МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Факультет № 4
Кафедра інформаційних технологій та кібербезпеки

ПРОГРАМА АТЕСТАЦІЇ

ЗДОБУВАЧІВ СТУПЕНЯ «БАКАЛАВР»
ЗА ОСВІТНЬОЮ ПРОГРАМОЮ
125 КІБЕРБЕЗПЕКА (БЕЗПЕКА ІНФОРМАЦІЙНИХ ТА КОМУНІКАЦІЙНИХ СИСТЕМ)

КОМПЛЕКСНИЙ ЕКЗАМЕН

із навчальних дисциплін: «Прикладна криптологія», «Кібербезпека», «Комплексні системи захисту інформації: проектування, впровадження, супровід»

Харків
2021

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 22.04.2021 № 4

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 21.04.2021 № 4

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 21.04.2021 № 4

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки факультету № 4 (протокол від 16.04.2021 № 8).

Розробники:

професор кафедри інформаційних технологій та кібербезпеки факультету № 4, к.т.н., доцент Носов В.В.
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4, к.ю.н., доцент Манжай О.В.
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4, к.т.н., доцент Соляник Т.М.

Рецензенти:

завідувач кафедри інформаційних управляючих систем факультету комп'ютерних наук Харківського національного університету радіоелектроніки, д.т.н., професор Петров К.Е.

доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент Тулупов В.В.

1. Загальні методичні рекомендації

Комплексний екзамен у здобувачів вищої освіти, які навчаються за спеціальністю 125 «Кібербезпека» (Безпека інформаційних та комунікаційних систем) є частиною їх атестації та проводиться з метою перевірки науково-теоретичної та практичної підготовки випускників. Екзамен проводиться за білетами, складеними у відповідності до навчальних програм з дисциплін «Прикладна криптологія», «Кібербезпека», «Комплексні системи захисту інформації: проектування, впровадження, супровід».

Екзаменаційний білет містить два теоретичних та одне практичне запитання.

Метою комплексного екзамену є оцінка готовності здобувачів вищої освіти використовувати і впроваджувати технології безпеки інформаційних та комунікаційних систем.

Для успішного складання комплексного екзамену здобувач вищої освіти повинен

знати:

- концепції шифрування з секретним ключем;
- методи автентифікації повідомлень;
- концепції шифрування з публічним ключем;
- схеми цифрових підписів;
- реалізації криптографічних протоколів;
- концепції забезпечення кібербезпеки;
- актуальні кібератаки на інформаційні і комунікаційні системи;
- методи та засоби захисту від кібератак
- принципи створення, організацію та порядок проведення робіт з проектування, впровадження та супроводу комплексних системи захисту інформації (КСЗІ) в інформаційних, комунікаційних та інформаційно-телекомунікаційних системах (ІТС).

вміти:

- обґрунтовувати параметри безпеки та ефективно впроваджувати криптосистеми з приватним та публічним ключом;
- дотримуватися умов безпеки криптосистем;
- здійснювати аналіз криптографічних протоколів;
- проводити тестові атаки на ключову інформацію реалізованих криптографічних алгоритмів;
- аналізувати кіберзагрози та використовувати сервіси безпеки інформаційних і комунікаційних систем;
- тестувати на вразливість до кібератак комп'ютерні системи;
- здійснювати заходи щодо проектування, впровадження та супроводу КСЗІ в ІТС.

Критерії оцінювання знань

Результати складання комплексного екзамену визначаються оцінками «відмінно», «добре», «задовільно» і «незадовільно». Оцінка рівня знань здобувача вищої освіти за складання комплексного екзамену виставляється у наступному порядку.

Оцінка «відмінно» – кали здобувач вищої освіти глибоко та твердо засвоїв весь програмний матеріал, повністю, послідовно, грамотно і логічно його викладає, тісно пов'язує теорію з практикою, завданнями та діяльністю у сфері забезпечення кібербезпеки; може відповісти на будь-яке запитання при зміні його форми, вільно справляється з завданнями, показує знання монографічного матеріалу, правильно обґрунтовує прийняті рішення, виявляє уміння самостійно узагальнювати та викладати матеріал, не допускаючи помилок.

Оцінка «добре» – коли здобувач вищої освіти твердо знає програмний матеріал, грамотно і по суті викладає його, не допускає суттєвих помилок у відповіді на питання, може правильно використати теоретичні положення і володіє необхідними навичками при виконанні практичних завдань.

Оцінка «задовільно» – коли здобувач вищої освіти засвоїв тільки основний матеріал, але не знає окремих деталей, допускає неточні відповіді, недостатньо чіткі формулювання,

порушує послідовність у викладанні програмного матеріалу та має певні труднощі при виконанні практичних завдань.

Оцінка «незадовільно» – коли здобувач вищої освіти не знає значної частини програмного матеріалу, допускає суттєві помилки, має значні труднощі при виконанні практичних завдань.

Оцінка виводиться залежно від окремих оцінок за відповіді на теоретичні і практичні питання. Зокрема при трьох оцінках виводиться:

«відмінно» – коли серед оцінок не більше однієї оцінки «добре», а решта «відмінно»;

«добре» – коли серед оцінок не більше однієї оцінки «задовільно»;

«задовільно» – коли серед оцінок не більше однієї оцінки «незадовільно».

Рішення про виставлення оцінки приймається простою більшістю голосів членів комісії шляхом голосування при закритому засіданні. При однаковій кількості голосів голос голови є вирішальним. Рішення оголошується у цей же день після оформлення протоколу засідання державної комісії.

Комплексна оцінка складається з перевірки теоретичних знань та практичних вмінь за трьома питаннями екзаменаційного білету. Кожне питання білету належить до різних дисциплін комплексного екзамену.

Оцінка за відповіді на питання з білету	**Оцінка з екзамену в протоколі ЕК**	**Оцінка в балах**	**Оцінка за шкалою ЄКТС**	**Критерії оцінювання здобувачів вищої освіти**	**Характеристика повноти відповіді в протоколі ЕК**
5/5/5	**Відмінно**	100	A	Глибоко та в повному обсязі засвоєний програмний матеріал, повністю, системно та послідовно, грамотно і логічно висвітлений матеріал, тісно пов'язана теорія з практикою. Відсутнє вагання з відповіддю, володіння навичками виконання аналітичних робіт; знання монографічного матеріалу; правильне обґрунтування, аргументація власних висновків; вміння самостійно узагальнювати та викладати матеріал, не допускаючи помилок	Повна виважена відповідь
5/5/4		90	A		Стисла та змістовна відповідь
4/4/5	**Добре**	85	B	Тверді знання програмного матеріалу, грамотно та по суті викладає його, не допускається істотних неточностей у відповіді на запитання; вміння правильно пов'язати теоретичні положення з практикою та володіння навичками при виконанні завдань. Відповіді на значну частину додаткових запитань.	Відповідь охоплює основний матеріал, але є неточності
4/4/4 3/4/5		80	B		Майже повна, має незначні неточності
4/4/3		75	C		Майже повна, має значні неточності

3/3/4	**Задовільно**	70	D	Засвоєння основного програмного матеріалу, допущення під час відповіді неточностей та недостатньо правильних формулювань понять дисципліни; допущення істотних помилок при відповіді на додаткові запитання. Вагання при виконанні завдань.	Відповідь має істотні неточності
3/3/3		60	E		Питання білету розкриті неповно
Одна або більше «2»	**Незадовільно**	35-59	FX	Не володіє основним програмним матеріалом, допущення суттєвих помилок при відповіді, виконання завдань з великими труднощами, неправильні відповіді на більшість додаткових запитань.	Правильна відповідь відсутня, не орієнтується в питаннях

2. Короткий опис змісту програми

Розділ 1: "Прикладна криптологія"

Тема № 1. Криптосистеми з секретним ключем

Концепції шифрування з секретним ключем. Принципи сучасної криптографії. Теоретичні основи досконалої секретності. Одноразовий блокнот (шифр Вернама). Обчислювальна секретність. Псевдовипадкові послідовності. Доказовість безпечності криптографії. Поняття дуже сильної безпеки та псевдовипадкові функції блокових шифрів. CPA-безпечні криптографічні перетворення. Chosen-Ciphertext і Padding-Oracle атаки. Коди автентифікації повідомлення. Хеш-функції та шифрування з автентифікацією.

Тема № 2. Криптосистеми з публічним ключем

Обчислення модулярної арифметики та алгебраїчні групи. Важкі теоретико-числові проблеми. Концепції шифрування з публічним ключем. Розподіл ключів та шифрування з публічним ключем. Алгоритми шифрування з публічним ключем. Алгоритми цифрових підписів. Схеми ідентифікації та інфраструктура відкритих ключів.

Тема № 3. Криптографічні протоколи

Основні відомості про криптопротоколи: розподілу ключів, автентифікації сторін, доказу з нульовим знанням, сліпих підписів.

Розділ 2: "Кібербезпека"

Тема № 1. Основні відомості про кібербезпеку

Терміни та визначення. Умови безпеки інформації. Поняття кіберпростору. Базова технічна модель безпеки інформаційних технологій. Зменшення інформаційних ризиків. Загальна структура інформаційно-телекомунікаційних систем (ІТС). Архітектура безпеки ІТС. Застосування сервісів безпеки до рівнів безпеки ІТС. Типи атак на інформаційні системи. Принципи захисту від атак.

Тема № 2. Пасивний збір інформації

Отримання інформації про організацію, її мережу, вузли та сервіси з відкритих джерел. Побудова та аналіз зв'язків між частинами отриманої інформації. Способи протидії пасивному збору інформації.

Тема № 3. Активний збір інформації про мережу

Основні протоколи стеку TCP/IP. Побудова схеми мережі. Засоби для отримання інформації щодо вузлів та сервісів у мережі. Пошук вразливостей та інструменти сканування вузлів мережі на вразливості. Отримання інформації з сервісів: NetBIOS, LDAP, SMTP, DNS.

Тема № 4. Механізми захисту мережі від збору інформації, сканування та проникнення

Системи виявлення вторгнень та системи запобігання вторгненням; мережні екрани; мережні пастки; обхід механізмів захисту: тунелювання.

Налаштування системи виявлення вторгнень Snort; використання стандартних правил та створення своїх правил для виявлення підозрілого трафіку. Налаштування мережного екрану; застосування технік обходу мережних екранів; встановлення та використання Honeypot.

Тема № 5. Аналіз трафіку в комп'ютерних мережах

Механізми перехоплення трафіку в комп'ютерних мережах; використання програм для перехоплення та аналізу трафіку; атаки в локальній мережі та захист від них: протоколи ARP та DHCP, переповнення таблиці комутації, ARP підміна, підміна DHCP; атака отруєння DNS та захист від неї.

Використання програм для перехоплення та аналізу трафіку; засоби для MAC затоплення, ARP підміни; засоби для атаки на DHCP; створення підробленого DHCP серверу.

Тема № 6.Безпека в безпровідних мережах

Збір інформації про безпровідні мережі. Шифрування та автентифікація в безпровідних мережах. Атака на безпровідні мережі. Засоби захисту від безпровідних атак.

Тема № 7.Безпека в операційних системах

Організація контролю доступу в ОС**.** Руткіти та шпигунські програми**.** Інструменти, що використовуються для здійснення атак на операційні системи. Атака на парольний захист. Протидія атакам на операційні системи.

Огляд пакету програм Metasploit; використання Metasploit для зламування віддаленого вузла з ОС Windows; оболонка Meterpreter, основні команди (робота з файлами, налаштуваннями мережі, створення дампу файлу з паролями, отримання списку процесів, отримання знімку екрану, керування веб-камерою, приховування слідів); атака на парольний захист: ПЗ для підбору паролів, типи атак.

Тема № 8. Шкідливе програмне забезпечення

Типи шкідливого ПЗ. Принципи створення та аналізу троянських програм. Принципи створення та аналізу вірусів. Протидія і виявлення троянських програм, черв'яків та вірусів. Шкідливе ПЗ для мобільних пристроїв з ОС: iOS, Android, Windows Phone, BlackBerry.

Створення троянських програм (шкідливий код в окремому файлі, троянська програма з декількох файлів, вкладення шкідливого коду в існуючу корисну програму); троянська програма у документі MS Word; протидія і виявлення троянських програм, черв'яків та вірусів. Використання Metasploit для створення шкідливого коду для ОС Android.

Тема № 9. Безпека веб-серверів та веб-застосувань

Вразливості веб-серверів та веб-застосувань. Види атак на веб-сервер. Види атак на веб-застосування. Механізми захисту веб-серверів та веб-застосувань. ПЗ для сканування веб-серверів та веб-застосувань на вразливості.

Тема №10. SQL-ін'єкції

Короткий огляд мови SQL. Інструменти для підключення до SQL-сервера та роботи з SQL. Типи SQL-ін'єкцій. Способи виконання SQL-ін'єкцій. Причини виникнення вразливостей, пов'язаних з SQL-ін'єкціями. Захист від SQL-ін'єкцій. Інструменти для автоматичного пошуку вразливостей, пов'язаних з SQL-ін'єкціями.

Розділ 3: "Комплексні системи захисту інформації: проектування, впровадження, супровід"

Тема № 1. Загальні питання організації та функціонування систем технічного захисту інформації.

Захист інформації: основні терміни та визначення. Класифікація інформації. Властивості інформації. Захист інформації в інформаційно-комунікаційних системах. Вимоги до захисту інформації.

Тема № 2. Нормативно-правова база України у сфері технічного захисту інформації.

Нормативні документи системи технічного захисту інформації. Поняття державного регулювання. Основні складові державного регулювання технічного захисту інформації.

Тема № 3. Комп'ютерні системи захисту інформації як об'єкт дослідження.

Об'єкт критичної інформаційної інфраструктури. Загальні положення інформаційних систем. Склад, структура та основні вимоги до комп'ютерних систем захисту інформації. Комплекси технічного захисту інформації. Комплекс засобів захисту інформації в інформаційно-телекомунікаційних системах.

Тема № 4. Побудова комплексних систем захисту інформації.

Основні етапи створення комплексних систем захисту інформації. Передпроектні роботи зі створення КСЗІ. Обстеження середовищ функціонування ІТС. Аналіз ризиків та джерел загроз інформаційної безпеки. Оцінка захищеності інформації в інформаційно-комунікаційних системах. Модель загроз та модель порушника в ІТС.

Тема № 5. Процес створення комплексних систем захисту інформації.

Розробка Політики безпеки інформації в ІТС. Нормативно-методичні матеріали з організації захисту інформації. Розробка технічного завдання (ТЗ) на створення КСЗІ. Склад і отримання розділів ТЗ. Вимоги до засобів захисту інформації від несанкціонованого доступу та витоку інформації технічними каналами. Функціональні профілі захищеності. Вимоги до проектної та експлуатаційної документації.

Тема № 6. Розробка проекту комплексних систем захисту інформації.

Стадії проектування. Ескізний проект, Технічний проект, Робоча документація. Нормативні документи та стандарти, що регламентують проектування КСЗІ в ІТС. Склад документів, що розробляються при проектуванні КСЗІ. Види документів на програмні засоби, що використовуються при створенні КСЗІ. Робоча та експлуатаційна документація КСЗІ. Управління проектами. Система розроблення та поставлення продукції на виробництво.

Тема № 7. Введення комплексних систем захисту інформації в дію та оцінка захищеності інформації в ІТС.

Роботи з підготовки організаційної структури (Служба захисту інформації) та розробка розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС. Комплектування КСЗІ. Будівельно-монтажні та пусконалагоджувальні роботи. Випробування та атестація комплексу технічного захисту інформації. Програми та методики випробувань

Тема № 8. Експертиза комплексних систем захисту інформації.

Суб'єкти та об'єкти експертизи. Порядок організації та проведення експертизи. Програма та методика проведення експертизи. Приймальні випробування ІТС при функціонуючій в її складі КСЗІ.

Тема № 9. Впровадження та супровід КСЗІ.

Роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації (відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ). Гарантійне і післягарантійне технічне обслуговуванню засобів захисту інформації.

3. Контрольні питання та завдання до атестації

3.1. Теоретичні питання

Розділ «Прикладна криптологія»

1. Концепції шифрування з секретним ключем.
2. Принципи сучасної криптографії.
3. Теоретичне обґрунтування досконалої секретності.
4. Одноразовий блокнот (шифр Вернама).
5. Обчислювальна секретність.
6. Формування псевдовипадкових послідовностей.
7. Доказовість безпечності криптографії.
8. Поняття дуже сильної безпеки криптосистем з секретним ключом.
9. Псевдовипадкові функції блокових шифрів.
10. CPA-безпечні криптографічні перетворення.
11. Chosen-Ciphertext атаки на шифртекст.
12. Padding-Oracle атаки на шифртекст.
13. Коди автентифікації повідомлення.
14. Геш функції.
15. Шифрування з автентифікацією.
16. Основні обчислення модулярної арифметики
17. Поняття і властивості алгебраїчних груп.
18. Важкі теоретико-числові проблеми.
19. Концепції шифрування з публічним ключем.
20. Розподіл ключів та шифрування з публічним ключем.
21. Алгоритми шифрування з публічним ключем.
22. Алгоритми цифрових підписів.
23. Схеми ідентифікації.
24. Інфраструктура відкритих ключів.
25. Поняття криптопротоколів.
26. Криптопротоколи розподілу ключів.
27. Криптопротоколи автентифікації сторін.

Розділ «Кібербезпека»

28. Терміни та визначення в області забезпечення кібербезпеки.
29. Об'єкт захисту при забезпеченні кібербезпеки.
30. Принципи безпеки.
31. Загрози кібербезпеки і вектори атаки.
32. Типи кібератак.
33. Базова технічна модель IT-безпеки.
34. Архітектура безпеки ITC.
35. Механізми забезпечення кібербезпеки.
36. Отримання інформації про організацію, її мережу, вузли та сервіси з відкритих джерел.
37. Способи протидії пасивному збору інформації про об’єкт кібератаки.
38. Основні протоколи стеку TCP/IP.
39. Засоби для отримання інформації щодо вузлів та сервісів у комп’ютерній мережі.
40. Пошук вразливостей та інструменти сканування вузлів комп’ютерної мережі на вразливості.
41. Системи виявлення вторгнень та системи запобігання вторгненням.
42. Мережні екрани.
43. Мережні пастки.
44. Збір інформації про безпровідні мережі.
45. Шифрування та автентифікація в безпровідних мережах.
46. Атака на безпровідні мережі.
47. Засоби захисту від безпровідних атак.

48. Організація контролю доступу в ОС.
49. Атаки на парольний захист ОС.
50. Протидія атакам на операційні системи.
51. Типи шкідливих програм.
52. Принципи створення та аналізу троянських програм.
53. Протидія і виявлення шкідливих програм.
54. Вразливості веб-серверів та веб-застосувань.
55. Види атак на веб-сервер.
56. Види атак на веб-застосування.
57. Типи та способи виконання SQL-ін'єкцій.
58. Захист від SQL-ін'єкцій.

Розділ «Комплексні системи захисту інформації: проектування, впровадження, супровід»

59. Поняття державного регулювання. Нормативні документи системи технічного захисту інформації.
60. Поняття державного регулювання. Основні складові державного регулювання технічного захисту інформації.
61. Об'єкт критичної інформаційної інфраструктури.
62. Основні задачі політики інформаційної безпеки об'єктів критичної інформаційної інфраструктури.
63. Загальні вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури.
64. Основні вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури: організаційні та технічні заходи.
65. Базові вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури: загальна політика інформаційної безпеки.
66. Базові вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури: управління доступом користувачів та адміністраторів до об'єктів.
67. Базові вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури: ідентифікація та автентифікація користувачів та адміністраторів об'єкта.
68. Базові вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури: реєстрація подій компонентами об'єкта та їх періодичний аудит.
69. Базові вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури: забезпечення мережного захисту компонентів та інформаційних ресурсів об'єкта.
70. Базові вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури: забезпечення мережного захисту компонентів та інформаційних ресурсів об'єкта.
71. Базові вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури: забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об'єкта.
72. Базові вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури: визначення умов використання програмного та апаратного забезпечення об'єкта.
73. Базові вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури: визначення умов розміщення компонентів об'єкта.
74. Загальні положення технічного захисту інформації.
75. Основні етапи технічного захисту інформації.
76. Основні етапи створення комплексних систем захисту інформації. Визначення й аналіз загроз.
77. Основні етапи створення комплексних систем захисту інформації. Окрема модель загроз.
78. Розробка технічного завдання на створення комплексних систем захисту інформації.
79. Розробка технічного завдання на створення комплексних систем захисту інформації. Реалізація організаційних заходів захисту.

80. Розробка технічного завдання на створення комплексних систем захисту інформації. Реалізація первинних технічних засобів захисту.
81. Розробка технічного завдання на створення комплексних систем захисту інформації. Реалізація основних технічних засобів захисту.
82. Розробка технічного завдання на створення комплексних систем захисту інформації. Приймання, визначення повноти та якості робіт.
83. Вимоги до засобів захисту інформації від несанкціонованого доступу та витоку інформації технічними каналами.

3.2. Практичні завдання

1. У фреймворку OpenSSL продемонструвати вразливість шифрування криптосистеми DES в режимі роботи ECB.
2. У фреймворку OpenSSL продемонструвати вирівнювання (padding) відкритого тексту перед шифруванням.
3. В ОС Kali Linux продемонструвати існування колізії алгоритму гешування MD5 для файлів hello і erase.
4. В ОС Kali Linux згенерувати словник із номерів мобільних телефонів України з кодом оператора 050.

на базі English Dictionary

5. В ОС Kali Linux згенерувати похідний словник, в якому: друга літера слова змінює регістр; повсюди йде заміна: e -> 3; i -> 1; o -> 0; наприкінці слів додаються цифри від 1 до 5.
6. В ОС Kali Linux спираючись на інформацію про користувача (ім'я, прізвище, дата народження) згенерувати словник можливих паролів.
7. Здійснити криптоаналіз зашифрованого файлу `file1.docx` методом перебору варіантів зі словника `passwd-u.txt`.
8. Здійснити криптоаналіз зашифрованого файлу `file2.docx`, якщо відомо, що пароль складається із двох маленьких літер і двох цифр наприкінці.
9. Здійснити криптоаналіз зашифрованого файлу `file1.pdf`, якщо відомо, що пароль складається із маленьких літер, точна довжина невідома але не більше 7 символів.
10. Здійснити криптоаналіз зашифрованого архіву `arc1.7z`, якщо відомо, що паролем є рядок в зворотному порядку зі словника `example.dict`.
11. Здійснити криптоаналіз зашифрованого архіву `arc2.7z`, якщо відомо, що паролем є рядок зі словника `example.dict`, в якому скорочена довжина до 8 символів та зроблені заміни "o" на "0", "i" на "1".
12. Здійснити криптоаналіз зашифрованого архіву `myzip.zip`, якщо відомо, що паролем є номер мобільного телефону України з кодом 050.
13. Аліса для криптосистеми RSA вибрала параметри $p = 17$, $q = 11$, $e = 7$. Обчислите параметри ключів Аліси: N, φ, d. Покажіть як Боб може послати зашифроване повідомлення "88" Алісі, якщо йому стане відомий її публічний ключ.
14. Обчислите закритий ключ d криптосистеми RSA з параметрами $p=47$, $q=83$, $e=163$. Зашифруйте за допомогою отриманої системи повідомлення "123". Здійсніть перевірку шляхом розшифрування повідомлення.
15. В програмі Cryp Tool в розділі RSA Demonstration здійснити генерацію ключів, зашифрувати на англійській мові своє ім'я та прізвище, продемонструвати дешифрування.
16. У фреймворку OpenSSL здійснити генерацію RSA ключів, продемонструвати текстове представлення публічного та приватного ключів, пояснити параметри приватного ключа.
17. За допомогою програми Cryp Tool здійснити криптоаналіз шифртексту

`6340 8309 14010 8936 27358 25023 16481 25809 23614 7135 24996 30590 27570 26486 30388 9395 27584 14999 4517 12146 29421 26439 1606 17881 25774 7647 23901 7372 25774 18436 12056 13547 7908 8635 2149 1908 22076 7372 8686 1304 4082 11803 5314 107 7359 22470 7372 22827 15698 30317 4685 14696 30388 8671 29956 15705 1417 26905 25809 28347 26277 7897 20240 21519 12437 1108 27106 18743 24144 10685 25234 30155 23005 8267 9917 7994 9694 2149 10042 27705 15930 29748 8635 23645 11738 24591 20240 27212 27486 9741 2149 29329 2149 5501 14015 30155 18154 22319 27705 20321 23254 13624 3249 5443 2149 16975 16087 14600 27705 19386 7325 26277 19554 23614 7553 4734 8091 23973 14015 107 3183 17347 25234 4595 21498 6360 19837 8463 6000 31280 29413 2066 369 23204 8425 7792 25973 4477 30989`, який був отриманий при використанні RSA алгоритму і публічного ключа с параметрами $N = 31313$, $e = 4913$.

18. За допомогою програми Cryp Tool здійснити криптоаналіз шифртексту
    45411667895024938209259253423,
    16597091621432020076311552201,
    46468979279750354732637631044,
    32870167545903741339819671379, який був отриманий при використанні RSA алгоритму і публічного ключа с параметрами *N = 639784868795271438588314150 41*, *e = 17579*.
19. В програмі Cryp Tool продемонструвати електронний підпис документу за алгоритмом еліптичних кривих prime239v1.
20. Продемонструвати за допомогою програми gpg4usb підпис та шифрування повідомлень.
21. В ОС Kali Linux встановити та перевірити роботу утиліти Kalitorify. Через 2ip.ua пройти тест на приватність, а через dnsleaktest.com - на виток інформації через DNS.
22. За наданим доменним ім'ям ресурсу, який використовує послуги Cloudflare, встановити його справжню IP адресу.
23. За наданим доменним ім'ям ресурсу і програми Web data extractor здійснити збір даних із сайту.
24. За наданим доменним ім'ям ресурсу зібрати DNS інформацію про ресурс із використанням robtex.com.
25. За наданим доменним ім'ям ресурсу знайти перелік сайтів, які розміщуються на тому ж самому сервері, що й цільовий.
26. За наданим доменним ім'ям ресурсу знайти перелік субдоменів цільового домену.
27. Здійснити пошук та аналіз каталогів і файлів для вебсайту на віртуальній машині metasploitable2.
28. За наданим доменним ім'ям ресурсу за допомогою metagoofil знайти і завантажити для аналізу метаданих доступні файли.
29. З визначеного ресурсу за допомогою Theharvester і Infoga зібрати доступні записи електронної пошти, імен користувачів, вузлів та субдоменів.
30. Визначити доступні мережні сервіси (відкриті порти) для scanme.nmap.org.
31. Визначити наявні вразливості віртуальної машини metasploitable2.
32. Продемонструвати налаштування iptables (міжмережного екрану) в ОС Kali Linux.
33. Продемонструвати створення та застосування бекдору для ОС Windows 10.
34. Продемонструвати експлуатацію вразливості вебзастосунку для віртуальної машини Five86:1 (Vulnhub).

4. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна література

1. Дистанційний курс University of Maryland by Jonathan Katz "Криптографія". https://www.coursera.org/course/cryptography.
2. Захарченко М.В., Йона Л.Г., Щербина Ю.В., Онацький О.В. Розвинення криптології та її місце в сучасному суспільстві : Навч. посібник. – Одеса: ОНАЗ ім. О. С. Попова, 2003. – 80 с.
3. Богуш В.М., Мухачов В.А. Криптографічні застосування елементарної теорії чисел. Навчальний посібник. К.: ДУІКТ, 2006. 126 с.
4. Носов В.В. Прикладна криптологія // Курс дистанційного навчання. URL: https://student.univd.edu.ua (дата звернення: 13.04.2020).
5. Носов В.В. Кібербезпека // Курс дистанційного навчання. URL: https://student.univd.edu.ua (дата звернення: 13.04.2020).
6. Schneier, Bruce. Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition edition // Bruce Schneier. – 2017. – 784 p.
7. Matt Walker. CEH Certified Ethical Hacker All-in-One Exam Guide. McGraw-Hill, 2012.
8. ITU-T Rec. X.805. Security architecture for systems providing end-to-end communications. / ITU-T Recommendation X.805, 10/2003. URL: https://www.itu.int/rec/T-REC-X.805-200310-I/en (дата звернення: 20.09.2016).
9. Носов В.В., Манжай О.В. Організація та забезпечення інформаційної безпеки: Навч. посібник. – Харків: Вид-во Харк. нац. ун-ту внутр. справ, 2007.
10. Замула О.А., Горбенко Ю.І., Шумов А.І. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації»: Навч. посібник. - Харків: ХНУРЕ, 2010 - 16 с.
11. Про основні засади забезпечення кібербезпеки України: Закон України від 03.07.2020, № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 01.09.2020).
12. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. – Чинний з 1997-01-01. – К.: Держспоживстандарт України, 1997. – 11 с.
13. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. –Чинний з 1997-01-01. – К.: Держспоживстандарт України, 1997. – 11 с.
14. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Терміни та визначення. –Чинний з 1998-01-01. – К.: Держспоживстандарт України, 1997. – 11 с.
15. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: https://tzi.ua/assets/files/3.7-003-2005.pdf (дата звернення: 01.09.2020).
16. НД ТЗІ 1.1-005-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення». URL: https://tzi.com.ua/downloads/1.1-005-07.pdf (дата звернення: 01.09.2020).
17. НД ТЗІ 3.1-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи». URL: https://tzi.ua/assets/files/3.1-001-07.pdf (дата звернення: 01.09.2020).
18. НД ТЗІ 3.3-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації». URL: https://tzi.ua/assets/files/3.3-001-07.pdf (дата звернення: 01.09.2020).
19. НД ТЗІ 2.1-002-07 «Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення». URL: https://tzi.com.ua/downloads/2.1-002-07.pdf (дата звернення: 01.09.2020).
20. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22. URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-

004-99.pdf (дата звернення: 01.09.2020).
21. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22. URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-005--99.pdf (дата звернення: 01.09.2020).
22. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 20.12.2000 № 60. URL: http://tzi.com.ua/downloads/3.6-001-2000.pdf (дата звернення: 01.09.2020).
23. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22. URL: http://tzi.com.ua/downloads/3.7-001-99.pdf (дата звернення: 01.09.2020).
24. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22. URL: https://tzi.ua/assets/files/%D0%9D%D0%94%20%D0%A2%D0%97%D0%98%201.1-002-99.pdf (дата звернення: 01.09.2020).
25. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22. URL: https://tzi.ua/assets/files/1.1_003_99.pdf (дата звернення: 01.09.2020).
26. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf (дата звернення: 01.09.2020).
27. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТСЗІ СБ України від 09.02.2001 № 2. URL: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-2.1-001-2001.pdf (дата звернення: 01.09.2020).

Допоміжна

28. Henk C.A. van Tilborg, FUNDAMENTALS OF CRYPTOLOGY. A Professional Reference and Interactive Tutorial. Eindhoven University of Technology. The Netherlands. KLUWER ACADEMIC PUBLISHERS, Boston/Dordrecht/London.
29. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих.
30. Aaron Philipp, David Cowen, Chris Davis. Hacking exposed computer forensics. Second edition. The McGraw-Hill Companies, 2010.
31. ITU-T E.408. Telecommunication networks security requirements. / ITU-T Recommendation E.408, 05/2004. URL: https://www.itu.int/rec/T-REC-E.408-200405-I/en(дата звернення: 20.09.2016).
32. ITU-T Rec. X.800. Security architecture for Open Systems Interconnection for CCITT applications. / Recommendation X.800, Geneva, 1991. URL: http://www.itu.int/rec/T-REC-X.800-199103-I (дата звернення: 20.09.2016).
33. NIST Special Publication 800-33. Underlying Technical Models for Information Technology Security. / Gary Stoneburner. CODEN: NSPUE2, December 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf (дата звернення: 20.09.2016).
34. Петренко С.А., Петренко А.А. Аудит інформаційної безпеки Internet. – М. ДМК Пресс, 2002-416 с.

Інформаційні ресурси в Інтернеті

35. https://www.coursera.org/course/cryptography
36. https://www.coursera.org/course/crypto
37. https://www.coursera.org/course/crypto2

38. https://www.cryptool.org/en/
39. https://securityonline.info/category/forensics.
40. https://resources.infosecinstitute.com/category/forensics-2.
41. http://www.dfrws.org.
42. https://www.forensicmethods.com.
43. http://www.hackerhighschool.org.
44. https://securityonline.info.
45. https://gbhackers.com.
46. https://securityonline.info.
47. https://www.hackingarticles.in.