

Английский

Содержание

| | | |
|----------|-------------------|----------|
| 1 | Задания | 2 |
| 1.1 | Словарь | 3 |

1 Задания

1.1 Задание 1

1) A biological virus is a very small, simple organism that infects living cells, known as the host, by **attaching** itself to them and using them to **reproduce** itself. This often **causes harm** to the host cells.

Перевод: Биологический вирус — это очень маленький, простой организм, который заражает живые клетки, известные как хозяева, *прикрепляясь* к ним и используя их для *воспроизводства* себя. Это часто *наносит вред* клеткам хозяина.

2) The virus may also contain a **payload** that remains dormant until a trigger event activates it, such as the user pressing a particular key.

Перевод: Вирус также может содержать *загрузку*, которая остается неактивной до тех пор, пока какое-либо триггерное событие не активирует ее, например, нажатие пользователем определенной клавиши.

3) To be a virus, a program only needs to have a **reproduction routine** that enables it to infect other programs.

Перевод: Чтобы быть вирусом, программе нужно иметь *рутину воспроизводства*, которая позволяет ей заражать другие программы.

4) For the system to work, two parties **engaging** in a secure transaction must know each other's **public** keys. **Private** keys, however, are closely guarded secrets known only to their owners.

Перевод: Для работы системы две стороны, *участвующие* в безопасной транзакции, должны знать друг друга *открытые* ключи. *Закрытые* ключи, однако, являются строго охраняемыми секретами, известными только их владельцам.

5) The dynamics of the Web dictate that a user **authentication** system must exist. This can be done using digital **certificates**.

Перевод: Динамика Интернета диктует, что должна существовать система *аутентификации* пользователей. Это может быть сделано с использованием цифровых *сертификатов*.

6) To make the right decisions we must be able to **handle** and administer information safely and securely. It also means we must have systems that are **available** whenever we need them, and that will produce information we can **rely** on.

Перевод: Чтобы принимать правильные решения, мы должны уметь *обрабатывать* и обеспечивать безопасность информации. Это также означает, что у нас должны быть системы, которые будут *доступны* всякий раз, когда нам это нужно, и которые будут производить информацию, на которую мы можем *полагаться*.

7) A large percentage of computer data loss is **attributed** to accidental error. Accountability for use of assets (systems, data) is a strong **deterrent** to any wrongdoing.

Перевод: Большой процент потери компьютерных данных *приписывается* случайным ошибкам. Ответственность за использование активов (систем, данных) является сильным *сдерживающим*

фактором для любого правонарушения.

8) A successful security program consists of a number of **interrelated key elements**, each of which has a definite purpose and is supported by management.

Перевод: Успешная программа безопасности состоит из множества *взаимосвязанных ключевых элементов*, каждый из которых имеет определенную цель и поддерживается руководством.

9) A **disgruntled** employee is one who works for or used to work for an organization and wants to cause harm or embarrassment to the organization itself.

Перевод: *Недовольный* сотрудник — это тот, кто работает или работал в организации и хочет причинить вред или смущение самой организации.

10) The opportunity for a dishonest or disgruntled employee to **exploit** the organization increases as the network grows.

Перевод: Возможность для недобросовестного или недовольного сотрудника *эксплуатировать* организацию возрастает по мере роста сети.

11) Physical protection of network components from theft and from **hostile environment** must be considered.

Перевод: Физическая защита компонентов сети от кражи и от *враждебной среды* должна быть учтена.

12) The biggest **exposure** of information systems is due to errors caused by honest employees who make mistakes in data entry, data update changes to applications, etc.

Перевод: Наибольшая *подверженность* информационных систем возникает из-за ошибок, допущенных добросовестными сотрудниками, которые делают ошибки при вводе данных, изменениях обновление данных в приложениях и т. д.

1.2 Задание 2

1.3 Словарь

Handle — обрабатывать; управлять (применяется в контексте управления информацией или системами).

Exploit — эксплуатировать; использовать (часто используется в контексте уязвимостей или ресурсов).

Public — открытый; публичный (относится к информации или ключам, доступным для всех).

Authentication — аутентификация; удостоверение личности (процесс проверки личности пользователя).

Disgruntled — недовольный (человек, работающий в организации и имеющий негативные чувства, часто в контексте потенциальной угрозы).

Exposure — подверженность; открытость (в контексте рисков и уязвимостей).

Payload — загрузка; полезная нагрузка (вирусная программа, которая выполняет задачи

после заражения).

Interrelated key elements — взаимосвязанные ключевые элементы (части системы безопасности, которые работают вместе).

Attributed — приписываемый; относимый (часто используется в контексте причин и следствий).

Available — доступный (информация или ресурсы, которые могут быть использованы).

Hostile environment — враждебная среда (условия или ситуации, представляющие угрозу безопасности).

Private — частный (информация, доступная только определенным лицам или защищенная от общего использования).

Attaching — прикрепление (процесс соединения вируса с программой).

Rely — полагаться (на что-то; например, на безопасность систем или информации).

Reproduce — воспроизводить (процесс создания копий чего-либо, как в случае вирусов).

Deterrent — сдерживающий фактор (что-то, что предотвращает нежелательные действия, например, преступления).

Reproduction routine — рутина воспроизводства (алгоритм, позволяющий вирусу создавать свои копии).

Causes harm — причиняет вред (описывает действия, которые наносят ущерб).

Engaging — вовлечь; привлечь (участие в чем-то; например, в транзакции).

Certificates — сертификаты (цифровые документы, используемые для аутентификации и безопасности).

Information assets — информационные активы

Encryption — шифрование

Payload — полезная нагрузка

Cost/benefit — затраты/выгода

Infects — заражает

Tenets — принципы / основополагающие положения

Unauthorized — несанкционированный

Public key — открытый ключ

Reproduction routine — рутина воспроизводства

Host — хост / узел

Tampered — подделанный / искаженный

Protecting — защита

Security objectives — цели безопасности

Protective — защитный

Encrypted — зашифрованный

Sequence — последовательность

Message integrity — целостность сообщения

Occurrence — случ occurrence

Destination — пункт назначения

Gibberish — бессмыслица

Executed — выполненный / осуществленный

Reproduce — воспроизводить

Impostor — самозванец

Authentication — аутентификация