
1 Exercise 2.17

1.1 Протягом багатьох років люди турбувалися про безпеку своїх комп'ютерів.

People have worried about the security of their computers for many years.

1.2 Питання комп'ютерної безпеки завжди були важливим фактором у розробці та застосуванні комп'ютерних технологій в усьому суспільстві.

Computer security concerns have always been a significant factor in the development and application of computer technology throughout society.

1.3 На ранній стадії розвитку комп'ютерів безпека була важливим фактором, оскільки обчислення, що служили причиною їх розробки, мали військове застосування.

In the early development of computers, security was a strong factor since the computations that motivated their development had military applications.

1.4 Але самі комп'ютери були такими великими і нечисленними, що захистити їх було відносно легко, просто обмеживши фізичний доступ до них їх програмістами та операторами.

But the computers themselves were so big and so few that they were relatively easy to protect simply by limiting physical access to them to their programmers and operators.

1.5 Комп'ютери постійно взаємодіють один з одним; комп'ютер, який не підключений до мережі — неповноцінний.

Computers constantly communicate with one another; an isolated computer is crippled.

1.6 Значення і зміст поняття «комп'ютерна безпека» з роками також зазнавав змін.

The meaning and implications of “computer security” have changed over the years as well.

1.7 Сьогодні комп'ютерною безпекою називають галузь обчислювальної техніки, предметом якої є запобігання і виявлення незаконного використання вашого комп'ютера.

Today computer security refers to the branch of computer technology that deals with preventing and detecting unauthorized use of your computer.

1.8 Запобіжні заходи допомагають вам не дозволити неправомочним користувачам отримати доступ до будь-якої частини вашої комп'ютерної системи.

Prevention measures help you to stop unauthorized users from accessing any part of your computer system.

1.9 Виявлення допомагає вам визначити, чи намагався хтось «зламати» вашу систему, чи вдалося їм це і що вони могли зробити.

Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

1.10 Мета комп'ютерної безпеки включає в себе захист інформації та власності від викрадення, пошкодження або природного лиха, в той самий час даючи можливість цим самим інформації та власності залишатися доступними і корисними для обраних користувачів.

The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.

1.11 Термін «комп'ютерна безпека» означає сукупність процесів і механізмів, за допомогою яких конфіденційна і цінна інформація та послуги захищаються від опублікування, псування та знищення ненадійними особами або внаслідок незаконної діяльності чи незапланованих подій.

The term computer system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering and unplanned events respectively.

1.12 Стратегії та методики комп'ютерної безпеки часто відрізняються від більшості інших комп'ютерних технологій через її дещо невиразну мету запобігання небажаний поведінці комп'ютера замість уможливлення його бажаної поведінки.

The strategies and methodologies of computer security often differ from most other computer technologies because of its somewhat elusive objective of preventing unwanted computer behavior instead of enabling wanted computer behavior.

1.13 Основні технічні сфери комп'ютерної безпеки зазвичай виражаються ініціалами CIA.

The major technical areas of computer security are usually represented by the initials CIA.

1.14 Конфіденційність означає, що до інформації не можуть мати доступ неправомочні суб'єкти.

Confidentiality means that information cannot be accessed by unauthorized parties.

1.15 Необхідність тримати інформацію в секреті виникає через використання комп'ютерів у пов'язаних із секретністю галузях, таких як державне управління та промисловість.

The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry.

1.16 Військові та цивільні урядові установи часто обмежують доступ до інформації тими, кому ця інформація необхідна.

Military and civilian institutions in the government often restrict access to information to those who need that information.

1.17 Цілісністю називають достовірність даних або ресурсів, і зазвичай про неї говорять в контексті запобігання недоречним або несанкціонованим змінам.

Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change.

1.18 Цілісність означає, що інформація захищена від несанкціонованих змін, які не можуть бути виявлені правомочними користувачами.

Integrity means that information is protected against unauthorized changes that are not detectable to authorized users.

1.19 Багато випадків хакерства порушують цілісність баз даних та інших ресурсів.

Many incidents of hacking compromise the integrity of databases and other resources.

1.20 Доступністю називають можливість користуватися потрібною інформацією або ресурсом.

Availability refers to the ability to use the information or resource desired.

1.21 Аспектом доступності в тому, що стосується безпеки є те, що хтось може зумисно влаштувати заборону доступу до даних або послуги, зробивши їх недоступними.

The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable.

1.22 Доступність означає, що до ресурсів мають доступ правомочні суб'єкти.

Availability means that resources are accessible by authorized parties.

1.23 Атаки типу «відмова обслуговування», що іноді є темою загальнонаціональних новин, є нападами на доступність.

“Denial of service” attacks, which are sometimes the topic of national news, are attacks against availability.

1.24 Аутентифікація означає, що користувач справді є тим, ким він стверджує.

Authentication means that users are who they claim to be.

1.25 Без належної аутентифікації неможливо визначити, чи правочинними є зроблені зміни.

Without proper authentication it is not possible to determine whether the applied modifications have been properly authorized.

1.26 Забезпечення контролю доступу означає не тільки те, що користувачі можуть мати доступ лише до тих ресурсів і послуг, на які вони мають право, але також і те, що їм не заборонені ресурси, на які вони обгрунтовано сподіваються мати доступ.

Maintaining access control means not only that users can access only those resources and services to which they are entitled, but also that they are not denied resources that they legitimately can expect to access.

1.27 Неможливість заперечення авторства означає, що особа, яка надсилає повідомлення, не може заперечувати, що вона його надіслала, і, навпаки, що особа, яка отримала повідомлення, не може заперечувати, що вона його отримала.

Nonrepudiation refers to assuring that a person who sends a message cannot deny that they sent it, and, conversely, that a person who has received a message cannot deny that they received it.

1.28 Приватність, яка може розглядатися як конфіденційність стосовно окремої особи, можливо є найважливішим аспектом комп'ютерної безпеки для щоденних користувачів Інтернету.

Privacy, which can be viewed as confidentiality applied to an individual, is perhaps the most important aspect of computer security for everyday Internet users.

1.29 Приватність в Інтернеті — це захист особистої інформації, навіть якщо ця інформація не видається конфіденційною.

Privacy on the Internet is about protecting one's personal information even if the information does not seem sensitive.

1.30 Зараз дуже важливо, щоби людина могла контролювати, яку інформацію про неї збирають, як, ким і з якою метою її використовують.

Now it's very important that an individual is able to control which information about them is collected, how it is used, who may use it and what purpose it is used for.