МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Державний університет інтелектуальних технологій і зв'язку

ЗАТВЕРДЖУЮ
Голова приймальної комісії
Ректор
Олександр НАЗАРЕНКО
«13» травня 2022 р.

ПРОГРАМА

ФАХОВОГО ІСПИТУ
для конкурсного відбору вступників за другим рівнем вищої освіти «магістр»

Ступінь: Магістр
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека»

Одеса – 2022

ПЕРЕДМОВА

Мета фахового іспиту полягає у визначенні рівня підготовки абітурієнтів для проведення конкурсного відбору для навчання в Державному університеті інтелектуальних технологій і зв’язку (далі: Університет) на магістерському рівні за відповідною спеціальністю.

Фаховий іспит полягає в комплексній перевірці знань абітурієнтів, отриманих ними в результаті вивчення циклу дисциплін, передбачених освітньо-професійною програмою та навчальними планами бакалаврату спеціальності 125 «Кібербезпека». Студент повинен продемонструвати фундаментальні та професійно-орієнтовані уміння та знання щодо узагальненого об’єкта дослідження і здатність вирішувати типові професійні завдання, передбачені для відповідних посад.

Фаховий іспит базується на матеріалах з дисциплін: «Криптографічний захист інформації», «Забезпечення безпеки телекомунікацій», «Теорія інформації та кодування», «Комплексні системи захисту інформації: проектування, впровадження та супровід».

Екзаменаційний білет містить 4 завдання відповідно до змісту вищезазначених дисциплін – по одному завданню на кожну дисципліну.

ФОРМА ФАХОВОГО ВСТУПНОГО ІСПИТУ

Згідно з чинними «Правилами прийому до Державного університету інтелектуальних технологій і зв'язку у 2022 р.», для бажаючих продовжити навчання за ступенем магістра на основі базової вищої освіти передбачено обов'язкове складання комплексного вступного іспиту з фахових дисциплін. Нижче наведена структура даного іспиту та навчальні матеріали, які рекомендовані для опрацювання в ході підготовки до нього.

1. Абітурієнт відповідає на 4 питання, що зазначені в екзаменаційному білеті. Питання взяті з відповідних навчальних програм дисциплін «Криптографічний захист інформації», «Забезпечення безпеки телекомунікацій», «Теорія інформації та кодування», «Комплексні системи захисту інформації: проектування, впровадження та супровід», відповідно до програми підготовки бакалаврів.

Час на підготовку відповідей – 3 академічних години. Сумарна оцінка розраховується як середня арифметична з чотирьох окремих оцінок.

2. Перелік питань, покладених в основу вступного іспиту з фахових дисциплін, наведено у Додатку 1 та представлено у відповідному розділі на сайті Університету (*suitt.edu.ua*).

3. При оцінюванні знань абітурієнта під час вступного іспиту з фахових дисциплін відповідно до чинних «Правил прийому до Державного університету інтелектуальних технологій і зв'язку у 2022 р.» використовується 200-бальна система оцінки, за якою оцінка «відмінно» відповідає 175-200 балам, оцінка «добре» – 135-174 балам, оцінка «задовільно» – 100-134 балам, при отриманні менш ніж 100 балів абітурієнт отримує оцінку «незадовільно».

КРИТЕРІЇ ОЦІНЮВАННЯ

При оцінюванні знань абітурієнта вихідними критеріями є такі:

- оцінку «**відмінно**» (175-200 балів) абітурієнт отримує, якщо він, після підготовки відповідей в межах встановленого для цього часу, правильно виразив власну думку, що не суперечить теоретичному матеріалу з відповідної дисципліни; не зробив жодної помилки при формулюванні усних відповідей; зв'язано, логічно, тематично адекватно і зрозуміло побудував свої відповіді, а також може невимушено, без жодних складнощів, вільно дати пояснення представнику комісії під час іспиту (реагувати на пропозиції та запитання, ставити запитання в разі виникнення непорозуміння щодо отриманого завдання або зазначеного в білеті запитання);

- оцінку «**добре**» (135-174 балів) абітурієнт отримує, якщо він, після підготовки відповідей в межах встановленого для цього часу, виразив власну думку, що не суперечить теоретичному матеріалу з відповідної дисципліни; зробив незначні помилки при формулюванні усних відповідей; не завжди зв'язано, логічно, тематично адекватно і зрозуміло будував свої відповіді, але певною мірою може невимушено, без жодних складнощів, вільно дати пояснення представнику комісії під час іспиту (реагувати на пропозиції та запитання, ставити запитання в разі виникнення непорозуміння щодо отриманого завдання або зазначеного в білеті запитання);
- оцінку «**задовільно**» (100-134 балів) абітурієнт отримує, якщо він, після підготовки відповідей в межах встановленого для цього часу, намагався виразити власну думку, що не суперечить теоретичному матеріалу з відповідної дисципліни; зробив певною мірою некритичні помилки при формулюванні усних відповідей; не завжди зв'язано, логічно, тематично адекватно і зрозуміло будував свої відповіді, але певною мірою може дати пояснення своїх відповідей на запитання представнику комісії під час іспиту (реагувати на пропозиції та запитання, ставити запитання в разі виникнення непорозуміння щодо отриманого завдання або зазначеного в білеті запитання);
- оцінку «**незадовільно**» (менше 100 балів) абітурієнт отримує, якщо він не може дати відповіді після їх підготовки в межах встановленого для цього часу; припускає грубі помилки у відповідях, які не відповідають змісту теоретичного матеріалу з відповідної дисципліни та не дає представнику комісії відповідей на жодне з додаткових запитань.

Додаток 1

Перелік запитань до фахового іспиту для осіб, що виявили бажання продовжити навчання для здобуття ступеня магістра

За спеціальністю: 125 «Кібербезпека»

Теорія інформації та кодування

1. Кількість символів алфавіту складає N=43. Чому дорівнює ентропія повідомлення? Яка потрібна кількість двійкових елементів в кодовій комбінації для передавання символів цього алфавіту.

2. Запишіть номер правильної, на Ваш погляд, відповіді:
Яка із телекомунікаційних систем з багатократною передачею повідомлення має кращу здатність по виправленню помилок:
1) з мажоритарним поелементним прийомом;
2) з мажоритарним посимвольним прийомом.

Обґрунтуйте відповідь.

3. Чому дорівнює кратність виправлення та виявлення помилок при застосуванні завадостійкого коду з мінімальною кодовою відстанню $d_0 = 5$? В якому випадку завадостійкість телекомунікаційної системи буде кращою: у режимі виправлення або виявлення помилок. Обґрунтуйте відповідь.

4. Запишіть номер правильної, на Ваш погляд, відповіді:
У телекомунікаційній системі з інформаційним зворотнім зв'язком оцінка якості прийнятого повідомлення приймачем виробляється на:
1) передавальній стороні прямого каналу;
2) приймальній стороні прямого каналу;
3) як на передавальній так і на приймальній сторонах прямого каналу.
Обґрунтуйте відповідь.

5. Запишіть номер варіанту правильної, на Ваш погляд, відповіді:
У телекомунікаційній системі (з вирішальним зворотнім зв'язком та очікуванням) наступний кодовий блок передається лише після:
1) одержання сигналу підтвердження по зворотньому каналу;
2) одержання сигналу перезапиту по зворотньому каналу;
3) одержання будь-якого сигналу по зворотньому каналу.
Обґрунтуйте відповідь.

6. Запишіть номер варіанту правильної, на Ваш погляд, відповіді:
Зворотній зв'язок у телекомунікаційній системі необхідний для:
1) збільшення швидкості модуляції у каналі зв'язку;
2) розширення функціональних можливостей апаратури;
3) адаптації процесу передавання до зміни якості каналу зв'язку.
Обґрунтуйте відповідь.

7. Запишіть номер правильної, на Ваш погляд, відповіді:
У телекомунікаційній системі без зворотнього зв'язку в основному використовується режим завадостійкого коду:
1) з виявленням помилок:
2) з виправленням помилок;
3) у комбінованому режимі.
Обґрунтуйте відповідь.

8. Запишіть номер правильної, на Ваш погляд, відповіді:
Ефективність телекомунікаційної системи із зворотним зв'язком знижується при:
1) групуванні помилок в каналі;
2) незалежному потоці помилок в каналі.
Обґрунтуйте відповідь.

9. Запишіть номер правильної, на Ваш погляд, відповіді:
В якому каналі зв'язку кратність появи помилок в кодовому блоку більша:
1) з групуванням помилок;
2) з незалежними помилками.
Як впливає довжина кодового блоку на ймовірність $P(\geq 1, n)$.
Обґрунтуйте відповідь.

10. Запишіть номера правильних, на Ваш погляд, відповідей:
Що відбувається в каналі при збільшенні коефіцієнту групування помилок α:
1) кратність появи помилок в кодовій комбінації зменшується;
2) кратність появи помилок в кодовій комбінації збільшується;
3) ймовірність спотворення кодової комбінації зменшується;

4) ймовірність спотворення кодової комбінації збільшується;
5) число запитів в системі із зворотнім зв'язком зменшується.
Обґрунтуйте відповідь.

11. Встановити відповідність відповідей у вигляді комбінації цифр та літер:
Імовірність помилки кодової комбінації $P(\geq 1, n)$ для каналу з незалежними помилками і при їхньому пакетуванні можна розрахувати за допомогою формули:

Формула	Канал
1 $P(\geq 1, n) \cong np_{пом}$	A З незалежним розподілом помилок
2 $P(\geq 1, n) = \sum_{t=1}^{n} C_n^t p_{пом}^t (1 - p_{пом})^{n-t}$	B З пакетуванням помилок
3 $P(\geq 1, n) \cong n^{1-\alpha} p_{пом}$	

1 2 3.
Обґрунтуйте відповідь.

12. Ймовірність прийому помилкової комбінації $P(\geq 1,n)$ довжиною n=12 елементів з ймовірністю помилки $p_{пом}$=0,001 складає:
1) 1,19* 10^{-4}
2) 1,19* 10^{-6}
3) 1,20*10^{-2}
Обґрунтуйте відповідь.

13. Кількість символів алфавіту складає N =69. Чому дорівнює ентропія повідомлення?
Яка кількість двійкових елементів в кодовій комбінації потрібна для передавання символів цього алфавіту.

14. Запишіть номер правильної, на Ваш погляд, відповіді:
Телекомунікаційна система з багатократною передачею (S =5) та мажоритарним поелементним прийомом гарантує кратність виправлення помилок у кодовому блоку $k = 8$:
1) 3;
2) 2;
3) 5.
Обґрунтуйте відповідь.

15. Чому дорівнює кратність виправлення та виявлення помилок при застосуванні завадостійкого коду з мінімальною кодовою відстанню $d_0 = 7$? В якому випадку завадостійкість телекомунікаційної системи буде кращою: у режимі виправлення або виявлення помилок. Обґрунтуйте відповідь.

16. Запишіть номер правильної, на Ваш погляд, відповіді.
Ефективна швидкість передавання R у телекомунікаційній системі з повним інформаційним зворотнім зв’язком:
1) >0,5;
2) $\leq 0{,}5$;
3) <0,5.
Обґрунтуйте відповідь.

17. Запишіть номер варіанту правильної, на Ваш погляд, відповіді:
У телекомунікаційній системі (з вирішальним зворотнім зв’язком та очікуванням) наступний кодовий блок передається лише після:
1) одержання сигналу підтвердження по зворотньому каналу;
2) одержання сигналу перезапиту по зворотньому каналу;
3) одержання будь-якого сигналу по зворотньому каналу.
Обґрунтуйте відповідь.

18. Запишіть номер правильної, на Ваш погляд, відповіді:
Зворотній зв’язок в телекомунікаційній системі забезпечує:
1) збільшення швидкості модуляції у каналі зв’язку;
2) розширення функціональних можливостей апаратури;
3) адаптацію процесу передавання інформації до зміни якості каналу зв’язку.
Обґрунтуйте відповідь.

19. Запишіть номер правильної, на Ваш погляд, відповіді:
У телекомунікаційній системі без зворотнього зв’язку в основному використовується режим завадостійкого коду:
1) з виявленням помилок:
2) з виправленням помилок;
3) у комбінованому режимі.
Обґрунтуйте відповідь.

20. Запишіть номер правильної, на Ваш погляд, відповіді:
Ефективність телекомунікаційної системи із зворотнім зв'язком знижується при:
1) групуванні помилок в каналі;
2) незалежному потоці помилок в каналі
Обґрунтуйте відповідь.

21. Запишіть номер правильної, на Ваш погляд, відповіді:
У якому каналі кратність появи помилок більша:
1) з групуванням помилок;
2) з незалежними помилками.
Обґрунтуйте відповідь.

22. Запишіть формулу Шеннона про пропускну здатність каналу і охарактеризуйте методи підвищення швидкості передавання в сучасних телекомунікаційних системах.

23. Кількість символів алфавіту складає N=28. Чому дорівнює ентропія повідомлення? Яка потрібна кількість двійкових елементів в кодовій комбінації для передавання символів цього алфавіту.

24. Для чого застосовується завадостійке кодування. Основні параметри завадостійких кодів. Розрахувати кодову швидкість, якщо довжина інформаційної послідовності k=11, а довжина перевірочної частини складається з r=4 елементів

25. Чому дорівнює кратність виправлення та виявлення помилок при застосуванні завадостійкого коду з мінімальною кодовою відстанню $d_0 = 6$? В якому випадку завадостійкість телекомунікаційної системи буде кращою: у режимі виправлення або виявлення помилок. Обґрунтуйте відповідь.

26. Запишіть номер правильної, на Ваш погляд, відповіді:
У телекомунікаційній системі з інформаційним зворотнім зв’язком оцінка якості прийнятого повідомлення приймачем виробляється на:
1) передавальній стороні прямого каналу;
2) приймальній стороні прямого каналу;
3) як на передавальній так і на приймальній сторонах прямого каналу.
Обґрунтуйте відповідь.

27. Запишіть номер варіанту правильної, на Ваш погляд, відповіді:
У телекомунікаційній системі (з вирішальним зворотнім зв’язком та очікуванням) наступний кодовий блок передається лише після:
1) одержання сигналу підтвердження по зворотньому каналу;
2) одержання сигналу перезапиту по зворотньому каналу;
3) одержання будь-якого сигналу по зворотньому каналу.
Обґрунтуйте відповідь.

28. Кількість символів алфавіту складає N =23. Чому дорівнює ентропія повідомлення?
Яка кількість двійкових елементів в кодовій комбінації потрібна для передавання символів цього алфавіту.

29. Чому дорівнює кратність виправлення та виявлення помилок при застосуванні завадостійкого коду з мінімальною кодовою відстанню $d_0 = 8$? В якому випадку завадостійкість телекомунікаційної системи буде кращою: у режимі виправлення або виявлення помилок. Обґрунтуйте відповідь.
30. Запишіть номер правильної, на Ваш погляд, відповіді:
У телекомунікаційній системі (з вирішальним зворотнім зв'язком та адресним перезапитом) перезапит пакета здійснюється лише після:
1) виявлення помилки в пакеті при декодуванні, блокування приймача, одержання сигналу перезапиту по зворотньому каналу;
2) виявлення помилки в пакеті при декодуванні та одержання сигналу перезапиту по зворотньому каналу;
3) одержання будь-якого сигналу по зворотньому каналу.
Обґрунтуйте відповідь.

31. Запишіть формулу Шеннона про пропускну здатність каналу і охарактеризуйте методи підвищення швидкості передавання інформації за рахунок різних методів модуляції.

32. Методи модуляції. Наведіть часові діаграми маніпуляції послідовності 10101 за допомогою ФМ, ЧМ і АМ.

Забезпечення безпеки телекомунікацій.

1. Порівняти модель OSI та TCP/IP, та навести основні протоколи інформаційної безпеки що використовуються на різних рівнях цих моделей.
2. Протокол ARP. Призначення, принцип дії та типові атаки на цей протокол.
3. Списки контролю доступу ACL.
4. Протокол DHCP. Призначення, принцип дії та типові атаки на цей протокол.
5. Протокол ICMP. Призначення, принцип дії та типові атаки на цей протокол.
6. Перерахувати типові проблеми та загрози, що виникають на кінцевих пристроях при роботі в мережі на прикладі підключення до мережі персонального комп'ютера.
7. Дайте визначення складових протоколу AAA.
8. Що таке автентифікація? Які методи автентифікації існують?
9. Що таке авторизація? Основні типи керування доступом.
10. Що таке аудит? Вимоги до систем аудиту.
11. Протокол Kerberos. Принцип роботи.
12. Протокол RADIUS. Які основні задачі можна вирішувати за його допомогою?
13. Протокол TACACS+. Принципи роботи.
14. Які рівні захисту існують в сучасних операційних системах? Які задачі вони вирішують?
15. Як вирішується задача захисту від НСД в ОС Windows?
16. Як вирішується задача захисту від НСД в ОС Linux?
17. Система безпеки PAM в ОС Linux.
18. Використання пакетних фільтрів в Linux на прикладі iptables.
19. Написати правила брандмауера для ОС linux, які відкривають 23 порт і 22 порт (і який сервіс, на вашу думку, працює через дані порти).
20. Написати правила брандмауера Cisco, які відкривають 21 порт і 25 порт (і який сервіс, на вашу думку, працює через дані порти).
21. Технологія NAT. Використання, які питання безпеки вирішуються.
22. Поняття віртуальної локальні мережі. Які питання інформаційної безпеки вона вирішує?
23. Брандмауери та їх використання на прикладі пакетних фільтрів.
24. Концепція Next Generation firewall.

25. Атаки на брандмауери.
26. Проксі сервера, види та задачі.
27. Поняття honeypot (хост-приманка).
28. Поняття sandbox.
29. Віртуальні приватні мережі. Види та задачі, основні протоколи що використовуються. Які загрози виникають при налаштуванні VPN-серверу?
30. Протокол PPTP. Загальні характеристики, які алгоритми авторизації та шифрування використовуються?
31. Протокол L2F. Загальні характеристики, які алгоритми авторизації та шифрування використовуються?
32. Протокол IPSec. Загальні характеристики, принципи роботи, приклади використання.
33. Протокол L2TP. Загальні характеристики, які алгоритми авторизації та шифрування використовуються?
34. Технології віртуалізації. Загальні відомості про захист віртуальних машин.
35. Які кроки треба зробити для підвищення захисту інформації в віртуальних машин 2 типу.
36. Хмарні обчислення. З якими ризиками інформаційно безпеки стикаються користувачі хмарних провайдерів.
37. Протокол SSL. Через яку вразливість його не рекомендовано використовувати?
38. Протокол TLS. Загальні характеристики, які алгоритми авторизації та шифрування використовуються?
39. Служба доменних імен DNS. Принципи роботи, основні загрози. DNSSEC.
40. Служба каталогів на прикладі LDAP. Модель безпеки LDAP.
41. Технічні методи та засоби захисту телефонних ліній.
42. Організаційні міри щодо захисту інформації в телефонних лініях зв'язку.
43. Технологія VoIP. Функціональні можливості. Які основні ризики з'являються з переходом від звичайної до IP-телефонії?
44. Протокол SIP. Як захиститися від підслуховування в IP-телефонії?
45. Загальні принципи передачі інформації по радіоканалу. Які загрози існують при використанні радіоканалу?
46. Як захищають Wi-Fi мережі? Принцип роботи алгоритму WPA-2.
47. Стандарт 802.1X. Принципи роботи.
48. Які кроки можна зробити для підвищення захищеності Wi-fi мережі підприємства?
49. Як захищають мобільні мережі? Коротко порівняти стандарти CDMA та GSM.
50. Захист інформації, що циркулює у супутникових каналах зв'язку.
51. Системи централізованого управління обліковими записами користувачів.
52. Інструменти централізованого моніторінгу мережі.
53. Системи виявлення та запобігання(IDS/IPS) НСД до мережі.
54. Заходи безпеки від DDos атак.
55. DLP-системи.
56. SIEM-системи.
57. Захист електронної пошти. S/MIME.

Криптографічний захист інформації.

1. Що визначає поняття автентифікація. Методи автентифікації.
   Привести алгоритм та схему цифрового підпису на базі криптосистеми RSA. Підписати документ та перевірити підпис, якщо параметри системи: хеш повідомлення m=15, модуль N=55 , відкритий ключ k_1=33, секретний ключ k_2 =17 .
2. Електронний цифровий підпис. Недоліки алгоритму цифрового підпису RSA. Пояснити принцип мультиплікативної атаки. Привести приклад фальсифікації цифрового підпису під документом.
3. Електронний цифровий підпис Зміст цифрового підпису та етапи ЕЦП RSA. Підписати до-

кумент та перевірити підпис, якщо параметри системи: хеш повідомлення m=15, модуль N=49 , відкритий ключ k_1=23, секретний ключ k_2 =11 .

4. Суть методів шифрування: заміни, переставляння та гамування. Пояснити принцип каскадування. За допомогою афінної системи підстановок Цезаря для української абетки перетворити в шифртекст повідомлення, яке складається із перших 4 літер прізвища студента, якщо $E_{a,б}(t) = (at + b) \bmod m$, де m=31, a = 5, b = 4, t – *літера прізвища за номером абетки.*
5. Привести схему секретної системи зв′язку. Які існують класи криптоалгоритмів? Порівняти відомі симетричні криптоалгоритми за параметрами (довжина ключа; кількість етапів шифрування одного блока; кількість ключів; реалізація за мережею Фейстеля; операції, які використовуються для криптографічних перетворень).
6. Привести схему секретної системи зв′язку. Які існують класи криптоалгоритмів? Порівняти відомі криптоалгоритми за класами та призначенням (AES, IDEA, ДСТУ 28147-2009 (ГОСТ 28147-89), Діффі-Хеллмана, RSA, Ель Гамаля, ДСТУ 4145-2002)
7. Привести схему секретної системи зв′язку. Які існують класи криптоалгоритмів? Стандарт шифрування ДСТУ 28147-2009 (ГОСТ 28147-89). Реалізація мережі Фейстеля в алгоритмі ДСТУ 28147-2009 (ГОСТ 28147-89).
8. Стандарт шифрування ДСТУ 28147-2009 (ГОСТ 28147-89). Призначення режимів роботи алгоритму ДСТУ 28147-2009 (ГОСТ 28147-89). Привести схему режиму простої заміни.
9. Принципи керування ключовою системою. Розподілення ключів методом Діффі-Хеллмана. Обчислити спільний сеансовий ключ для абонентів А і В, якщо параметри системи: модуль N=13, g =7 , приватні ключі абонентів А і В відповідно k_a = 5, k_b = 4.
10. Привести схему секретної системи зв′язку. Які існують класи криптоалгоритмів? Алгоритм шифрування на підґрунті криптосистеми RSA. Вимоги щодо вибору ключів в криптосистемі RSA. Зашифрувати повідомлення БАД, якщо параметри системи: P =3 , Q =11 , відкритий ключ k_1=7, секретний ключ k_2 =3 .
11. Привести схему секретної системи зв′язку. Алгоритм шифрування на підґрунті криптосистеми Ель Гамаля. Зашифрувати повідомлення M=6, якщо параметри системи: модуль N=11, g =3, приватні ключі абонентів А і В відповідно k_a =7, k_b =4.
12. Привести схему секретної системи зв′язку для асиметричних криптосистем. Задачі, що розв’язуються асиметричними криптосистемами. Записати рівняння зашифровування та розшифровування в криптосистемах RSA та Ель Гамаля. Переваги криптосистем на еліптичних кривих.
13. Засади керування ключовою системою. Алгоритм розподілення ключів Діффі-Хеллмана. Обчислити спільний сеансовий ключ для абонентів А і В, якщо параметри системи: модуль N=11, g = 2 , приватні ключі абонентів А і В відповідно k_a =5 , k_b = 6.
14. Блочні алгоритми шифрування. Принципи побудови шифрів на базі мережі Фей стеля. Реалізація мережі Фейстеля в криптосистемах DES, IDEA, ДСТУ 28147-2009 (ГОСТ 28147-89).
15. Які питання вивчає стеганографія? Призначення, види стегосистем та різновиди злочинників. Привести загальну схему стегосистеми.
16. Порівняти за призначенням алгоритм Діффі-Хеллмана та алгоритм Ель Гамаля, що побудований на його підґрунті. Привести схему алгоритму шифрування Ель Гамаля. Зашифрувати повідомлення M=5, якщо параметри системи: модуль N = 11, g = 2 , приватні ключі абонентів А і В, відповідно, k_a = 6, k_b = 9.
17. Електронний підпис на базі алгоритму Ель Гамаля. Переваги алгоритму ЕЦП Ель Гамаля перед ЕЦП RSA. Підписати документ та перевірити підпис, якщо параметри системи: хеш повідомлення m =5, модуль N=11, g = 2, x = 9 , секретний ключ k = 8.
18. Електронні гроші. Недоліки схем ЕГ. Оптимальна схема ЕГ. Сформувати електронну банкноту з номером x=33, r=67. У системі ЕГ обрано секретні параметри банку: p=17, q=7, секретний ключ $к_2$=77 та відповідні їм відкриті параметри модуль N=119, $к_1$=5.
19. Як здійснюється захист інформації, що передається телекомунікаційними каналами. Привести загальну схему стегосистеми. Призначення та види стегосистем.
20. Що визначає поняття автентифікація. Методи автентифікації.

Привести алгоритм та схему цифрового підпису на базі криптосистеми RSA. Етапи ЕЦП RSA. Підписати документ та перевірити підпис, якщо параметри системи: хеш повідомлення m=5, модуль N=11 , відкритий ключ k_1=7, секретний ключ k_2 = 3.

21. Принципи керування ключовою системою. Розподілення ключів методом Діффі-Хеллмана. Обчислити спільний сеансовий ключ для абонентів А і В, якщо параметри системи: модуль N=11, g = 2 , приватні ключі абонентів А і В відповідно k_a =5 , k_b =7 .
22. Привести схему секретної системи зв′язку. Які існують класи криптоалгоритмів? Алгоритм шифрування на підґрунті криптосистеми RSA. Вимоги щодо вибору ключів в криптосистемі RSA. Зашифрувати повідомлення БАВ, якщо параметри системи: P =11 , Q = 3, відкритий ключ k_1=7, секретний ключ k_2 =3 .
23. Привести схему алгоритму шифрування на підґрунті криптосистеми Ель Гамаля. Зашифрувати повідомлення M = 5, якщо параметри системи: модуль N = 11, g = 2 , приватні ключі абонентів А і В, відповідно, k_a = 8, k_b = 9.
24. Привести схему секретної системи зв′язку. Які існують класи криптоалгоритмів? Алгоритм шифрування на підґрунті криптосистеми RSA. Вимоги щодо вибору ключів в криптосистемі RSA. Зашифрувати повідомлення ВАБ, якщо параметри системи: P =11 , Q = 3, відкритий ключ k_1=7, секретний ключ k_2 =3 .
25. Привести схему секретної системи зв′язку. Які існують класи криптоалгоритмів? Алгоритм шифрування на підґрунті криптосистеми RSA. Вимоги щодо вибору ключів в криптосистемі RSA. Зашифрувати повідомлення АВБ, якщо параметри системи: P =3 , Q = 11, відкритий ключ k_1=3, секретний ключ k_2 =7 .

Комплексні системи захисту інформації: проектування, впровадження та супровід

1. Основи, напрямки та етапи побудови систем захисту інформації.
2. Технічна модель IT-безпеки стандарту ISO/IEC 15408.
3. Положення про службу захисту інформації в інформаційно-телекомунікаційних системах.
4. Порядок проведення категоріювання інформаційно-телекомунікаційної системи
5. Порядок проведення робіт із створення комплексної системи захисту інформації.
6. Функції служби захисту інформації під час створення комплексної системи захисту інформації.
7. Функції служби захисту інформації під час експлуатації комплексної системи захисту інформації.
8. Структура та зміст Плану захисту інформації в інформаційно-телекомунікаційних системах.
9. Основні етапи створення комплексної системи захисту інформації.
10. Формування загальних вимог до комплексної системи захисту інформації в інформаційно-телекомунікаційних системах.
11. Обґрунтування необхідності створення комплексної системи захисту інформації.
12. Обстеження середовищ функціонування інформаційно-телекомунікаційної системи.
13. Розробка моделі порушника безпеки інформації в інформаційно-телекомунікаційних системах.
14. Модель загроз для інформації в інформаційно-телекомунікаційних системах.
15. Розробка політики безпеки інформації в інформаційно-телекомунікаційних системах.
16. Розробка технічного завдання на створення комплексної системи захисту інформації.
17. Оцінка ефективності й проектування систем захисту.
18. Складання плану захисту та календарного плану робіт із захисту інформації.
19. Системно-концептуальний похід до захисту інформації в автоматизованих системах.
20. Науковий підхід до побудови систем захисту інформації.

ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К.: ЦП «Компринт» О.В., 2021. – 444 с.
2. Йона Л. Г., Онацький О. В., Швець О. В. Системи банківської безпеки: навч. посіб. Одеса: ДУІТЗ, 2022. – 190 с.
3. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія, Харків: Видавництво «Форт», 2010. 608 с.
4. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика: монографія, Харків: Видавництво «Форт», 2012. 880 с.
5. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Л.Я. Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с.
6. Тарнавський Ю. А. Технології захисту інформації / Ю.А. Тарнавський – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
7. Захарченко М.В. Асиметричні методи шифрування в телекомунікація. – Криптографічні методи захисту інформації в телекомунікаційних системах та мережах: модуль 2 з дисципліни „Захист інформації в телекомунікаційних системах та мережах”: навч. посіб. / М.В. Захарченко, О.В. Онацький, Л.Г. Йона, Т.М. Шинкарчук. – Одеса: ОНАЗ ім. О. С. Попова, 2011. – 184 с.
8. Курко М.Н. Криптологія: навч. посібник / М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. – К.: Видавничий дім «Кондор», 2020. — 248 с.

Онацький О.В., Йона Л.Г. Криптографічні системи. Навчальний посібник з дисципліни «Криптографія», «Криптоаналіз» для освітньо-професійної підготовки бакалаврів з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека» 2020. 157с. (ел. видання)

9. Peter Stavroulakis. Handbook of Information and Communication Security /Peter Stavroulakis, Mark Stamp // – Berlin: Springer-Verlag. – 2010. – 863 p.
10. Hankerson D. Guide to Elliptic Curve Cryptography / D. Hankerson, A. Menezes, S. Vanstone. – Springer-Verlag, 2004. – 358 p.
11. Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C / B. Schneier. – Wiley, 2015. – 784 p.
12. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник – К.: «МК-Прес», 2005. – 432 с.
13. Гребенніков В. Комплексні системи захисту інформації: проектування, впровадження, супровід. «Ridero», 2018. – 374 с.
14. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник /А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш.справ, 2020. – 144 с.
15. Створення комплексної системи захисту інформаційних ресурсів унаціональній ґрід-інфраструктурі України / А.Г. Загородній, О.М. Боровська, С.Я. Свістунов, І.П. Сініцин, Є.С. Родін – К.: «Видавництво «Сталь», 2014. – 374 с.
16. Захист інформації в автоматизованих системах управління: навч. посібник/ Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
17. Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч. 2 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 196 с.
18. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – Київ. ООО "Д.В.К.", 2004 . – 508 с.
19. Горохов С.М., Йона Л.Г., Онацький О.В. «Сучасні криптографічні системи». Навчальний посібник. – Одеса.: ОНАС, 2007. – 152 с.
20. Системи передавання даних: навчальний посібник для студентів вищих навчальних закладів, які навчаються за напрямами «Телекомунікації», «Мережі та системи поштового зв’язку», «Радіотехніка» – Т.1. Ефективність блокового кодування, 2014.
21. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України № 125 від 8.11.2005. – (Серія видань “Нормативний документ”).
22. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України № 93 від 16.05.07. – Офіційний вісник України. – 2007. – № 52, ст. 2153. – (Серія видань “Нормативний документ”).

23. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Затверджено наказом Адміністрації ДССЗЗІ України № 65 від 12 березня 2011. – (Серія видань “Нормативний документ”).
24. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
25. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.
26. НД ТЗ 2.6-002-2015 Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99.
27. НД ТЗІ 2.7-013-2016 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99.

23. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Затверджено наказом Адміністрації ДССЗЗІ України № 65 від 12 березня 2011. – (Серія видань "Нормативний документ").
24. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
25. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.
26. НД ТЗ 2.6-002-2015 Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99.
27. НД ТЗІ 2.7-013-2016 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99.

Голова фахової

атестаційної комісії _____ В.В. Корчинський
підпис

Програма розглянута та схвалена
на засіданні приймальної комісії

протокол № 6 від «13» 05 2022 р.

Відповідальний секретар
приймальної комісії _____ Таїсія ГАНЄВА