Під визначення засобів захисту інформаціїпідпадають:
1) засоби виявлення зловмисної активності
2) засоби забезпечення відмовостійкості
3) засоби забезпечення гарантоздатності
4) засоби контролю за ефективністю захисту інформації
5) інша відповідь

Політика безпеки:
1) фіксує правила розмежування доступу
2) відображає підхід організації до захисту своїх інформаційних активів
3) відображає витрати на закуплю засобів захисту
4) описує засоби захисту керівництва організації
5) інша відповідь

Принцип посилення найслабшої ланки можна переформулювати як:
1) принцип рівносильності оборони
2) принцип видалення слабкої ланки
3) принцип виявлення головної ланки, вхопившись за яку, можна витягнути весь ланцюг
4) безпеку, що верифікується
5) інша відповідь

Тунелювання може використовуватися на наступному рівні еталонної семирівневої моделі OSI:
1) мережний
2) сеансовий
3) програмний
4) апаратний
5) інша відповідь

Системи аналізу захищеності допомагають запобігти:
1) відомим атакам
2) новим видам атак
3) нетиповій поведінці користувачів
4) тунелюванню
5) інша відповідь

Екранування на мережному та транспортному рівнях може забезпечити:
1) типову поведінку користувачів
2) розмежування доступу до мережних адрес
3) вибіркове виконання команд прикладного протоколу
4) контроль обсягу даних, переданих через TCP-з'єднання
5) інша відповідь

«Демілітаризована зона», зазвичай, розташовується:
1) перед зовнішнім міжмережним екраном
2) між внутрішнім та зовнішнім міжмережними екранами
3) за внутрішнім міжмережним екраном
4) на виході в мережу Інтернет
5) інша відповідь

Міжмережний екран виконує функції:
1) розмежування доступу
2) полегшення доступу
3) ускладнення доступу
4) відновлення доступу
5) інша відповідь

Криптографія забезпечує:
1) контроль конфіденційності
2) контроль цілісності
3) контроль доступу
4) контроль актуальності
5) інша відповідь

Цифровий сертифікат містить:
1) ім'я користувача
2) пароль користувача
3) відкритий ключ користувач
4) таємний (закритий) ключ користувача
5) інша відповідь

До основних понять рольового управління доступом входять:
1) об'єкт, суб'єкт, метод
2) об'єкт, метод, засіб
3) об'єкт, суб'єкт
4) метод, засіб, суб’єкт
5) інша відповідь

Що з наведеного є поняттям рольового управління:
1) власник ролі
2) виконавець ролі
3) користувачі ролі
4) роль
5) інша відповідь

Аутентифікація на основі пароля, переданого через мережу в зашифрованому вигляді, забезпечує захист від:
1) перехоплення
2) відтворення
3) атак на доступність
4) усіх перерахованих типів атак
5) інша відповідь

Контроль цілісності може використовуватись для:
1) попередження порушень інформаційної безпеки
2) виявлення порушень інформаційної безпеки
3) локалізації наслідків порушеньінформаційної безпеки
4) екранування інформації
5) інша відповідь

Для забезпечення інформаційної безпеки мережних конфігурацій слід керуватися принципом:
1) використання власних ліній зв'язку;
2) забезпечення конфіденційності та цілісності при мережних взаємодіях;
3) повного аналізутрафіку
4) екранування інформації
5) інша відповідь

Для забезпечення інформаційної безпеки мережних конфігурацій слід керуватися принципом:
1) використання власних ліній зв'язку
2) вироблення та здійснення єдиної політики безпеки
3) уніфікація апаратно-програмних платформ
4) мінімізація кількості додатків, що використовуються
5) інша відповідь

До етапів процесу планування відновлювальних робіт входять:
1) ситуаційне керування
2) визначення переліку можливих аварій
3) проведення випробувань аварій
4) стрес-тести
5) інша відповідь

Протоколювання та аудит **не**можуть використовуватись для:
1) попередження порушень інформаційної безпеки
2) виявлення порушеньінформаційної безпеки
3) відновлення режиму інформаційної безпеки
4) фіксування порушень інформаційної безпеки
5) інша відповідь

До принципів управління персоналом входять:
1) мінімізація привілеїв
2) мінімізація зарплати
3) максимізація плати
4) преміювання
5) інша відповідь

Перший крок у аналізі загроз – це:
1) ідентифікація загроз
2) автентифікація загроз
3) авторизація загроз
4) усунення загроз
5) інша відповідь

Рольове управління доступом використовує такий засіб об'єктно-орієнтованого підходу:
1) інкапсуляція
2) успадкування
3) поліморфізм
4) наслідування функцій
5) інша відповідь

Інформаційний ризик є функцією:
1) розміру можливої шкоди
2) числа користувачів інформаційної системи
3) статутного капіталу організації
4) розмірності інформаційних активів
5) інша відповідь

До цілей політики безпеки верхнього рівня входять:
1) формулювання адміністративних рішень щодо найважливіших аспектів реалізації програми безпеки
2) вибір методів автентифікації користувачів
3) вибір методів авторизації користувачів
4) забезпечення бази для дотримання законів та правил
5) інша відповідь

Політика безпеки будується на основі:
1) загальних уявлень про інформаційну систему організації
2) вивчення політик родинних організацій
3) аналізу ризиків
4) моніторингу якості
5) інша відповідь

У рамках політики безпеки нижнього рівня здійснюються:
1) стратегічне планування
2) тактичне планування
3) відстеження слабких місць захисту
4) вивчення політик родинних організацій
5) інша відповідь

До цілей політики безпеки верхнього рівня входить:
1) управління ризиками
2) визначення відповідальних за інформаційні послуги
3) визначення заходів покарання за порушення політики безпеки
4) вивчення політик родинних організацій
5) інша відповідь

До цілей політики безпеки верхнього рівня **не**входить:
1) рішення сформувати чи переглянути комплексну програму безпеки
2) забезпечення бази для дотримання законів та правил
3) забезпечення конфіденційності поштових повідомлень
4) усе перераховане
5) інша відповідь

Рівень безпеки А відповідно до «Помаранчевої книги» характеризується:
1) довільним керуванням доступом
2) примусовимкеруванням доступом
3) відсутністю керування доступом
4) безпекою, що верифікується
5) інша відповідь

Відповідно до «Помаранчевої книги» політика безпеки включає такий елемент:
1) периметр безпеки
2) мітка безпеки
3) сертифікат безпеки
4) протокол безпеки
5) інша відповідь

Властивість інформаційних ресурсів, що полягає в їх незмінності в процесі передачі або зберігання - це:
1) цілісність
2) доступність
3) актуальність
4) конфіденційність
5) інша відповідь

Властивість інформаційних ресурсів, що полягає у їх недоступності для не уповноважених осіб - це:
1) цілісність
2) доступність
3) актуальність
4) конфіденційність
5) інша відповідь

Властивість інформаційних ресурсів, що полягає у їх отриманні та використанні на вимогу уповноважених осіб- це:
1) цілісність
2) доступність
3) актуальність
4) конфіденційність
5) інша відповідь

Шлях несанкціонованого поширення носія інформації від джерела до зловмисника називається:
1) проксі-сервером
2) хакерським тунелем
3) вразливістю
4) каналом витоку інформації
5) інша відповідь

Якщо загроза спрямована на несанкціоноване добування інформації, то вона є:
1) хакерською
2) навмисною
3) ненавмисною
4) випадковою
5) інша відповідь

Які загрози безпеці інформації з перерахованих є ненавмисними?
1) вибух внаслідок теракту
2) розкрадання носіїв інформації
3) підпал
4) незаконне отримання паролів
5) інша відповідь

Що з наведеного справедливо для інформації:
1) інформація може бути для її користувача достовірною та помилковою, корисною та шкідливою.
2) інформацію не можна продавати як товар
3) корисність інформації є постійною
4) інформація завжди є матеріальною
5) інша відповідь

Зловмисний код має такі відмінні риси: не вимагає програми-носія, викликає поширення своїх копій та їх виконання.
Назвіть тип цього зловмисного коду.
1) вірус
2) спам
3) сніфер
4) хробак
5) інша відповідь

Які загрози безпеці інформації з перерахованих є навмисними?
1) дії випадкових перешкод
2) помилки користувачів
3) збої в роботі апаратури та обладнання
4) ненавмисне ушкодження каналів зв'язку
5) інша відповідь

Які завдання інформаційної безпеки вирішуються на організаційному рівні?
1) сертифікація засобів захисту
2) розробка документації
3) навчання персоналу
4) обмеження доступу на об'єкт
5) інша відповідь

Які методи інженерно-технічного захисту інформації з перерахованих не можуть бути використані для протидії спостереженню?
1) структурне приховування
2) тимчасове приховування
3) просторове приховування
4) енергетичне приховування
5) інша відповідь

Які методи інженерно-технічного захисту інформації з перерахованих використовуються для протидії підслуховуванню?
1) структурне приховування
2) тимчасове приховування
3) просторове приховування
4) підвищення звукопоглинання
5) інша відповідь

Як аутентифікаторв мережному середовищі доцільно використовувати:
1) рік народження суб'єкта
2) прізвище суб'єкта
3) ім’я суб’єкта
4) таємний криптографічний ключ
5) інша відповідь

Середній час напрацювання до відмови:
1) прямо пропорційний інтенсивності відмов
2) обернено пропорційний інтенсивності відмов
3) не залежить від інтенсивності відмов
4) рівнозначний інтенсивності відмов
5) інша відповідь

Найменш витратний криптоаналіз для криптоалгоритму DES – це:
1) перебір по вибірковому ключовому простору
2) розкладання числа на складні множники
3) перебір по всьому ключовому простору
4) розкладання числа на прості множники
5) інша відповідь

Розраховані на багато користувачів системи з інформацією одного рівня конфіденційності відповідно до «Помаранчевої книги» відносяться до класу:
1) C1
2) B2
3) C2
4) B1
5) інша відповідь

Метод управління доступом, у якому кожному об'єкту системи присвоюється мітка критичності, визначальна цінність інформації, називається:
1) виборчим (дискретним)
2) мандатним
3) привілейованим
4) ідентифікованим
5) інша відповідь

Конкретизацією моделі Белла-ЛаПадула є модель політики безпеки:
1) LWM
2) на основі аналізу загроз
3) Лендвера
4) з повним перекриттямзагроз
5) інша відповідь

Ступінь захищеності інформації від негативного впливу на неї з точки зору порушення її фізичної та логічної цілісності чи несанкціонованого використання – це:
1) вразливість інформації
2) надійність інформації
3) захищеність інформації
4) базова небезпека інформації
5) інша відповідь

Відповідність засобів безпеки вирішуваним завданням характеризує:
1) ефективність
2) коректність
3) адекватність
4) уніфікація
5) інша відповідь

00-08-74-4C-7F-1D – приклад:
1) апаратної адреси
2) мережної адреси
3) доменного імені
4) номера маршрутизатора
5) інша відповідь

172.16.0.12 - приклад:
1) апаратної адреси
2) мережної адреси
3) доменного імені
4) номера маршрутизатора
5) інша відповідь

192.168.0.16 - приклад:
1) апаратної адреси
2) мережної адреси
3) доменного імені
4) номера маршрутизатора
5) інша відповідь

FTP підтримує
1) один логічний зв’язок по протоколу прикладного рівня
2) два логічні зв'язки, один з них протокол Telnet
3) два логічні зв'язки, один з них протокол SMTP
4) три логічні зв’язки, один з них протокол XML
5) інша відповідь

---

https://software.com.ua/uk/ – приклад:
1) апаратної адреси
2) мережної адреси
3) доменного імені
4) номера маршрутизатора
5) інша відповідь

---

https://www.google.com – це приклад:
1) апаратної адреси
2) мережної адреси
3) доменного імені
4) номера маршрутизатора
5) інша відповідь

Апаратна адреса – це:
1) MAC
2) IP
3) DNS
4) LTE
5) інша відповідь

Аутентифікація, при якій ім'я користувача і пароль передаються в заголовках http-пакетів – це:
1) Basic
2) Digest
3) Integrated
4) SSL-сертифікат
5) інша відповідь

Аутентифікація, при якій клієнт і сервер обмінюються повідомленнями для з'ясування дійсності один одного за допомогою протоколів Kerberos – це:
1) Basic
2) Digest
3) Integrated
4) SSL-сертифікат
5) інша відповідь

Аутентифікація, при якій пароль користувача передається в хешованому виді – це:
1) Basic
2) Digest
3) Integrated
4) SSL-сертифікат
5) інша відповідь

Базовий протокол керування мережі Internet – це:
1) HTTPS
2) SMTP
3) SNMP
4) XMPP
5) інша відповідь

Що з наведеного **не є** відгуком FTP:
1) позитивний проміжний відгук
2) команда не виконана і не може бути виконана
3) негативний відгук
4) відгук неуспішного завершення процедури
5) інша відповідь

Вкажіть різновиди протоколів, які використовуються при роботі електронної пошти:
1) SMTP, POP-POP3, HTTP
2) SMTP, POP-POP3, IMAP
3) SMTP, POP-POP3, IMAP, MIME
4) STMP, POP-POP3, IIIMAP
5) інша відповідь

Для ідентифікації мережних інтерфейсів **не** використовуються:
1) апаратні адреси
2) мережні адреси
3) доменні імена
4) апаратні та мережні адреси
5) інша відповідь

Доменне ім’я – це:
1) MAC
2) IP
3) DNS
4) LTE
5) інша відповідь

До складу HTTP-запиту, переданого клієнтом серверові, **не**входить наступний компонент:
1) рядок стану
2) поля заголовка
3) порожній рядок
4) тіло запиту
5) інша відповідь

Криптографічний протокол, що забезпечує безпечну передачу даних – це:
1) HTTPS
2) SSL
3) SNMP
4) XMPP
5) інша відповідь

Криптографічні методи захисту інформації відносяться до методів:
1) програмно-апаратних
2) методичних
3) статичних
4) динамічних
5) інша відповідь

Мережна адреса – це:
1) MAC
2) IP
3) LTE
4) PCS
5) інша відповідь

Методи захисту інформації бувають:
1) програмними та апаратними
2) фізичними та апаратними
3) статичними та динамічними
4) програмними та статичними
5) інша відповідь

Методи захисту, що використовують фізичні особливості носіїв інформації, називаються:
1) апаратними
2) програмними
3) фізичними
4) динамічними
5) інша відповідь

Методи маніпуляції з кодом програми відносяться до методів захисту:
1) апаратних
2) програмних
3) статичних
4) динамічних
5) інша відповідь

Методи прив'язки до ідентифікатора можна віднести до методів захисту:
1) фізичних
2) програмних
3) статичних
4) динамічних
5) інша відповідь

Методи, що базуються на роботі зі стеком відносяться до методів захисту:
1) апаратних
2) програмних
3) статичних
4) динамічних
5) інша відповідь

Механізм перевірки приналежності суб'єкту доступу пред'явленого ним ідентифікатора – це:
1) ідентифікація
2) аутентифікація
3) ініціалізація
4) логування
5) інша відповідь

Механізм присвоєння суб'єктам і об'єктам доступу особистого ідентифікатора – це:
1) ідентифікація
2) аутентифікація
3) ініціалізація
4) логування
5) інша відповідь

Оберіть з наведеного базові механізми забезпечення інформаційної безпеки:
1) ідентифікація та аутентифікація
2) аутентифікації та ініціалізація
3) ініціалізація та логування
4) логування та ідентифікація
5) інша відповідь

Позначте обов’язкові команди протоколу SMTP:
1) HELO, MAIL, DATA
2) RSET, MAIL, RCPT
3) HELO, MAIL, RCPT
4) VRFY, HELO, MAIL, DATA
5) інша відповідь

Пристроївизначення індивідуальних характеристик людини з метою її ідентифікації відносяться до методів захисту:
1) програмних
2) методичних
3) статичних
4) динамічних
5) інша відповідь

Пристрої для шифрування інформації відносяться до методів захисту:
1) програмних
2) методичних
3) статичних
4) динамічних
5) інша відповідь

При якій моделі розповсюдження програмного забезпечення відсутня будь-яка оплата або інші умови, що обмежують його використання?
1) Freeware
2) Nagware
3) Trialware
4) Donationware
5) інша відповідь

При якій моделі розповсюдження програмного забезпечення в програмі присутні функціональні обмеження?
1) Demoware
2) Donationware
3) Nagware
4) Trialware
5) інша відповідь

При якій моделі розповсюдження програмного забезпечення користувач для отримання доступу повинен надіслати авторові програми поштову листівку з виглядом місцевості, де він проживає?
1) Freeware
2) Demoware
3) Nagware
4) Trialware
5) інша відповідь

При якій моделі розповсюдження програмного забезпечення користувач для отримання доступу повинен надіслати авторові програми електронний лист?
1) Freeware
2) Demoware
3) Nagware
4) Trialware
5) інша відповідь

При якій моделі розповсюдження програмного забезпеченнякористувачу нагадується про те, що дана версія програми не є повноцінною комерційною версією?
1) Freeware
2) Donationware
3) Nagware
4) Trialware
5) інша відповідь

При якій моделі розповсюдження програмного забезпеченнякористувачу пропонують пожертвувати довільну суму?
1) Freeware
2) Donationware
3) Nagware
4) Trialware
5) інша відповідь

При якій моделі розповсюдження програмного пропонують, якщо сподобалася програма, надіслати авторові якийсь подарунок?
1) Freeware
2) Notware
3) Demoware
4) Trialware
5) інша відповідь

Програма, яка перехоплює дані, що вводяться з клавіатури, називається:
1) сніфер
2) кейлогер
3) сканер
4) інсайдер
5) інша відповідь

Протокол для доступу до служби каталогів X.500– це:
1) LDAP
2) SMTP
3) SNMP
4) XMPP
5) інша відповідь

Протокол, заснований на XML – це:
1) LDAP
2) SMTP
3) SNMP
4) XMPP
5) інша відповідь

Протокол доступу до електронної пошти в Інтернет – це:
1) HTTPS
2) SMTP
3) IMAP
4) POP3
5) інша відповідь

Протокол передачі гіпертексту з шифруванням – це:
1) HTTPS
2) FTP
3) Telnet
4) POP3
5) інша відповідь

Протокол передачі гіпертексту – це:
1) HTTP
2) FTP
3) Telnet
4) POP3
5) інша відповідь

Протокол поштового клієнта – це:
1) HTTPS
2) SSH
3) Telnet
4) POP3
5) інша відповідь

Протокол, призначений для передачі файлів у комп'ютерних мережах – це:
1) HTTPS
2) FTP
3) Telnet
4) POP3
5) інша відповідь

Протокол, призначений для реалізації текстового інтерфейсу по мережі – це:
1) HTTPS
2) FTP
3) Telnet
4) POP3
5) інша відповідь

Протокол прикладного рівня, що дозволяє робити вилучене керування операційною системою і передачу файлів – це:
1) HTTPS
2) SSH
3) Telnet
4) POP3
5) інша відповідь

Протокол, що використовується для відправлення пошти між серверами – це:
1) HTTPS
2) SMTP
3) IMAP
4) POP3
5) інша відповідь

Основні параметри шифру – це:
1) стійкість та довжина ключа
2) довжина ключа та апаратна складність
3) програмна та апаратна складність
4) стійкість, довжина ключа та складність перетворення
5) інша відповідь

Встановлення справжності сторін – це:
1) ідентифікація
2) автентифікація
3) шифрування
4) атака
5) інша відповідь

Криптографічний алгоритм, в якому ключ, який використовується для шифрування повідомлень, може бути отриманий з ключа дешифрування і навпаки, називається:
1) асиметричним
2) синхронним
3) симетричним
4) асинхронним
5) інша відповідь

У більшості симетричних алгоритмів застосовують:
1) 1 ключ
2) 2 ключі
3) 3 ключі
4) 4 ключі
5) інша відповідь

Надійність алгоритму з одним ключем визначається:
1) складністю програмної або апаратної реалізації ключа
2) статистичними властивостями ключа
3) кількістю ключів
4) обчислювальною складністю реалізації ключа
5) інша відповідь

До симетричних схем шифрування відносяться:
1) схема Вернама
2) RSA
3) DSA
4) шифр Ель-Гамаля
5) інша відповідь

Найкращими для використання у симетричних схемах шифрування є випадкові ключі, побудовані на основі:
1) генераторів псевдовипадкових послідовностей
2) генераторів випадкових чисел
3) завадостійких кодів
4) ефективних кодів
5) інша відповідь

У сучасних комп'ютерних алгоритмах блокового шифрування зазвичай довжина блоку становить:
1) 64 біти
2) 128 біт
3) 256 біт
4) 512 біт
5) інша відповідь

Текст, який потрібно зашифрувати, називається:
1) закритим
2) таємним
3) секретним
4) відкритим
5) інша відповідь

Застосування перетворення, в результаті якого утворюється криптограма, називається:
1) шифрування
2) дешифрування
3) кодування
4) декодування
5) інша відповідь

Абсолютно стійкою криптосистемою є:
1) криптосистема RSA
2) криптосистема на еліптичній кривій
3) криптосистема Вернама
4) блокова криптосистема
5) інша відповідь

Сучасна криптографія не вивчає:
1) симетричні криптосистеми
2) криптосистеми з відкритим ключем
3) системи електронного підпису
4) управління ключами
5) інша відповідь

Кінцева множина використовуваних для шифрування інформації знаків – це:
1) латиниця
2) символіка
3) алфавіт
4) ентропія
5) інша відповідь

Пошук та дослідження математичних методів перетворення інформації – це:
1) криптографія
2) криптоаналіз
3) шифрування
4) дешифрування
5) інша відповідь

Дослідження можливості розшифровування інформації без знання ключів – це:
1) криптографія
2) криптоаналіз
3) шифрування
4) дешифрування
5) інша відповідь

Впорядкований набір елементів алфавіту – це:
1) шифр
2) текст
3) стенограма
4) експлікація
5) інша відповідь

Що з наведеного не є прикладом алфавіту, який може використовуватися у сучасних криптосистемах:
1) алфавіт Z256 – символи, що входять до стандартних кодів ASCII та KOI-8
2) бінарний алфавіт - Z2 = {0,1}
3) вісімковий алфавіт - Z8 = {0,1,2,3,4,5,6,7}
4) шістнадцятковий алфавіт - Z16 = {0,1,2,3,4,5,6,7,8,9,10,11, 12,13,14, 15}
5) інша відповідь

Яка інформація, необхідна для шифрування та дешифрування текстів:
1) знак
2) контроль
3) секрет
4) ключ
5) інша відповідь

До класу перетворень відкритого тексту відноситься:
1) ключова шифросистема
2) автономна система електронних платежів
3) криптографічна система
4) асиметрична система
5) інша відповідь

Що з наведеного не є класом криптосистем:
1) криптосистеми обмеженого використання
2) криптосистеми загального використання
3) криптосистеми із секретним ключем
4) криптосистеми з відкритим ключем
5) інша відповідь

Як називаються криптосистеми, якщо їх стійкість ґрунтується на збереженні в секреті самого характеру алгоритмів шифрування та дешифрування?
1) криптосистеми обмеженого використання
2) криптосистеми загального використання
3) криптосистеми із секретним ключем
4) криптосистеми з відкритим ключем
5) інша відповідь

Як називаються криптосистеми, якщо в них будь-які дві сторони, перед тим, як зв'язатися одна з одною, повинні заздалегідь домовитися між собою про використання певної секретної частини інформації?
1) криптосистеми обмеженого використання
2) криптосистеми загального використання
3) криптосистеми із секретним ключем
4) криптосистеми з відкритим ключем
5) інша відповідь

Які з наведених термінів відносяться до процесів обробки інформації, змістом яких є складання та розподіл ключів між користувачами:
1) розподіл паролів
2) управління ключами
3) електронний (цифровий) підпис
4) хеш-функція
5) інша відповідь

Як називається криптографічне перетворення, яке долучається до тексту та дозволяє при отриманні тексту іншим користувачем перевірити авторство і справжність повідомлення:
1) шифросистема з ключем відкритим
2) шифросистема з секретним ключем
3) хеш-функція
4) електронний (цифровий) підпис
5) інша відповідь

У 1 ст. н.е. Ю. Цезар під час війни з галлами, листуючись зі своїми друзями в Римі, замінював у повідомленні:
1) першу літеру латинського алфавіту (A) на четверту (D)
2) другу літеру латинського алфавіту (B) на четверту (D)
3) третю літеру латинського алфавіту (C) на сьому (G)
4) усі літери спеціальними числовими позначеннями
5) інша відповідь

Систему, в якій одному символу відповідають одна або кілька комбінацій двох і більше символів називають:
1) багатоалфавітною системою шифрування
2) багатолітерною системою шифрування
3) багатоцифровою системою шифрування
4) багатознаковою системою шифрування
5) інша відповідь

До класу перестановки належить шифр:
1) рядкова транспозиція
2) шахова транспозиція
3) стовпчикова транспозиція
4) маршрутна транспозиція
5) інша відповідь

У процесі шифрування (і дешифрування) іноді використовується таблиця, яка влаштована наступним чином: у першому рядку виписується весь алфавіт, у кожному наступному здійснюється його циклічне зрушення на одну літеру. Її назва:
1) матриця Комівояжера
2) таблиця Віженера
3) транспортне завдання
4) маршрутна транспозиція
5) інша відповідь

Теорема Евкліда свідчить, що множина P={2,3,5,11,13,…} всіх найпростіших чисел є:
1) дискретною
2) скінченою
3) нескінченою
4) немає такої теореми
5) інша відповідь

Здатність протистояти спробам добре озброєного сучасною технікою та знаннями криптоаналітика дешифрувати перехоплений шифротекст, розкрити ключі шифру або порушити цілісність та справжність інформації – це:
1) сила
2) міцність
3) стійкість
4) постійність
5) інша відповідь

Криптосистема шифрування даних RSA заснована на:
1) проблемі генерації великих простих чисел
2) проблемі розкладання великих чисел для генерації відкритого та закритого ключа
3) проблемі вирішення завдання дискретного логарифмування
4) проблемі пошуку примітивного елемента в циклічній групі
5) інша відповідь

При алгоритмі шифрування Ель-Гамалякриптостійкість ґрунтується на:
1) проблемі генерації великих простих чисел
2) проблемі розкладання великих чисел для генерації відкритого та закритого ключа
3) проблемі вирішення завдання дискретного логарифмування
4) проблемі пошуку примітивного елемента в циклічній групі
5) інша відповідь

Мультиплікативна арифметична функція, що дорівнює кількості натуральних чисел, менших n і взаємно простих з ним – це:
1) функція ентропії
2) функція Ейлера
3) функція Ейзенштейна
4) функція Ейрі
5) інша відповідь

Безліч оборотних перетворень тексту, які виконуються з метою його захисту називають:
1) шрифт
2) код
3) шифр
4) символ
5) інша відповідь

Якщо текст M і шифротекст C статистично незалежні, тобто отримання шифротексту не дає криптоаналітику додаткової інформації про надісланий відкритий текст, то це називається:
1) абсолютна секретність
2) доказова секретність
3) доказова стійкість
4) абсолютна стійкість
5) інша відповідь

Які системи характеризуються тим, що у них ключовий потік k1, k2 ,... виходить незалежно від відкритого і шифрованого текстів:
1) самосинхронізовані потокові криптосистеми
2) детерміновані потокові криптосистеми
3) асиметричні потокові криптосистеми
4) синхронні потокові криптосистеми
5) інша відповідь

Які системи характеризуються тим, що у них кожен знак ключового потоку (гами) будь-якої миті часу визначається фіксованим числом попередніх знаків шифротекста:
1) самосинхронізовані потокові криптосистеми
2) детерміновані потокові криптосистеми
3) асиметричні потокові криптосистеми
4) синхронні потокові криптосистеми
5) інша відповідь

Алгоритм, який виробляє ключовий потік (гаму) може бути:
1) детермінованим
2) псевдовипадковим
3) незалежним
4) нерегулярним
5) інша відповідь

Звичайні криптосистеми із секретним ключем називають:
1) одноключовими криптосистемами
2) симетричними криптосистемами
3) асиметричними криптосистемами
4) двоключовими криптосистемами
5) інша відповідь

Що з наведеного не відноситься до схем атаки на шифр або методів дешифрування:
1) схема атаки на шифр (методи розшифрування) на основі знання лише шифротексту
2) схема атаки на шифр (методи дешифрування) при відомих відкритому M та шифрованому C текстах.
3) схема атаки на шифр (методи дешифрування) по відкритому тексту, що вибирається, і відповідному йому шифрованому тексту, тобто, атака на основі тестування
4) схема атаки на шифр (методи дешифрування для криптосистем з відкритим ключем) по вибраним шифротекстам і відповідним відкритим текстам
5) інша відповідь

Якщо криптоаналітик не може уточнювати розподіл ймовірностей можливих відкритих текстів за наявним шифротекстом, навіть якщо він має всі необхідні для цього засоби, то криптосистема називається:
1) теоретично стійкою
2) практично стійкою
3) середньо стійкою
4) непохитною
5) інша відповідь

Логіко-математичні поняття у криптології, що виражають уподібнення будови систем:
1) гомоморфізм
2) ізоморфізм
3) поліморфізм
4) антропоморфізм
5) інша відповідь

Логіко-математичні поняття у криптології, що виражають однакову будову систем:
1) гомоморфізм
2) ізоморфізм
3) поліморфізм
4) антропоморфізм
5) інша відповідь

Поле, що складається з кінцевого числа елементів, називається:
1) дискретне поле
2) нескінчене поле
3) криптографічне поле
4) поле Галуа
5) інша відповідь

Функція, яка стискає рядок чисел довільного розміру в рядок чисел фіксованого розміру:
1) криптографічна функція
2) хеш-функція
3) хаш-функція
4) зіп-функція
5) інша відповідь

Що з наведеного не відноситься до шифрів заміни:
1) шифр простої заміни
2) шифр Цезаря
3) моноалфавітний шифр
4) шифр підстановки
5) інша відповідь

Потенційна небезпека порушення однієї або декількох властивостей криптографічної системи (криптографічного протоколу) – це:
1) атака
2) вторгнення
3) загроза
4) несанкціонований доступ
5) інша відповідь

Функція, яка описує процес шифрування та здійснює залежне від ключа відображення послідовностей шифрованих блоків тексту – це:
1) блокова функція
2) функція шифрування
3) криптографічна функція
4) одностороння функція
5) інша відповідь

Функція, що використовується для збільшення аналітичної складності проміжних послідовностей, наприклад, у фільтруючих та комбінуючих генераторах шифросистем – це:
1) блокова функція
2) функція шифрування
3) криптографічна функція
4) одностороння функція
5) інша відповідь

Дискретна функція, для якої існують певні обмеження або заборони – це:
1) блокова функція
2) функція шифрування
3) криптографічна функція
4) одностороння функція
5) інша відповідь

Функція – сервіс безпеки, що забезпечує можливість перевірки того, що отримані дані справді створені конкретним джерелом – це:
1) блокова функція
2) функція шифрування
3) криптографічна функція
4) одностороння функція
5) інша відповідь

Функція – сервіс безпеки, що забезпечує можливість перевірки того, що всі дані, які передаються при встановленому з'єднанні, не зазнали модифікації – це:
1) блокова функція
2) функція шифрування
3) криптографічна функція
4) одностороння функція
5) інша відповідь

Функція, що відображає вхідне слово кінцевої довжини в кінцевому алфавіті – це:
1) блокова функція
2) функція шифрування
3) криптографічна функція
4) одностороння функція
5) інша відповідь

Хеш-функція, для якої завдання пошуку прообразів заданих значень є обчислювально важким – це:
1) хеш-функція одностороння
2) хеш-функція двостороння
3) хеш-функція багатостороння
4) хеш-функціяобчислювально складна
5) інша відповідь

Відсутність змін у інформації, що передається або зберігається в порівнянні з її вихідним записом, називається:
1) єдність
2) синтез
3) повнота
4) цілісність
5) інша відповідь

Особливий учасник криптографічного протоколу, якому довіряють решта його учасників, введений у протокол для посилення його безпеки – це:
1) центр довіри
2) центр реєстрації
3) центр сертифікації
4) центр захисту
5) інша відповідь

У потокових шифросистемах вироблення ключової послідовності називається:
1) вироблення ключа
2) розгортання ключа
3) розголошення ключа
4) у потокових шифросистемах ключі не виробляються
5) інша відповідь

Шифр, у якому шифрований текст (повідомлення) отримується шляхом перестановки блоків відкритого тексту (повідомлення) називається:
1) шифр підстановки
2) шифр перестановки
3) шифр гамування
4) шифр досконалий
5) інша відповідь

Теоретико-інформаційна характеристика розподілу випадкової величини – це:
1) функція Ейлера
2) ендотропія
3) азотропія
4) ізотропія
5) інша відповідь

Як у криптографічних протоколах з двома учасниками **не**називається часовий інтервал, у якому активний лише один із учасників:
1) цикл
2) раунд
3) прохід
4) перехід
5) інша відповідь

Послідовність стадій, що проходять ключі від моменту генерації до моменту знищення, називається:
1) цикл (раунд) шифрування
2) центр установки міток
3) життєвий цикл ключів
4) алгоритм шифрування
5) інша відповідь

Послідовність символів, яка служить для отримання доступу до криптографічних засобів, обчислювальних засобів і ін., називається:
1) перепустка
2) код
3) шифр
4) пароль
5) інша відповідь

Атака на криптосистему, що перехоплює повідомлення та заміняє його іншим повідомленням – це:
1) фальсифікація
2) підстановка
3) переміщення
4) підміна
5) інша відповідь

Послідовність, породжена недетермінованим фізичним пристроєм чи процесом– це:
1) послідовність псевдовипадкова
2) послідовність істинно випадкова
3) послідовність ключова
4) послідовність лінійна конгруентна
5) інша відповідь

Послідовність, у якій кожен елемент однозначно визначається деяким фіксованим числом попередніх елементів з допомогою функції, іменованої законом рекурсії – це:
1) послідовність псевдовипадкова
2) послідовність істинно випадкова
3) послідовність ключова
4) послідовність лінійна конгруентна
5) інша відповідь

Зберігання копії ключа криптосистеми у довіреної особи (організації, учасника протоколу) з метою відновлення працездатності криптосистеми, наприклад, у разі втрати ключа називається:
1) розгортання ключів
2) розподіл ключів
3) депонування ключів
4) копіювання ключів
5) інша відповідь

Структура множини ключів криптосистеми, що відображає різні функції, які виконуються окремими частинами складного ключа називається:
1) граф ключів
2) ідентифікація ключів
3) угруповання ключів
4) ієрархія ключів
5) інша відповідь

Атака на криптографічний протокол, метою якої є нав'язування однієї зі сторін повідомлення від імені іншої сторони, яке не буде відкинуто при прийомі – це:
1) імітація
2) інсценування
3) дублювання
4) загроза
5) інша відповідь

Один із методів генерації псевдовипадкових чисел, який застосовується в простих випадках і не має криптографічної стійкості називається:
1) лінійний конгруентний метод
2) нелінійний конгруентний метод
3) паралельний конгруентний метод
4) лінійний рекурентний метод
5) інша відповідь

Послідовність чисел, яка була обчислена за деяким арифметичним правилом, але має всі властивості випадкової послідовності чисел у рамках розв'язуваного завдання – це:
1) доказово випадкова послідовність
2) псевдовипадкова послідовність
3) випадкова послідовність
4) цілеспрямована послідовність
5) інша відповідь

Послідовність, якщо її не можна відтворити, називається:
1) доказово випадкова послідовність
2) псевдовипадкова послідовність
3) випадкова послідовність
4) цілеспрямована послідовність
5) інша відповідь

Якщо послідовність непередбачувана, тобто неможливо обчислити наступний біт, маючи повне знання алгоритму (або апаратури) і всіх попередніх бітів потоку, то вона є:
1) доказово випадкова послідовність
2) псевдовипадкова послідовність
3) випадкова послідовність
4) цілеспрямована послідовність
5) інша відповідь

Якщо генератор послідовності виглядає випадковим, тобто проходить усі статистичні тести випадковості, то він називається:
1) псевдовипадковий
2) випадковий
3) надійний
4) доказовий
5) інша відповідь

Якщо генератор послідовності не може бути достовірно відтворений, то він називається:
1) псевдовипадковий
2) випадковий
3) надійний
4) доказовий
5) інша відповідь

Що з наведеного не входить до структури генератора ключової послідовності:
1) блок пам'яті, що зберігає інформацію про стан генератора
2) вихідна функція, що генерує біт ключової послідовності залежно від стану
3) функція переходів, що задає новий стан, у який перейде генератор на наступному кроці
4) функція висновку, що завершує роботу генератору
5) інша відповідь

Міжмережний екран – це:
1) пристрій управління доступом, що захищає внутрішні мережі від зовнішніх атак
2) пристрій комутаціїтрафіку
3) пристрій кешування мережного трафіку
4) пристрій, що забезпечує захист від зловмисника, який використовує для входу до системи легальну програму
5) інша відповідь

Загрози конфіденційності інформації у інформаційно-комунікаційних системах- це:
1) «маскарад», перехоплення даних, зловживання повноваженнями
2) «карнавал», переадресування, перехоплення даних
3) переадресування, блокування, зловживання повноваженнями
4) блокування, видалення, зловживання повноваженнями
5) інша відповідь

Виберіть більш правильне поняття моделі взаємодії відкритих систем OSI:
1) визначає чотири транспортних рівні взаємодії комп'ютерів - фізичний, канальний, мережний, транспортний
2) визначає правила взаємодії систем з комутацією пакетів
3) модель, що визначає рівні взаємодії систем для стека IPX/SPX
4) модель, що визначає сім рівнів взаємодії систем
5) інша відповідь

Визначте найбільш правильне поняття інтерфейсу для багаторівневого підходу у інформаційно-комунікаційних системах:
1) це стандартні формати повідомлень, необхідні для взаємодії модулів на різних рівнях
2) взаємодія модулів сусідніх вузлів відповідно до певних правил
3) набір програмних модулів, що реалізують процедуру обміну між сусідніми рівнями на різних вузлах
4) взаємодія модулів один з одним, що перебувають на одному вузлі, відповідно до чітких правил і за допомогою стандартизованих форматів повідомлень
5) інша відповідь

Визначте поняття мережного протоколу:
1) IP протокол
2) протоколи, які збирають інформацію про топологію міжмережних з'єднань
3) це протоколи, які реалізують просування пакетів через мережу
4) протоколи, які забезпечують просування через концентратори
5) інша відповідь

З яких частин складається повідомлення, формоване конкретним рівнем моделі OSI
1) преамбули, заголовку, адреси джерела та призначення
2) заголовку, поля даних і контрольної суми
3) заголовку поля даних
4) заголовку та поля даних
5) інша відповідь

Куди відправляються пакети, якщо адреса призначення не відповідає адресі мережі відправника:
1) до DNS сервера
2) до найближчого маршрутизатора
3) до шлюзу за замовчуванням
4) до найближчого комутатора
5) інша відповідь

На які два рівні розділений канальний рівень у відповідності зі стандартами IEEE 802?
1) рівень доступу до середовища та рівень фізичних адрес
2) мережний і транспортний
3) аналоговий і цифровий рівні
4) керування логічним каналом (LLC) і керування доступом до середовища (MAC)
5) інша відповідь

Виберіть правильне поняття моделі TCP/IP:
1) визначає чотири рівні взаємодії систем:прикладний, транспортний, мережний, канальний
2) визначає правила взаємодії систем з комутацією пакетів
3) модель, що визначає рівні взаємодії систем для стека IPX/SPX
4) модель, що визначає сім рівнів взаємодії систем
5) інша відповідь

Призначення MAC рівня:
1) реалізує функції інтерфейсу із прилягаючим до нього мережним рівнем
2) забезпечує коректне спільне використання загального середовища передачі даних, надаючи її в розпорядження того або іншого вузла відповідно до певного алгоритму
3) необхідний для надання кожному комп'ютеру MAC адреси
4) реалізує алгоритм доступу до середовища Fast Ethernet, PPP
5) інша відповідь

Мережні технології - це:
1) модель OSI
2) служба електронної пошти та гіпертекстова інформаційна служба WorldWideWeb
3) синхронна мережна ієрархія - SDH
4) Ethernet, FDDI, TokenRing
5) інша відповідь

У яких мережах використовується метод доступу до середовища передачі даних CSMA/CD?
1) FDDI
2) TokenRing
3) Ethernet
4) ArcNet
5) інша відповідь

Що таке декомпозиція завдань мережної взаємодії?
1) це визначення порядку взаємодії модулів системи
2) це набір функцій, які підпорядковані вищому рівню
3) це багаторівневий підхід для рішення завдань мережної взаємодії
4) це розбивка одного складного завдання на простіші завдання-модулі
5) інша відповідь

Що таке логічна структуризація мережі?
1) використання багатопортового комутатора для розбиття мережі
2) поділ мережі на кілька частин за допомогою комутаторів
3) розбиття мережного середовища на кілька частин за допомогою комутаторів, маршрутизаторів
4) поділ мережі на кілька частин за допомогою маршрутизаторів
5) інша відповідь

Що таке протокол у інформаційно-комунікаційних системах?
1) апаратний модуль, що реалізує процедуру обміну інформацією в мережі
2) правила, що визначають послідовність і формат повідомлень, якими обмінюються комп'ютерні компоненти
3) формальнапроцедура обміну інформацією в мережі
4) правила, що визначають взаємодію пари відповідних рівнів
5) інша відповідь

Що таке стек комунікаційних протоколів?
1) ієрархічно організований набір протоколів, достатній для організації взаємодії вузлів у мережі
2) це програмні модулі, встановлені на одному комп'ютері, що працює в мережі Ethernet
3) набір програмних модулів, що реалізують протоколи конкретної фірми виробника
4) набір технічних і програмних засобів, що реалізують взаємодію комп'ютерів у мережі
5) інша відповідь

Що являє собою процедура без установлення з'єднань і без підтвердження одержання даних?
1) режим роботи, використовуваний для передачі даних з використанням електронної пошти
2) дейтаграмний режим роботи, що дає користувачеві засоби для передачі даних з мінімумом витрат
3) режим роботи, використовуваний у глобальних мережах для забезпечення надійної передачі кадрів на зашумленних лініях
4) режим роботи, реалізований протоколом NetBIOS/NetBEUI
5) інша відповідь

Якими питаннями займається підкомітет IEEE 802.15?
1) Ethernet з методом доступу CSMA/CD
2) керуванням логічною передачею даних
3) бездротовими мережами
4) волоконно-оптичними мережами
5) інша відповідь

Які з перерахованих протоколів можна віднести до мережного рівня моделі OSI?
1) ARP
2) SMB
3) Ethernet
4) FDDI
5) інша відповідь

Які мережні пристрої будують таблицю маршрутизації?
1) Bridge
2) DWL-2100AP
3) Switch
4) Bluetooth
5) інша відповідь

Які стандарти розробляються підкомітетом IEEE 802.15?
1) способи пріоритезаціїтрафіку на канальному рівні
2) локальні радіомережі з методами доступу, аналогічними мережам Ethernet
3) загальні визначення локальних мереж і їхніх властивостей, визначений зв'язок моделі IEEE 802 з моделлю ISO
4) мережна безпека
5) інша відповідь

Які три рівні моделі OSI є мережнозалежними?
1) прикладний, транспортний, фізичний
2) фізичний, канальний, мережний
3) транспортний, представлення, сеансовий
4) канальний, мережний, прикладний
5) інша відповідь

Яку маску мережі необхідно використати, щоб побудувати мережу з 14-ма вузлами?
1) 255.255.255.224
2) 255.255. 255.240
3) 255.255.255.128
4) 255.255.0.0
5) інша відповідь

Засоби захисту об'єктів файлової системи засновані на:
1) визначення прав користувача на операції з файлами та каталогами
2) задаванні атрибутів файлів і каталогів, незалежних від прав користувачів
3) використанні антивірусних програмних засобів
4) використанні біометричної аутентифікації
5) інша відповідь

Який виду модуляції сигналів базується на теорії відображення Найквіста-Котельникова:
1) кодово-імпульсна модуляція (КІМ)
2) фазова модуляція (ФМ)
3) частотна модуляція (ЧМ)
4) амплітудна модуляція (АМ)
5) інша відповідь

Рандомізація коду використовується для:
1) порушення статистичної залежності появи символів алфавіту в текстах
2) перемішування кодів символів алфавіту
3) випадкового (псевдовипадкового) вибору коду символів з тексту
4) захисту кодованих повідомлень від завад
5) інша відповідь

Яку розрядність має двійковий код ASCII в початковій версії (версія без символів кирилиці):
1) 4
2) 7
3) 8
4) 16
5) інша відповідь

Яку розрядність має двійковий код ASCII в розширеній версії Win-1251 (з символами кирилиці):
1) 4
2) 7
3) 8
4) 16
5) інша відповідь

Яку розрядність має двійковий код символу в стандарті кодування Unicode:
1) 4
2) 7
3) 8
4) 16
5) інша відповідь

Який з перелічених стандартів кодування має найбільшу кількість кодів символів:
1) ASCII
2) ASCII Win-1251
3) UNICODE
4) КОИ-8
5) EBCDIC

Теорема відліків також відома як:
1) теорема Котельникова
2) основна теорема анализу
3) теорема Найквіста
4) теорема Шеннона
5) інша відповідь

Яку базову відстань відліків визначає теорема Котельникова:
1) 2 F
2) F
3) 0,5 F
4) 0,25 F
5) інша відповідь

Представлення безперервних електричних сигналів послідовностю їхніх дискретних значень це:
1) квантування сигналів
2) модулювання сигналів
3) диференціювання сигналів
4) кодування сигналів
5) інша відповідь

Теорема про максимальну швидкість передачі в малозашумленому каналі з обмеженою смугою пропускання також відома як:
1) теорема Котельникова
2) основна теорема анализу
3) теорема Найквіста
4) теорема Шеннона
5) інша відповідь

Перетворення Фур'є застосовується:
1) виключно до аналогових сигналів
2) виключно до дискретних сигналів
3) до аналогових і дискретних сигналів
4) для оптимального кодування
5) для завадосійкого кодування

Перетворення Фур'є, виконане над періодичною функцією, дає функцію:
1) дискретну
2) модульовану
3) періодичну
4) невизначену
5) секретну

Перетворення Фур'є, виконане над дискретною функцією, дає функцію:
1) дискретну
2) модульовану
3) періодичну
4) невизначену
5) секретну

Швидке перетворення Фур'є має альтернативну назву:
1) проріджування за часом
2) проріджування за рівнем
3) проріджування за часом і рівнем
4) проріджування за списком
5) псевдовипадкове проріджування

Основоположною для задач оптимального кодування є:
1) теорема Котельникова
2) основна теорема анализу
3) теорема Найквіста
4) перша теорема Шеннона
5) друга теорема Шеннона

Основоположною для задач завадостійкого кодування є:
1) теорема Котельникова
2) основна теорема анализу
3) теорема Найквіста
4) перша теорема Шеннона
5) інша відповідь

Перша теорема Шеннона (для каналу без завад) передбачає кодування при якому надлишковість коду повідомлень:
1) зменшується
2) не змінюється
3) збільшується
4) зменшується або збільшується залежно від умов
5) інша відповідь

Перша теорема Шеннона (для каналу без завад) передбачає кодування при якому надлишковість коду повідомлень:
1) зменшується
2) не змінюється
3) збільшується
4) зменшується або збільшується залежно від умов
5) інша відповідь

Що є метою криптоаналізу?
1) визначення стійкості алгоритму
2) збільшення кількості функцій заміщення у криптографічному алгоритмі
3) зменшення кількості функцій підстановок у криптографічному алгоритмі
4) визначення використаних перестановок
5) інша відповідь

Частота застосування брутфорс-атак зросла, оскільки:
1) збільшилася кількість перестановок і заміщень, що використовується в алгоритмах
2) алгоритми в міру підвищення стійкості ставали менш складними і більш схильними до атак
3) потужність та швидкість роботи процесорів зросла
4) довжина ключа з часом зменшилась
5) інша відповідь

Що з наведеного нижче не є властивістю або характеристикою односторонньої функції хешування?
1) вона перетворює повідомлення довільної довжини значення фіксованої довжини
2) маючи значення дайджесту повідомлення, неможливо отримати саме повідомлення
3) отримання однакового дайджесту з двох різних повідомлень неможливе, або трапляється вкрай рідко
4) вона перетворює повідомлення фіксованої довжини на значення змінної довжини
5) інша відповідь

Що може вказувати на зміну повідомлення?
1) змінився відкритий ключ
2) змінився закритий ключ
3) змінився дайджест повідомлення
4) повідомлення було правильно зашифровано
5) інша відповідь

Який із наведених нижче алгоритмів є алгоритмом американського уряду, призначеним для створення безпечних дайджестів повідомлень?
1) DataEncryptionAlgorithm
2) DigitalSignature Standard
3) SecureHashAlgorithm
4) DataSignatureAlgorithm
5) інша відповідь

Що з наведеного нижче найкраще описує відмінності між HMAC і CBC-MAC?
1) HMAC створює дайджест повідомлення та застосовується для контролю цілісності; CBC-MAC використовується для шифрування блоків даних з метою забезпечення конфіденційності
2) HMAC використовує симетричний ключ та алгоритм хешування; CBC-MAC використовує перший блок як контрольну суму
3) HMAC забезпечує контроль цілісності та автентифікацію джерела даних; CBC-MAC використовує блоковий шифр у процесі створення MAC
4) HMAC зашифровує повідомлення на симетричному ключі, а потім передає результат алгоритму хешування; CBC-MAC зашифровує все повідомлення повністю
5) інша відповідь

У чому перевага RSA над DSA?
1) він може забезпечити функціональність цифрового підпису та шифрування
2) він використовує менше ресурсів і виконує шифрування швидше, оскільки використовує симетричні ключі
3) це блоковий шифр і він кращий за поточний
4) він використовує одноразові шифрувальні блокноти
5) інша відповідь

Багато країн обмежують використання та експорт криптографічних систем. Для чого вони це роблять?
1) без обмежень може виникнути велика кількість проблем сумісності при спробі використовувати різні алгоритми у різних програмах
2) ці системи можуть використовуватися деякими країнами проти їх місцевого населення
3) кримінальні елементи можуть використовувати шифрування, щоб уникнути виявлення та переслідування
4) законодавство сильно відстає, а створення нових типів шифрування ще більше посилює цю проблему
5) інша відповідь

Що використовується для створення цифрового підпису?
1) закритий ключ одержувача
2) відкритий ключ відправника
3) закритий ключ відправника
4) відкритий ключ одержувача
5) інша відповідь

Що з наведеного нижче найкраще описує цифровий підпис?
1) це метод перенесення власноручного підпису на електронний документ
2) це метод шифрування конфіденційної інформації
3) це метод, що забезпечує електронний підпис та шифрування
4) це метод, що дозволяє одержувачу повідомлення перевірити його джерело та переконатися у цілісності повідомлення
5) інша відповідь

Якою є ефективна довжина ключа в DES?
1) 56
2) 64
3) 32
4) 16
5) інша відповідь

Чому засвідчуючий центр відкликає сертифікат?
1) якщо відкритий ключ користувача скомпрометовано
2) якщо користувач переходить на використання моделі PEM, яка використовує мережу довіри
3) якщо закритий ключ користувача скомпрометовано
4) якщо користувач переходить до іншого офісу
5) інша відповідь

Що з перерахованого нижче найкраще описує центр, що засвідчує сертифікат?
1) організація, яка випускає закриті ключі та відповідні алгоритми
2) організація, яка перевіряє процеси шифрування
3) організація, яка перевіряє ключі шифрування
4) організація, що випускає сертифікати
5) інша відповідь

Як розшифровується абревіатура DEA?
1) DataEncodingAlgorithm
2) DataEncodingApplication
3) DataEncryptionAlgorithm
4) DigitalEncryptionAlgorithm
5) інша відповідь

Хто брав участь у розробці першого алгоритму із відкритими ключами?
1) Аді Шамір
2) Росс Андерсон
3) Брюс Шнайєр
4) Мартін Хеллман
5) інша відповідь

Який процес зазвичай виконується після створення сеансового ключа DES?
1) підписання ключа
2) передача ключа на зберігання третій стороні (keyescrow)
3) кластеризація ключа
4) обмін ключем
5) інша відповідь

Скільки циклів перестановки та заміщення виконує DES?
1) 16
2) 32
3) 64
4) 56
5) інша відповідь

Що з наведеного нижче є правильним твердженням щодо шифрування даних, яке виконується з метою їх захисту?
1) воно забезпечує перевірку цілісності та правильності даних
2) воно вимагає уважного ставлення до процесу керування ключами
3) воно не вимагає великої кількості системних ресурсів
4) воно вимагає передачі ключа на зберігання третій стороні (escrowed)
5) інша відповідь

Як називається ситуація, в якій при використанні різних ключів для шифрування одного і того ж повідомлення в результаті виходить той самий шифротекст?
1) колізія
2) хешування
3) MAC
4) кластеризація ключів
5) інша відповідь

Що з наведеного нижче є визначенням фактора трудовитрат для алгоритму у криптології?
1) час зашифрування та розшифрування відкритого тексту
2) час, який займе злом шифрування
3) час, який займає виконання 16 циклів перетворень
4) час, який займає виконання функцій підстановки
5) інша відповідь

Що є основною метою використання одностороннього хешування пароля користувача?
1) це знижує потрібний об'єм дискового простору для зберігання пароля користувача
2) це запобігає ознайомленню будь-кого з відкритим текстом пароля
3) це дозволяє уникнути надлишкової обробки, необхідної асиметричним алгоритмом
4) це запобігає атакам повтору (replayattack)
5) інша відповідь

Який із наведених нижче алгоритмів заснований на складності розкладання великих чисел на два вихідних простих помножувачі?
1) ECC
2) RSA
3) DES
4) Діффі-Хеллман
5) інша відповідь

Що з наведеного нижче описує різницю між алгоритмами DES і RSA?
1) DES – це симетричний алгоритм, а RSA – асиметричний
2) DES – це асиметричний алгоритм, а RSA – симетричний
3) вони обидва є алгоритмами хешування, але RSA генерує 160-бітові значення хеш
4) DES генерує відкритий та закритий ключі, а RSA виконує шифрування повідомлень
5) інша відповідь

Який з наведених нижче алгоритмів використовує симетричний ключ і алгоритм хешування?
1) HMAC
2) 3DES
3) ISAKMP-OAKLEY
4) RSA
5) інша відповідь

Генерація ключів, для якої використовуються випадкові значення, називається Функцією генерації ключів (KDF). Які значення зазвичай при цьому не використовуються?
1) хеші
2) асиметричні значення
3) «сіль»
4) паролі
5) інша відповідь

C4-85-08-E1-67-ED – приклад:
1) апаратної адреси
2) мережної адреси
3) доменного імені
4) мережного протоколу
5) інша відповідь

Слово september, зашифроване шифром Цезаря зі зсувом на 4, буде виглядати як:
1) vhswhpehu
2) witxiqfiv
3) lcuhphpeh
4) vhswhpehe
5) інша відповідь

Спеціальні регістри для зберігання паролів, ідентифікаційних кодів відносяться до методів захисту:
1) апаратних
2) програмних
3) статичних
4) динамічних
5) інша відповідь

Що з перерахованого **не** відноситься до мети використання проксі-серверів:
1) забезпечення доступу з комп'ютерів локальної мережі в інтернеті
2) оптимізація трафіку в мережі Інтернет
3) обмеження доступу з локальної мережі до зовнішньої
4) пересилання електронних листів
5) інша відповідь

Якої аутентифікації не існує:
1) однофакторної
2) двофакторної
3) багатофакторної
4) однобічної
5) інша відповідь

Аутентифікатор користувача, за умови, що його логін для входу в систему - ivanenko, а пароль – 65u65u65, це:
1) ivanenko
2) 65u65u65
3) логарифмічне перетворення від 65u65u65
4) хеш-функція від ivanenko
5) інша відповідь

Ідентифікатор користувача, за умови, що його логін для входу в систему - ivanenko, а пароль – 65u65u65, це:
1) ivanenko
2) 65u65u65
3) логарифмічне перетворення від 65u65u65
4) хеш-функція від ivanenko
5) інша відповідь

Якщо різним групам користувачів із різним рівнем доступу потрібен доступ до однієї й тієї ж інформації, яку з наведених нижче дій слід виконатифахівцю з інформаційної безпеки?
1) зменшити рівень безпеки цієї інформації для забезпечення її доступності та зручності використання
2) вимагати підписання спеціального дозволу щоразу, коли людині потрібен доступ до цієї інформації
3) посилити контроль за безпекою цієї інформації
4) зменшити рівень класифікації цієї інформації
5) інша відповідь

Яка категорія є найбільш ризикованою для компанії з погляду можливого шахрайства та порушення безпеки?
1) співробітники
2) хакери
3) атакуючі
4) контрагенти (особи, що працюють за договором)
5) інша відповідь

Який фактор є найбільш важливим для того, щоб бути впевненим в успішному забезпеченні інформаційної безпеки в компанії?
1) підтримка вищого керівництва
2) ефективні захисні заходи та методи їх впровадження
3) актуальні та адекватні політики та процедури безпеки
4) проведення тренінгів з безпеки для всіх працівників
5) інша відповідь

Коли доцільно не робити жодних дій щодо виявлених ризиків?
1) ніколи, для забезпечення хорошої безпеки потрібно враховувати та знижувати всі ризики
2) коли ризики не можуть бути прийняті до уваги з політичних міркувань
3) коли необхідні захисні заходи надто складні
4) коли вартість контрзаходів перевищує цінність активу та потенційні втрати
5) інша відповідь

Яка з наведених технік є найважливішою під час виборів конкретних захисних заходів?
1) аналіз ризиків
2) аналіз витрат/вигоди
3) результати ALE
4) виявлення вразливостей та загроз, що є причиною ризику
5) інша відповідь

Що найкраще визначає мета розрахунку ALE?
1) кількісно оцінити рівень безпеки середовища
2) оцінити можливі втрати для кожного контрзаходу
3) кількісно оцінити витрати/вигоди
4) оцінити потенційні втрати від загрози на рік
5) інша відповідь

Що є визначенням впливу на безпеку?
1) щось, що призводить до шкоди від загрози
2) будь-яка потенційна небезпека для інформації чи систем
3) будь-який недолік чи відсутність інформаційної безпеки
4) потенційні втрати від загрози
5) інша відповідь

Ефективна програма безпеки вимагає збалансованого застосування:
1) технічні та нетехнічні методи
2) контрзаходів та захисних механізмів
3) фізичної безпеки та технічних засобів захисту
4) процедур безпеки та шифрування
5) інша відповідь

Функціональність безпеки визначає очікувану роботу механізмів безпеки, а гарантії визначають:
1) впровадження управління механізмами безпеки
2) класифікацію даних після впровадження механізмів безпеки
3) рівень довіри, що забезпечується механізмом безпеки
4) співвідношення витрат/вигід
5) інша відповідь

Яке твердження є правильним, якщо поглянути на різницю з метою безпеки для комерційної та військової організації?
1) тільки військові мають справжню безпеку
2) комерційна компанія зазвичай більше піклується про цілісність та доступність даних, а військові – про конфіденційність
3) військовим потрібен більший безпековий рівень, т.к. їх ризики істотно вищі
4) комерційна компанія зазвичай більше піклується про доступність та конфіденційність даних, а військові – про цілісність
5) інша відповідь

Що з наведеного не є метою проведення аналізу ризиків?
1) делегування повноважень
2) кількісна оцінка впливу потенційних загроз
3) виявлення ризиків
4) визначення
5) інша відповідь

Чому під час проведення аналізу інформаційних ризиків слід залучати до цього фахівців із різних підрозділів компанії?
1) щоб переконатися, що проводиться справедлива оцінка
2) не потрібно, для аналізу ризиків слід залучати невелику групу фахівців, які є співробітниками компанії, що дозволить забезпечити неупереджений і якісний аналіз
3) оскільки люди у різних підрозділах краще розуміють ризики у своїх підрозділах та зможуть надати максимально повну та достовірну інформацію для аналізу
4) оскільки люди в різних підрозділах самі є однією з причин ризиків, вони повинні відповідати за їх оцінку
5) інша відповідь

Що є найкращим описом кількісного аналізу ризиків?
1) аналіз, заснований на сценаріях, призначений виявлення різних загроз безпеки
2) метод, що використовується для точної оцінки потенційних втрат, ймовірності втрат та ризиків
3) метод, який зіставляє грошове значення з кожним компонентом оцінки ризиків
4) метод, заснований на судженнях та інтуїції
5) інша відповідь

Чому кількісний аналіз ризиків у чистому вигляді недосяжний?
1) він досягнутий і використовується
2) він надає рівні критичності, їх складно перевести у грошовий вигляд.
3) це пов'язано з точністю кількісних елементів
4) кількісні виміри повинні застосовуватися до якісних елементів
5) інша відповідь

До правових методів, що забезпечують інформаційну безпеку, належить:
1) розробка апаратних засобів забезпечення правових даних
2) розробка програмних засобів забезпечення правових даних
3) розробка та встановлення у всіх комп'ютерних правових мережах журналів обліку дій
4) розробка та конкретизація правових нормативних актів забезпечення безпеки
5) інша відповідь

Основними джерелами загроз інформаційній безпеці є:
1) викрадення жорстких дисків, підключення до мережі, інсайдерство
2) перехоплення даних, розкрадання даних, зміна архітектури системи
3) розкрадання даних, підкуп системних адміністраторів
4) порушення регламенту роботи
5) інша відповідь

Види інформаційної безпеки - це:
1) персональна, корпоративна, державна
2) клієнтська, серверна, мережна
3) локальна, глобальна, змішана
4) клієнт-серверна, комерційна
5) інша відповідь

Головна мета інформаційної безпеки – це своєчасне виявлення, попередження:
1) несанкціонованого доступу, дій в мережі
2) інсайдерства в організації
3) надзвичайних ситуацій
4) викрадення паролів користувачів
5) інша відповідь

Основними ризиками інформаційної безпеки є:
1) спотворення, зменшення обсягу інформації
2) перекодування інформації
3) технічне втручання, виведення з ладу обладнання мережі
4) втрата, спотворення, витік інформації
5) інша відповідь

Одним з принципів політики інформаційної безпеки є принцип:
1) неможливості уникнути захисних засобів мережі (системи)
2) посилення основної ланки мережі, системи
3) повного блокування доступу при ризик-ситуаціях
4) презумпції секретності
5) інша відповідь

Одним з принципів політики інформаційної безпеки є принцип:
1) посилення захищеності самої незахищеної ланки мережі (системи)
2) переходу в безпечний стан роботи мережі, системи
3) повного доступу користувачів до всіх ресурсів мережі, системи
4) недопущення ризиків безпеки мережі, системи
5) інша відповідь

Одним з принципів політики інформаційної безпеки є принцип:
1) поділу доступу (обов'язків, привілеїв) між клієнтами мережі (системи)
2) однорівневого захисту мережі, системи
3) сумісних, однотипних програмно-технічних засобів мережі, системи
4) недопущення ризиків безпеки мережі, системи
5) інша відповідь

Витоком інформації у системі називається ситуація, що характеризується:
1) втратою даних у системі
2) зміною форми інформації
3) зміною змісту інформації
4) виходомінформаціїза межі системи
5) інша відповідь

Загроза інформаційної безпеки – це:
1) ймовірна подія
2) детермінована подія
3) подія, що відбувається періодично
4) подія, що відбувається постійно
5) інша відповідь

Різновидами загроз інформаційної безпеки (мережі, системи) є загрози:
1) програмні, технічні, організаційні, технологічні
2) серверні, клієнтські, супутникові, наземні
3) особисті, корпоративні
4) соціальні, національні
5) інша відповідь

Остаточно, відповідальність за захищеність даних у комп'ютерній мережі несе:
1) власник мережі
2) адміністратор мережі
3) користувачі мережі
4) хакери
5) інша відповідь

Політика безпеки у системі (мережі) – це комплекс:
1) посібників, вимог забезпечення необхідного рівня безпеки
2) інструкцій, алгоритмів поведінки користувача у мережі
3) норм міжнародного права, яких дотримуються в мережі
4) норм інформаційного права, яких дотримуються в мережі
5) інша відповідь

Що таке CobiT і як він ставиться до розробки систем інформаційної безпеки та програм безпеки?
1) список стандартів, процедур та політик для розробки програми безпеки
2) поточна версія ISO 17799
3) структура, яка була розроблена для зниження внутрішнього шахрайства у компаніях
4) відкритий стандарт, що визначає цілі контролю
5) інша відповідь

Найважливішим при реалізації захисних заходів політики безпеки є:
1) аудит безпеки
2) аналіз витрат на проведення захисних заходів
3) аудит безпеки та аналіз вразливостей
4) мінімізація ризик-ситуацій
5) інша відповідь

З яких чотирьох доменів складається CobiT?
1) Планування та Організація, Придбання та Впровадження, Експлуатація та Супровід, Моніторинг та Оцінка
2) Планування та Організація, Підтримка та Впровадження, Експлуатація та Супровід, Моніторинг та Оцінка
3) Планування та Організація, Придбання та Впровадження, Супровід та Покупка, Моніторинг та Оцінка
4) Придбання та Впровадження, Експлуатація та Супровід, Моніторинг та Оцінка
5) інша відповідь

OCTAVE, NIST 800-30 та AS/NZS 4360 є різними підходами до реалізації управління ризиками у компаніях. У чому різниця між цими методами?
1) NIST та OCTAVE є корпоративними
2) NIST та OCTAVE орієнтований на IT
3) AS/NZS орієнтований на IT
4) NIST та AS/NZS є корпоративними
5) інша відповідь

Захист інформації від витоку – це діяльність із запобігання:
1) отримання інформації, що захищається заінтересованим суб'єктом з порушенням встановлених правовими документами або власником правил доступу до інформації, що захищається
2) впливу з порушенням встановлених прав та/або правил на зміну інформації, що призводить до спотворення, знищення, копіювання, блокування доступу до інформації, а також до втрати, знищення чи збою функціонування носія інформації
3) впливу на інформацію, що захищається, помилок користувача інформацією, збою технічних і програмних засобів інформаційних систем, а також природних явищ,;
4) неконтрольованого поширення інформації, що захищається, її розголошення, несанкціонованого доступу
5) інша відповідь

Захист інформації – це:
1) процес збирання, накопичення, обробки, зберігання, розподілу та пошуку інформації
2) перетворення інформації, внаслідок якого зміст інформації стає незрозумілим для суб'єкта, який не має доступу
3) отримання суб'єктом можливості ознайомлення з інформацією, у тому числі за допомогою технічних засобів
4) діяльність щодо запобігання витоку інформації, несанкціонованих та ненавмисних впливів на неї
5) інша відповідь

Природні загрози безпеці інформації викликані:
1) діяльністю людини
2) помилками при проектуванні системи, її елементів чи розробці програмного забезпечення
3) впливами об'єктивних фізичних процесів чи стихійних природних явищ, незалежних від людини
4) корисливими цілями зловмисників
5) інша відповідь

Штучні загрози безпеці інформації викликані:
1) діяльністю людини
2) помилками при проектуванні системи, її елементів чи розробці програмного забезпечення
3) впливами об'єктивних фізичних процесів чи стихійних природних явищ, незалежних від людини
4) корисливими цілями зловмисників
5) інша відповідь

До основних ненавмисних штучних загроз інформаційної безпеки належить:
1) фізичне руйнування системи шляхом вибуху, підпалу тощо
2) перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв та ліній зв'язку
3) зміна режимів роботи пристроїв або програм, страйк, саботаж персоналу, постановка потужних активних перешкод тощо
4) читання залишкової інформації з оперативної пам'яті та з зовнішніх пристроїв
5) інша відповідь

До сторонніх порушників інформаційної безпеки можна віднести:
1) персонал, який обслуговує технічні засоби
2) персонал, який обслуговує будівлю
3) працівників служби безпеки
4) представників конкуруючих організацій
5) інша відповідь

Спам, який має на меті зганьбити ту чи іншу фірму, компанію, політичного кандидата тощо – це:
1) чорний піар
2) фішинг
3) нігерійські листи
4) порожні листи
5) інша відповідь

Спам, який розповсюджує підроблені повідомлення від імені банків або фінансових компаній, метою яких є збір логінів, паролів та пін-кодів користувачів – це:
1) чорний піар
2) фішинг
3) нігерійські листи
4) порожні листи
5) інша відповідь

Активне перехоплення інформації – це перехоплення, яке:
1) здійснюється за допомогою підключення до телекомунікаційного обладнання комп'ютера
2) засноване на фіксації електромагнітних випромінювань, що виникають під час функціонування засобів комп'ютерної техніки та комунікацій
3) неправомірно використовує технологічні відходи інформаційного процесу
4) здійснюється шляхом використання оптичної техніки
5) інша відповідь

Перехоплення інформації, яке полягає в установці підслуховуючого пристрою в апаратуру засобів обробки інформації називається:
1) активне перехоплення
2) пасивне перехоплення
3) аудіоперехоплення
4) відеоперехоплення
5) інша відповідь

Перехоплення інформації, яке засноване на фіксації електромагнітних випромінювань, що виникають при функціонуванні засобів комп'ютерної техніки та комунікацій називається:
1) активне перехоплення
2) пасивне перехоплення
3) аудіоперехоплення
4) відеоперехоплення
5) інша відповідь

Перехоплення інформації, яке здійснюється шляхом використання оптичної техніки називається
1) активне перехоплення
2) пасивне перехоплення
3) аудіоперехоплення
4) відеоперехоплення
5) інша відповідь

До внутрішніх порушників інформаційної безпеки можна віднести:
1) клієнтів
2) відвідувачів
3) будь-яких осіб, які перебувають усередині контрольованої території
4) персонал, який обслуговує технічні засоби
5) інша відповідь

При якісній оцінці (якісному підході) ризик вимірюється у термінах:
1) грошових втрат
2) заданих за допомогою шкали або ранжирування
3) оцінок експертів
4) обсягу інформації
5) інша відповідь

При повноважній безпековій політиці сукупність міток з однаковими значеннями утворює:
1) область рівної критичності
2) область рівного доступу
3) рівень безпеки
4) рівень доступності
5) інша відповідь

За допомогою закритого ключа інформація:
1) копіюється
2) транслюється
3) розшифровується
4) зашифровується
5) інша відповідь

Сукупність властивостей, що зумовлюють придатність інформації задовольняти певні потреби відповідно до її призначення, називається:
1) актуальністю інформації
2) доступністю інформації
3) якістю інформації
4) цілісністю інформації
5) інша відповідь

Відповідно до «Помаранчевої книги» дискреційний захист має група критеріїв:
1) D
2) A
3) B
4) C
5) інша відповідь

Відповідно до «Помаранчевої книги» мінімальний захист має група критеріїв:
1) D
2) A
3) B
4) C
5) інша відповідь

Відповідно до «Помаранчевої книги» унікальні ідентифікатори повинні мати:
1) найважливіші суб'єкти інформаційної діяльності
2) найважливіші об'єктиінформаційної діяльності
3) всі суб'єктиінформаційної діяльності
4) усі об'єктиінформаційної діяльності
5) інша відповідь

Кількіснізакономірності, зв'язані з одержанням передачею, обробкою і збереженнямінформації вивчає наука:
1) криптографія
2) теорія інформації
3) теорія кодування
4) теорія передачі даних
5) інша відповідь

Одержання оптимальних методів передачі повідомлень відносяться до завдань науки:
1) теорія інформації
2) теорія кодування
3) теорія передачі даних
4) криптографія
5) інша відповідь

Оптимальне кодування (стиск) даних відносяться до завдань науки:
1) теорія кодування
2) криптографія
3) теорія інформації
4) теорія передачі даних
5) інша відповідь

Завадостійке кодування даних відносяться до завдань науки:
1) теорія кодування
2) криптографія
3) теорія інформації
4) теорія передачі даних
5) інша відповідь

Формалізований у вигляді символів алфавіту кодування інформаційний зміст явища – це:
1) сигнали
2) дані
3) інформація
4) код
5) інша відповідь

Вивчення закономірностей передачі і перетворення інформації в теорії інформації виконується методами:
1) теорії імовірностей
2) теорії кодування
3) теорії передачі даних
4) криптографій
5) інша відповідь

Імовірнісний підхід до вивчення закономірностей передачі і перетворення інформації в теорії інформації зумовлює альтернативну назву цієї науки:
1) теорія міри кількості інформації і кодування
2) прикладна криптологія
3) теорія інформації
4) теорія передачі даних
5) інша відповідь

Формалізований у вигляді символів алфавіту кодування інформаційний зміст явища – це:
1) сигнали
2) дані
3) інформація
4) код
5) інша відповідь

Основний термін для характеристики чисельних показників невизначеності – це:
1) секретність
2) криптостійкість
3) імовірність
4) ентропія
5) інша відповідь

Повідомлення, які зменшують апріорну (початкову) невизначеність - це:
1) інформація
2) дезінформація
3) спам
4) інформаційні шуми
5) інша відповідь

Повідомлення, які збільшують апріорну (початкову) невизначеність - це:
1) інформація
2) дезінформація
3) спам
4) інформаційні шуми
5) інша відповідь

Повідомлення, отримання яких не змінює апріорну (початкову) невизначеність - це:
1) інформація
2) дезінформація
3) спам
4) інформаційні шуми
5) інша відповідь

Формалізований у вигляді символів алфавіту кодування інформаційний зміст явища – це:
1) сигнали
2) дані
3) інформація
4) код
5) інша відповідь

Дані, отримані від джерела інформації в системі передачі даних - це:
1) інформація
2) сигнали
3) повідомлення
4) код
5) інша відповідь

Носії інформації в системі передачі даних - це:
1) дані
2) сигнали
3) повідомлення
4) код
5) інша відповідь

Для якого способу кодування застосовується як базове поняття кодової відстані:
1) завадостійке
2) ентропійне
3) оптимальне
4) рівномірне
5) інша відповідь

Базове цифрове значення, що використовується при оцінці перевіряльної здатності коду - це:
1) кодова відстань
2) мінімальна кодова відстань
3) розрядність коду
4) максимальна кодова відстань
5) інша відповідь

Базове цифрове значення, що використовується при оцінці корегувальної здатності коду - це:
1) розрядність коду
2) максимальна кодова відстань
3) мінімальна кодова відстань
4) кодова відстань
5) інша відповідь

Яка операція алгебри логіки використовується для обчислення кодової відстані між комбінаціями коду:
1) додавання за модулем 2 (XOR)
2) логічне множення (AND)
3) логічне додавання (OR)
4) інверсія (NOT)
5) інша відповідь

Яка з перелічених задач не є класичною задачею теорії кодування (відноситься до задач іншої науки):
1) представлення інформації в технічних системах
2) стиск даних (оптимальне кодування)
3) забезпечення безпомилкової передачі інформації (завадостійке кодування)
4) забезпечення секретності інформації (криптографічне кодування)
5) інша відповідь

Сукупність технічних засобів, призначених для передачі інформації (повідомлень) від об'єкта до адресата – це:
1) канал зв'язку
2) інформаційна система
3) лінія зв'язку
4) комп'ютерна система
5) інша відповідь

Середовище, у якому поширюються сигнали, що несуть інформацію в система передачі даних – це:
1) канал зв'язку
2) інформаційна система
3) лінія зв'язку
4) комп'ютерна система
5) інша відповідь

Мультиплексування (ущільнення) в системах передачі даних забезпечує:
1) більш ефективне використання ресурсів лінії зв'язку її користувачем
2) більш ефективне використання ресурсів каналу зв'язку її користувачем
3) ефективне використання (розподіл) ресурсів лінії зв'язку декількома користувачами
4) ефективне використання (розподіл) ресурсів каналу зв'язку декількома користувачами
5) інша відповідь

Мультиплексування з частотним поділом каналів (FDM) передбачає:
1) виділення кожному користувачу певного діапазону частот (каналу) з загального спектру частот лінії зв'язку без обмежень в часі
2) виділення кожному користувачу певного діапазону частот (каналу) з загального спектру частот лінії зв'язку на певний час
3) виділення кожному користувачу всього діапазону частот лінії зв'язку на певний час
4) виділення кожному користувачу всього діапазону частот каналу зв'язку на певний час
5) інша відповідь

Мультиплексування з частотним поділом каналів (FDM) передбачає:
1) виділення кожному користувачу певного діапазону частот (каналу) з загального спектру частот лінії зв'язку без обмежень в часі
2) виділення кожному користувачу певного діапазону частот (каналу) з загального спектру частот лінії зв'язку на певний час
3) виділення кожному користувачу всього діапазону частот лінії зв'язку на певний час
4) виділення кожному користувачу всього діапазону частот каналу зв'язку на певний час
5) інша відповідь

Дискретну будівлю масивів інформації і їхній вимір простим підрахунком інформаційних елементів (квантів) вивчає :
1) структурна теорія інформації
2) комбінаторна теорія інформації
3) статистична теорія інформації
4) семантична теорія інформації
5) інша відповідь

Вимір інформації комбінаторним методом вивчає :
1) структурна теорія інформації
2) комбінаторна теорія інформації
3) статистична теорія інформації
4) семантична теорія інформації
5) інша відповідь

Яка теорія оперує поняттям ентропія як міри невизначеності, що враховує імовірність появи, а, отже, і інформативність тих чи інших повідомлень:
1) структурна теорія інформації
2) комбінаторна теорія інформації
3) статистична теорія інформації
4) семантична теорія інформації
5) інша відповідь

Яка теорія враховує доцільність, цінність, чи корисність (істотність) інформації (тобто, зміст повідомлення):
1) структурна теорія інформації
2) комбінаторна теорія інформації
3) статистична теорія інформації
4) семантична теорія інформації
5) інша відповідь

Середня величина невизначеності настання випадкових подій у кінцевій системі – це:
1) імовірність
2) статистика
3) ентропія
4) систематичність
5) інша відповідь

Вираз «джерело повідомлень має ентропію X двійкових одиниць в секунду» означає, що:
1) джерело видає X двійкових одиниць інформації в секунду
2) джерело видає X двійкових одиниць даних в секунду
3) джерело видає X двійкових одиниць коду в секунду
4) джерело видає X двійкових сигналів в секунду
5) інша відповідь

Ентропія системи максимальна у випадку:
1) зростання імовірностей подій
2) зменшення імовірностей подій
3) однакових імовірностей подій
4) непередбачуваності імовірностей подій
5) інша відповідь

До якої категорії кодів відноситься американська стандартна таблиця кодування ASCII:
1) завадостійкі коди
2) оптимальні коди
3) рівномірні коди
4) нерівномірні коди
5) інша відповідь

До якої категорії кодів відноситься міжнародний стандарт кодування Unicode:
1) рівномірні коди
2) завадостійкі коди
3) оптимальні коди
4) нерівномірні коди
5) інша відповідь

В результаті рандомізації коду повідомлень ентропія традиційно:
1) зменшується
2) збільшується
3) усувається
4) не змінюється
5) інша відповідь

В яких задачах використовується збільшення надлишковості коду для досягнення позитивного результату:
1) ентропійне кодування
2) рандомізація коду
3) оптимальне кодування
4) словникове кодування
5) інша відповідь

Який спосіб кодування використовує збільшення надлишковості коду для досягнення позитивного результату:
1) завадостійке кодування
2) оптимальне кодування
3) словникове кодування
4) ентропійне кодування
5) інша відповідь

Який з перелічених методів кодування може використовуватись для рандомізації коду повідомлень:
1) циклічний код
2) код з перевіркою на парність
3) код Хеммінга
4) код Шеннона-Фано
5) інша відповідь

Який з перелічених методів кодування може використовуватись для рандомізації коду повідомлень:
1) код Хаффмена
2) код Хеммінга
3) циклічний код
4) код з перевіркою на парність
5) інша відповідь

До якої категорії кодів відноситься код Хаффмена:
1) рівномірний
2) нерівномірний
3) завадостійкий
4) універсальний
5) інша відповідь

До якої категорії кодів відноситься код Шеннона-Фано:
1) рівномірний
2) нерівномірний
3) завадостійкий
4) універсальний
5) інша відповідь

До якої категорії кодів відноситься код Хеммінга:
1) рівномірний
2) нерівномірний
3) оптимальний
4) універсальний
5) інша відповідь

До якої категорії кодів відноситься циклічний код:
1) рівномірний
2) нерівномірний
3) оптимальний
4) універсальний
5) інша відповідь

До якої категорії кодів відноситься код з перевіркою на парність:
1) рівномірний
2) нерівномірний
3) оптимальний
4) універсальний
5) інша відповідь

До якої категорії кодів відноситься код Хаффмена:
1) оптимальний ентропійний
2) оптимальний словниковий
3) завадостійкий
4) криптографічний
5) інша відповідь

До якої категорії кодів відноситься код Шеннона-Фано:
1) оптимальний ентропійний
2) оптимальний словниковий
3) завадостійкий
4) криптографічний
5) інша відповідь

До якої категорії кодів відноситься спосіб кодування Лемпеля-Зіва (LZ):
1) оптимальний ентропійний
2) оптимальний словниковий
3) завадостійкий
4) криптографічний
5) інша відповідь

До якої категорії кодів відноситься спосіб кодування Лемпеля-Зіва-Велча (LZW):
1) оптимальний ентропійний
2) оптимальний словниковий
3) завадостійкий
4) криптографічний
5) інша відповідь

До якої категорії кодів відноситься спосіб кодування Лемпеля-Зіва-Маркова (LZMA):
1) оптимальний ентропійний
2) оптимальний словниковий
3) завадостійкий
4) криптографічний
5) інша відповідь

До якої категорії кодів відноситься код Хеммінга:
1) оптимальний ентропійний
2) оптимальний словниковий
3) завадостійкий
4) криптографічний
5) інша відповідь

До якої категорії кодів відноситься циклічний код:
1) оптимальний ентропійний
2) оптимальний словниковий
3) завадостійкий
4) криптографічний
5) інша відповідь

До якої категорії кодів відноситься код з перевіркою на парність:
1) оптимальний ентропійний
2) оптимальний словниковий
3) завадостійкий
4) криптографічний
5) інша відповідь

Як класифікується властивість завадостійкого коду виявляти помилки:
1) перевіряльна здатність
2) оптимізаційна здатність
3) криптостійкість
4) корегувальна здатність
5) інша відповідь

Як класифікується властивість завадостійкого коду виправляти виявлені помилки:
1) перевіряльна здатність
2) оптимізаційна здатність
3) криптостійкість
4) корегувальна здатність
5) інша відповідь

Яку кількість помилок може виявляти код Хаффмена:
1) 0
2) 1
3) 2
4) 3
5) інша відповідь

Яку кількість помилок може виявляти код Шеннона-Фано (гарантоване виявлення помилок заданої кратності):
1) 0
2) 1
3) 2
4) 3
5) інша відповідь

Яку кількість помилок може виявляти код Хаффмена (гарантоване виявлення помилок заданої кратності):
1) 0
2) 1
3) 2
4) 3
5) інша відповідь

Яку кількість помилок може виявляти код Хеммінга (гарантоване виявлення помилок заданої кратності):
1) 0
2) 1
3) 2
4) 3
5) інша відповідь

Яку кількість помилок може виявляти код з перевіркою на парність (гарантоване виявлення помилок заданої кратності):
1) 0
2) 1
3) 2
4) 4
5) інша відповідь

Яку кількість помилок може виявляти код з перевіркою на парність (гарантоване виявлення помилок заданої кратності):
1) 0
2) 4
3) 2
4) 3
5) інша відповідь

Яку кількість помилок може виправляти код Хеммінга:
1) 0
2) 1
3) 2
4) 3
5) інша відповідь

Яку кількість помилок може виправляти код з перевіркою на парність:
1) 0
2) 1
3) 2
4) 4
5) інша відповідь

В якому варіанті масок наведені варіанти спотворення коду відповідають груповим помилкам кратності 4 (* - спотворений біт):
1) 01*11**1, 10****00, 1*1***00
2) 01****01, 10**1**0, 111***0*
3) 01*11*01, 10**1*00, 11****00
4) *1*1*1*1, 10**10**, 111****0
5) інша відповідь

В якому варіанті масок наведені варіанти спотворення коду відповідають груповим помилкам кратності 5 (* - спотворений біт):
1) 10*****0, 0**11**1, 1*1***00
2) 10*****0, *1****01, **1***01
3) 11*11*01, 10**1*00, 11****01
4) *1*1*1**, 10**10**, 1*1****0
5) інша відповідь

В якому варіанті всі наведені комбінації коду не містять помилок, якщо для контролю використано завадостійке кодування з перевіркою на парність :
1) 101000000, 011100010, 000000000
2) 111010000, 010001100, 000000000
3) 101011011, 111001100, 000001000
4) 111010000, 010001101, 100000000
5) інша відповідь

В якому варіанті всі наведені комбінації коду не містять помилок, якщо для контролю використано завадостійке кодування з перевіркою на парність :
1) 111010, 001100, 010000
2) 101000, 100010, 000000
3) 101011, 111000, 011000
4) 111010, 001101, 000000
5) інша відповідь

Який вид завадостійкого коду формує при перевірці код номера позиції розряду з помилкою:
1) код Хеммінга
2) код з перевіркою на парність
3) код з перевіркою на непарність
4) циклічний код
5) інша відповідь

Який вид завадостійкого коду має реалізацію, що не дозволяє розділити інформаційні та контрольні розряди:
1) код Хеммінга
2) код з перевіркою на парність
3) код з перевіркою на непарність
4) циклічний код
5) інша відповідь

Який вид завадостійкого коду при кодуванні використовує утворюючий поліном:
1) код Хеммінга
2) код з перевіркою на парність
3) код з перевіркою на непарність
4) циклічний код
5) інша відповідь

Який вид завадостійкого коду розміщує контрольні розряди на фіксовані позиції між інформаційними:
1) код Хеммінга
2) код з перевіркою на парність
3) код з перевіркою на непарність
4) циклічний код
5) інша відповідь

Яка кількість контрольних розрядів додається до двійкового слова з 8 розрядів при застосуванні завадостійкого коду з перевіркою на парність:
1) 0
2) 1
3) 2
4) 4
5) інша відповідь

Яка кількість контрольних розрядів додається до двійкового слова з 6 розрядів при застосуванні завадостійкого коду з перевіркою на непарність:
1) 0
2) 1
3) 2
4) 4
5) інша відповідь

Яка кількість контрольних розрядів додається до двійкового слова з 8 розрядів при застосуванні завадостійкого коду Хеммінга:
1) 1
2) 2
3) 3
4) 4
5) інша відповідь

Яка кількість контрольних розрядів додається до двійкового слова з 4 розрядів при застосуванні завадостійкого коду Хеммінга:
1) 1
2) 2
3) 3
4) 4
5) інша відповідь

Яка кількість контрольних розрядів додається до двійкового слова з 8 розрядів при застосуванні циклічного кодування з утворюючим поліномом 10011:
1) 1
2) 2
3) 3
4) 4
5) інша відповідь

Яка кількість контрольних розрядів додається до двійкового слова з 8 розрядів при застосуванні циклічного кодування з утворюючим поліномом 1011:
1) 1
2) 2
3) 3
4) 4
5) інша відповідь

Який вид завадостійкого кодування при корегуванні помилок використовує операцію зсуву:
1) код Хеммінга
2) код з перевіркою на парність
3) код з перевіркою на непарність
4) циклічний код
5) інша відповідь

Яка операція алгебри логіки використовується при формуванні коду Хеммінга:
1) додавання за модулем 2 (XOR)
2) логічне множення (AND)
3) логічне додавання (OR)
4) інверсія (NOT)
5) інша відповідь

Яка операція алгебри логіки використовується при формуванні циклічного коду повідомлення:
1) логічне множення (AND)
2) логічне додавання (OR)
3) додавання за модулем 2 (XOR)
4) інверсія (NOT)
5) інша відповідь

Дискретизація сигналу є характерною ознакою процесу:
1) перетворення аналогового сигналу в цифрову форму
2) зменшення якості несучого сигналу при передачі секретного повідомлення
3) перетворення цифрового сигналу в аналоговий
4) демодуляції сигналу після кодово-імпульсної модуляції
5) інша відповідь

При якому виді модуляції сигналу використовуються його дискретизація:
1) кодово-імпульсна модуляція (КІМ)
2) фазова модуляція (ФМ)
3) частотна модуляція (ЧМ)
4) амплітудна модуляція (АМ)
5) інша відповідь

При якому виді модуляції не виконується частотне заповнення сигналів, що відповідають логічним значенням 0 і 1:
1) кодово-імпульсна модуляція (КІМ)
2) фазова модуляція (ФМ)
3) частотна модуляція (ЧМ)
4) амплітудна модуляція (АМ)
5) інша відповідь

При якому виді модуляції цифрових сигналів застосовувана частота і рівень напруги несучого сигналу, що відповідають логічним значенням 0 і 1, не змінюються:
1) кодово-імпульсна модуляція (КІМ)
2) фазова модуляція (ФМ)
3) частотна модуляція (ЧМ)
4) амплітудна модуляція (АМ)
5) інша відповідь

При якому виді модуляції цифрових сигналів змінюється рівень напруги несучого сигналу в посилках, що відповідають логічним значенням 0 і 1:
1) кодово-імпульсна модуляція (КІМ)
2) фазова модуляція (ФМ)
3) частотна модуляція (ЧМ)
4) амплітудна модуляція (АМ)
5) інша відповідь

При якому виді модуляції цифрових сигналів частота несучого сигналу в посилках, що відповідають логічним значенням 0 і 1:
1) кодово-імпульсна модуляція (КІМ)
2) фазова модуляція (ФМ)
3) частотна модуляція (ЧМ)
4) амплітудна модуляція (АМ)
5) інша відповідь

Загрози доступності інформації у інформаційно-комунікаційних системах - це:
1) ненавмисні помилки користувачів, відмова програмного та апаратного забезпечення, руйнування або пошкодження приміщень
2) зловмисна підміна даних, хакерська атака
3) перехоплення даних, хакерська атака
4) викрадення баз даних
5) інша відповідь

Суть компрометації інформації:
1) внесення змін до бази даних, внаслідок чого користувач позбавляється доступу до інформації
2) несанкціонований доступ до інформації, що передається по каналах зв'язку та знищення змісту переданих повідомлень
3) внесення несанкціонованих змін до бази даних, внаслідок чого споживач змушений або відмовитися від неї, або докладати зусиль для виявлення змін та відновлення істинних відомостей
4) отримання незаконного прибутку
5) інша відповідь

Інформаційна безпека автоматизованої системи – це стан автоматизованої системи, при якому вона:
1) з одного боку, здатна протистояти впливу зовнішніх та внутрішніх інформаційних загроз, а з іншого - її наявність та функціонування не створює інформаційних загроз для елементів самої системи та зовнішнього середовища
2) з одного боку, здатна протистояти впливу зовнішніх та внутрішніх інформаційних загроз, а з іншого – витрати на її функціонування нижчі, ніж передбачуваний збиток від витоку інформації, що захищається
3) здатна протистояти лише інформаційним загрозам, як зовнішнім так і внутрішнім
4) здатна протистояти лише зовнішнім інформаційним загрозам
5) інша відповідь

Методи підвищення достовірності вхідних даних у інформаційно-комунікаційних системах:
1) заміна процесу введення значення процесом вибору значення з запропонованої множини, введення надмірності в документ першоджерела, використання замість введення значення його зчитування з зовнішнього носія
2) відмова від використання даних, проведення комплексу регламентних робіт
3) проведення комплексу регламентних робіт, використання замість введення значення його зчитування з зовнішнього носія
4) багаторазове введення даних та звірення введених значень
5) інша відповідь

Принципова відмінність міжмережних екранів (МЕ) від систем виявлення атак (СОВ):
1) МЕ були розроблені для активного або пасивного захисту, а СОВ – для активного або пасивного виявлення
2) МЕ були розроблені для активного або пасивного виявлення, а СОВ – для активного або пасивного захисту
3) МЕ працюють лише на мережевому рівні, а СОВ – ще й на фізичному
4) нема ніякої різниці
5) інша відповідь

Сервіси безпеки у інформаційно-комунікаційних системах:
1) ідентифікація та аутентифікації, шифрування, контроль цілісності, забезпечення безпечного відновлення
2) інверсія паролів, контроль цілісності
3) регулювання конфліктів, екранування
4) забезпечення безпечного відновлення, інверсія паролів, кешування записів
5) інша відповідь

Під загрозою віддаленого адміністрування в комп'ютерній мережі розуміється загроза:
1) несанкціонованого керування віддаленим комп'ютером
2) впровадження агресивного програмного коду в рамках активних об'єктів Web-сторінок
3) перехоплення або заміни даних на шляхах транспортування
4) втручання у особисте життя
5) інша відповідь

Що з перерахованого **не є** причиною виникнення помилок даних в інформаційно-комунікаційних системах:
1) похибка вимірювань
2) помилка під час запису результатів вимірювань у проміжний документ
3) помилки при перенесенні даних із проміжного документа до комп'ютера
4) умисне спотворення даних
5) інша відповідь

Що з перерахованого є причиною виникнення помилок даних в інформаційно-комунікаційних системах:
1) неправильна інтерпретація даних
2) використання неприпустимих методів аналізу даних
3) непереборні причини природного характеру
4) помилки при ідентифікації об'єкта чи суб'єкта інформаційної діяльності
5) інша відповідь

Найефективніший засіб для захисту від мережних атак:
1) використання мережевих екранів або «firewall»
2) використання антивірусних програм
3) відвідування лише «надійних» Інтернет-вузлів
4) використання лише сертифікованих програм-браузерів при доступі до мережі Інтернет
5) інша відповідь

Витік інформації у інформаційно-комунікаційних системах – це:
1) несанкціонований процес перенесення інформації від джерела до зловмисника
2) процес розкриття таємної інформації
3) процес знищення інформації
4) ненавмисна втрата носія інформації
5) інша відповідь

Документ, який визначив найважливіші сервіси безпеки та запропонував метод класифікації інформаційно-комунікаційних систем з вимог безпеки - це:
1) рекомендації X.800
2) Помаранчева книга
3) Закон «Про інформацію, інформаційні технології та про захист інформації»
4) такого документу на сьогоднішній день ще не існує
5) інша відповідь

Концепція системи захисту від інформаційної зброї не повинна включати в себе:
1) засоби нанесення контратаки за допомогою інформаційної зброї
2) механізми захисту користувачів від різних типів та рівнів загроз для національної інформаційної інфраструктури.
3) ознаки, що сигналізують про можливий напад
4) процедури оцінки рівня та особливостей атаки проти національної інфраструктури в цілому та окремих користувачів
5) інша відповідь

Навмисна загроза безпеці інформації:
1) повінь
2) пошкодження кабелю, яким йде передача, у зв'язку з погодними умовами
3) помилка розробника ПЗ
4) крадіжка даних
5) інша відповідь

Захист інформації у інформаційно-комунікаційних системах**не** націлений на:
1) забезпечення захисту інформації від неправомірного доступу, знищення, модифікування, блокування, копіювання, надання, розповсюдження, а також від інших неправомірних дій щодо інформації
2) реалізацію права на доступ до інформації
3) виявлення порушників та притягнення їх до відповідальності
4) дотримання конфіденційності інформації обмеженого доступу
5) інша відповідь
