проверяет личность каждого пользователя перед предоставлением доступа к базе данных.

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

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Токенизация на основе хранилища хранит исходные значения в защищённом хранилище токенов, где каждый токен сопоставляется со своими данными.

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

B 1. ШИФРОВАНИЕ	A 2. РЕЗЕРВНАЯ КОПИЯ	H 3. МИНИМИЗАЦИЯ	F 4. ДОСТУП
C 5. СОСТОЯНИЕ	E 6. УТЕЧКА	D 7. СООТВЕТСТВИЕ ТРЕБОВАНИЯМ	G 8. МАСКИРОВКА

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 МАСКИРОВАНИЕ	2 В СОСТОЯНИИ ПОКОЯ	3 В ПРОЦЕССЕ ПЕРЕДАЧИ	4 ДОСТУП
5 РЕЗЕРВНАЯ КОПИЯ	6 СОСТОЯНИЕ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 F – ИНЦИДЕНТ	2 H – МАСКИРОВАНИЕ	3 D – ДОСТУП	4 E – СОСТОЯНИЕ
5 G – СООТВЕТСТВИЕ	6 C – МИНИМИЗАЦИЯ	7 A – ШИФРОВАНИЕ	8 B – РЕЗЕРВНАЯКОПИЯ

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

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

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

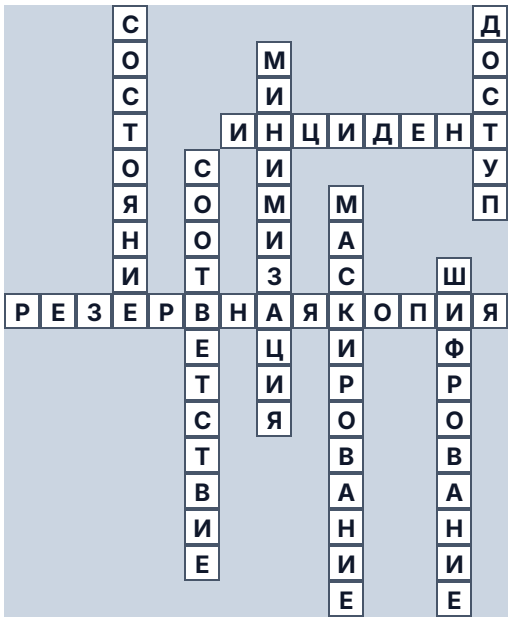
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

4 по горизонтали: ИНЦИДЕНТ Событие безопасности, при котором защищённые данные становятся доступны или раскрываются без разрешения (8 букв)

8 по горизонтали: РЕЗЕРВНАЯКОПИЯ Создание защищённых внешних копий данных для восстановления при сбоях системы (14 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: СОСТОЯНИЕ Совокупный статус безопасности и готовность организации к защите в облаке (9 букв)

2 по вертикали: ДОСТУП Ограничение прав чтения и записи в базе данных ролями аутентифицированных пользователей (6 букв)

3 по вертикали: МИНИМИЗАЦИЯ Ограничение сбора персональных данных абсолютным минимумом, необходимым для работы (11 букв)

5 по вертикали: СООТВЕТСТВИЕ Выполнение нормативных требований, таких как GDPR или CCPA, при обращении с частной информацией пользователей (12 букв)

6 по вертикали: МАСКИРОВАНИЕ Замена конфиденциальных символов в полях базы данных для защиты личностей (12 букв)

7 по вертикали: ШИФРОВАНИЕ Преобразование открытого текста в нечитаемый шифртекст, чтобы перехваченные данные оставались конфиденциальными (10 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. И А В О И Ш Н Е Р Ф — **ШИФРОВАНИЕ**
2. М Я И М И И Н Ц А З И — **МИНИМИЗАЦИЯ**
3. С Я О О Н Е Т И С — **СОСТОЯНИЕ**
4. И С В О Т Е Е В Т С О Т — **СООТВЕТСТВИЕ**
5. К З П Е А Я Р Я В О Н Р И Е — **РЕЗЕРВНАЯКОПИЯ**
6. У Т Д С П О — **ДОСТУП**
7. И Т Д Е Н Н И Ц — **ИНЦИДЕНТ**
8. В С И Н О Е М Р А И А К — **МАСКИРОВАНИЕ**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ЗАЩИЩАЙТЕ ЛИЧНЫЕ ДАННЫЕ НАДЕЖНЫМ КОНТРОЛЕМ"

Ответы к кейсам

A Кейс 1: Переход корпоративной базы данных на шифрование при хранении

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: интернет-магазин хранит базы данных транзакций в облачном хранилище без полного шифрования диска. Недавний аудит соответствия требованиям признал это серьёзным риском для безопасности данных по CCPA. Разработайте архитектуру восстановления.
- Рекомендуемая стратегия и решение: Внедрите полнодисковое шифрование AES-256 для данных в состоянии покоя на всех файловых системах. Используйте централизованную службу управления ключами (KMS) с автоматической ротацией и строгие политики IAM для контроля доступа к расшифровке.

B Кейс 2: Сдерживание программы-вымогателя и восстановление данных

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: активная атака программы-вымогателя шифрует сетевые диски в корпоративной локальной сети. Администратор обнаружил заражение на раннем этапе. Составьте план шагов по сдерживанию и восстановлению.
- Рекомендуемая стратегия и решение: Немедленно изолируйте скомпрометированный сегмент. Отформатируйте затронутые конечные точки и восстановите данные из последней автономной резервной копии WORM (однократная запись, многократное чтение). Проверьте целостность копии, прежде чем снова подключать системы.