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 (ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ)

КОМПЛЕКСНИЙ ЕКЗАМЕН

із навчальних дисциплін: «Поліцейська діяльність у кіберсфері», «Кібербезпека», «Цифрова криміналістика»

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.

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 зі спеціалізації у здобувачів вищої освіти, які навчаються за спеціальністю 125 «Кібербезпека», спеціалізацією «протидія кіберзлочинності», є частиною їх атестації та проводиться з метою перевірки науково-теоретичної та практичної підготовки випускників. Екзамен проводиться за білетами, складеними у повній відповідності до навчальних програм з дисциплін «Кібербезпека», «Поліцейська діяльність у кіберсфері», «Цифрова криміналістика».

Екзаменаційний білет містить два теоретичних та одне практичне запитання.

Запорукою успішного складання екзамену є успішне засвоєння здобувачем вищої освіти зазначених навчальних дисциплін в обсязі, встановленому робочими навчальними програмами. Зокрема, в результаті вивчення навчальних дисциплін, що виносяться на комплексний екзамен кожен здобувач вищої освіти повинен:

Знати:

- визначення, ознаки та класифікацію кіберзлочинів;
- нормативно-правову базу протидії кіберзллочинності;
- організаційну структуру протидії кіберзлочинності правоохоронним органами в Україні та за її межами;
- особливості організації і тактики оперативного маскування під час роботи в інформаційно-телекомунікаційних системах;
- моделі поліцейської розвідки;
- технічні особливості огляду засобів комп'ютерної техніки, виявлених на місці події;
- методи встановлення IP-адреси;
- різні види кібератак на інформаційні і комунікаційні системи та способи захисту від них;
- поняття електронних (цифрових) доказів;
- процедури первинних цифрових криміналістичних досліджень різноманітних цифрових пристроїв, операційних систем та застосувань;
- методи та засоби здобуття даних;
- методи та засоби протидії криміналістичним дослідженням.

Уміти:

- застосовувати норми законодавства у протидії кіберзлочинності;
- використовувати зарубіжний досвід у протидії кіберзлочинності;
- застосовувати прийоми оперативного маскування у кіберсфері;
- здійснювати віддалений збір інформації про вузли комп'ютерної мережі;
- шукати інформацію про об'єкти в мережі;
- аналізувати профілі соціальних мереж та поштові повідомлення;
- встановлювати інформацію про фінансові інструменти;
- аналізувати можливі кіберзагрози, впроваджувати та управляти сервісами безпеки інформаційних і комунікаційних систем;

- тестувати на вразливість до кібератак комп’ютерні системи;
- проводити криміналістичні дослідження операційних систем, комп'ютерних мереж, веб-атак, баз даних, хмарних сервісів, шкідливого програмного забезпечення, електронної пошти, мобільних пристроїв.

Набуті здобувачами вищої освіти на заняттях знання та уміння є необхідною основою для практичної діяльності з попередження та розслідування кримінальних правопорушень, в процесі якої із накопиченням досвіду знання будуть поглиблюватися, а уміння розів’ються до рівня навичок.

Критерії оцінювання якості підготовки випускників

Результати складання комплексного екзамену визначаються оцінками «відмінно», «добре», «задовільно» і «незадовільно». Оцінка рівня знань курсанта (слухача) за відповідь на державному екзамені виставляється у наступному порядку:

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

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.

2. КОРОТКИЙ ОПИС ЗМІСТУ ПРОГРАМИ

РОЗДІЛ І. ТЕХНІКА ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ У КІБЕРСФЕРІ

ТЕМА № 1. ЗАСАДНИЧІ ПРИНЦИПИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Поняття кіберпростору та кіберзлочинів. Об'єкти та суб'єкти протидії кіберзлочинності. Організаційно-правові засади протидії кіберзлочинності. Міжнародний досвід протидії кіберзлочинності.

ТЕМА № 2. ОПЕРАТИВНЕ МАСКУВАННЯ У КІБЕРСФЕРІ

Поняття, суб'єкти та підстави застосування оперативного маскування. Забезпечення анонімності під час роботи в інформаційно-телекомунікаційних системах. Термінологічні особливості спілкування у кіберпросторі. Легендування профілів користувача для використання у кіберсфері.

ТЕМА № 3. ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ПІД ЧАС ПОПЕРЕДЖЕННЯ ТА РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ.

Комп'ютерні мережі та веб-технології. Засоби комунікації та мережні засоби зберігання інформації. Фінансові комп'ютерні технології. Технічні особливості огляду засобів комп'ютерної техніки, виявлених на місці події.

ТЕМА № 4. ОПЕРАТИВНО-ТЕХНІЧНІ ЗАСОБИ

Основні положення щодо оперативно-технічних засобів. Технічні канали витоку інформації. Сигналізація та методи її нейтралізації. Класифікація та методи подолання запірних пристроїв.

РОЗДІЛ ІІ. 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 Android.

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.

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 ІІІ. ЦИФРОВА КРИМІНАЛІСТИКА

ТЕМА № 1. ЕЛЕКТРОННІ (ЦИФРОВІ) ДОКАЗИ

Цифрові дані як докази: визначення, роль, типи, характеристика, законодавчі вимоги. Характеристика криміналістичних досліджень. Типи кіберзлочинів, проблеми розслідувань, загальні правила криміналістичних досліджень. Типи електронних доказів. Криміналістичні дослідження як складова реагування на інциденти порушення кібербезпеки. Ролі та обов'язки осіб, що проводять криміналістичні дослідження. Загальна характеристика первинних цифрових криміналістичних досліджень.

ТЕМА № 2. ПРОЦЕС ПЕРВИННИХ ЦИФРОВИХ КРИМІНАЛІСТИЧНИХ ДОСЛІДЖЕНЬ

Терміни та визначення понять. Загальний огляд процесу первинних цифрових криміналістичних досліджень. Ключові компоненти ідентифікації, збирання, здобуття та збереження цифрових доказів. Процес первинних цифрових криміналістичних досліджень: комп'ютерів, периферійних пристроїв та носіїв для збереження цифрових даних, які не під'єднані до мережі; мережних пристроїв.

ТЕМА № 4. ЗДОБУТТЯ ДАНИХ ТА СТВОРЕННЯ ДУБЛІКАТІВ НОСІЇВ ДАНИХ

Загальний опис процесу вилучення даних. Здобуття даних наживо (live data). Здобуття сталих даних (static data). Послідовність у здобутті та дублюванні даних. Забезпечення незмінності оригінальних носіїв даних. Визначення ефективних методів і засобів здобуття даних. Здобуття даних з Windows і Linux комп'ютерів. Найкращі практики здобуття даних.

ТЕМА № 5. ПОДОЛАННЯ ПРОТИДІЇ КРИМІНАЛІСТИЧНИМ ДОСЛІДЖЕННЯМ

Поняття протидії криміналістичним дослідженням. Методи протидії криміналістичним дослідженням. Отримання доказів з видалених файлів і розділів, зашифрованих файлів, стеганографічних об'єктів. Ідентифікація обфускації, витирання залишків, перезапису даних та метаданих, шифрування. Криптографічні мережні протоколи, програмні пакувальники, руткіти як методи протидії криміналістичним дослідженням. Контрзаходи протидії криміналістичним дослідженням. Основні виклики у подоланні протидії криміналістичним дослідженням.

ТЕМА № 6. КРИМІНАЛІСТИЧНІ ДОСЛІДЖЕННЯ ОПЕРАЦІЙНИХ СИСТЕМ

Порядок збору і огляду стійких і нестійких даних з Windows комп'ютерів. Аналіз пам'яті і реєстру Windows. Огляд кешу, куків та історії веб-браузерів Windows.. Огляд файлів і метаданих в Windows. Аналіз журналів подій Windows. Аналіз журналів подій Linux. Збір і огляд стійких і нестійких даних з Linux комп'ютерів. Аналіз файлів і журналів подій Mac комп'ютерів.

3. КОНТРОЛЬНІ ПИТАННЯ ТА ЗАВДАННЯ ДО АТЕСТАЦІЇ

3.1. Теоретичні питання

1. Розвідка з відкритих джерел (OSINT).
2. Основні завдання, функції та організація діяльності роботи підрозділів Національної поліції України з протидії кіберзлочинам.
3. Примірний порядок визначення установчих даних особи за її мережними ідентифікаторами.
4. Шляхи отримання автентифікаційних даних особи у кіберсфері.
5. Поняття, структура та класифікація комп'ютерних мереж.
6. Поширені Інтернет-технології, застосовувані для вчинення та документування кіберзлочинів.
7. Мережні засоби зберігання інформації.
8. Електронні гроші.
9. Інтернет орієнтовані платіжні системи.
10. Альтернативні платіжні платформи.
11. Головні способи легалізації коштів з використанням електронних платіжних інструментів.
12. Об'єкти та види огляду засобів комп'ютерної техніки.
13. Загальний алгоритм огляду засобів комп'ютерної техніки.
14. Огляд стандартних засобів комп'ютерної техніки, носіїв та периферійних пристроїв.
15. Огляд мобільних засобів комп'ютерної техніки.
16. Складання аналітичних висновків.
17. Способи забезпечення анонімності в мережі.

18.Аналіз профілів соціальних мереж.

19.Встановлення інформації про володільця доменного імені та IP-адреси.

20.Аналіз електронного поштового повідомлення.

21.Методи встановлення IP-адреси.

22.Методи подолання шифрування та стеганографії.

23.Отримання доступу до ресурсів комп'ютера за допомогою SQL-ін'єкцій.

24.Вразливості систем управління контентом.

25.Методи встановлення володільця електронних фінансових інструментів.

26.Зняття інформації з електронних інформаційних систем.

27.Особливості взаємодії оперативних працівників кіберполіції зі слідчими.

28.Електронні інструменти криміналістичного аналізу.

29.Загальний порядок одержання інформації про електронні облікові записи, зареєстровані за межами України.

30.Програмне забезпечення для дослідження інформації з мобільних засобів комп'ютерної техніки.

31.Робота з великим даними під час попередження та розслідування злочинів.

32.Поняття оперативної техніки, оперативно-технічних засобів та спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших засобів негласного отримання інформації.

33.Класифікація та ознаки спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших засобів негласного отримання інформації.

34.Нормативно-правова база використання оперативно-технічних засобів.

35.Поняття та принципи застосування оперативної техніки.

36.Класифікація та ознаки запірних пристроїв.

37.Штифтові циліндрові механізми.

38.Циліндровий механізм із конічними фрезеруваннями на ключі.

39.Ознаки сувальдних запірних пристроїв.

40.Основні частини сувальдного запірного пристрою.

41.Дискові запірні пристрої.

42.Рейкові запірні пристрої.

43.Електронні запірні пристрої.

44.Кодові запірні пристрої.

45.Напрямлені мікрофони.

46.Основні елементи радіозакладки.

47.Електронні стетоскопи.

48.Електромережні закладки.

49.Види сигналізації.

50.Методи нейтралізації сигналізації.

51.Вразливості програмного забезпечення.

52.Терміни та визначення в області забезпечення кібербезпеки.

53.Об'єкт захисту при забезпеченні кібербезпеки.

54.Принципи безпеки.

55.Загрози кібербезпеки і вектори атаки.

56.Типи кібератак.

57.Механізми забезпечення кібербезпеки.

58.Базова технічна модель IT-безпеки.

59.Архітектура безпеки ІТС.

60.Отримання інформації про організацію, її мережу, вузли та сервіси з відкритих джерел.

61.Способи протидії пасивному збору інформації про об’єкт кібератаки.

62.Основні протоколи стеку TCP/IP.

63.Засоби для отримання інформації щодо вузлів та сервісів у комп’ютерній мережі.

64.Пошук вразливостей та інструменти сканування вузлів комп’ютерної мережі на вразливості.

65.Системи виявлення вторгнень та системи запобігання вторгненням.

66.Мережні екрани.

67.Мережні пастки.

68.Збір інформації про безпровідні мережі.

69.Шифрування та автентифікація в безпровідних мережах.

70.Атака на безпровідні мережі.

71.Засоби захисту від безпровідних атак.

72.Організація контролю доступу в ОС.

73.Атаки на парольний захист ОС.

74.Протидія атакам на операційні системи.

75.Типи шкідливих програм.

76.Принципи створення та аналізу троянських програм.

77.Протидія і виявлення шкідливих програм.

78.Вразливості веб-серверів та веб-застосувань.

79.Види атак на веб-сервер.

80.Види атак на веб-застосування.

81.Типи та способи виконання SQL-ін’єкцій.

82.Захист від SQL-ін’єкцій.

83.Поняття доказу і електронного доказу, законодавчі вимоги.

84.Особливості електронних (цифрових) доказів, рівні виявлення і фіксації цифрових слідів.

85.Типи кіберзлочинів, проблеми розслідувань, загальні принципи роботи з доказами із цифрових джерел інформації.

86.Ролі та обов’язки осіб, що проводять криміналістичні дослідження.

87.Основні та первинні цифрові криміналістичні дослідження, виконувачі первинних цифрових криміналістичних досліджень кримінального правопорушення.

88.Поняття ідентифікації, збирання, здобуття та зберігання цифрових доказів.

89.Поняття: копія цифрового доказу, функції верифікації, образ, виділений та невиділений простір.

90.Поняття: збереження, системний час, часовий штемпель, надійність.

91. Поняття: збіжність та відтворюваність, затвердження, псування та втручання.
92. Ролі, відповідальності, компетентності DEFR та DES.
93. Вирішення питання збирати чи здобувати потенційні цифрові докази.
94. Алгоритм збирання цифрових доказів - цифрові пристрої увімкнено.
95. Алгоритм збирання цифрових доказів - цифрові пристрої вимкнено.
96. Алгоритм здобуття цифрових доказів на увімкнених цифрових пристроях.
97. Алгоритм здобуття цифрових доказів на вимкнених цифрових пристроях.
98. Причини та процес часткового здобуття цифрових доказів.
99. Здобуття даних наживо (live data).
100. Здобуття сталих даних (static data).
101. Послідовність у криміналістичному дублюванні даних.
102. Визначення ефективних методів і засобів здобуття даних.
103. Методи протидії криміналістичним дослідженням.
104. Отримання доказів з видалених файлів і розділів, зашифрованих файлів, стеганографічних об'єктів.
105. Ідентифікація обфускації, витирання залишків, перезапису даних та метаданих, шифрування.
106. Криптографічні мережні протоколи, програмні пакувальники, руткіти як методи протидії криміналістичним дослідженням.
107. Контрзаходи протидії криміналістичним дослідженням.
108. Порядок здобуття і огляду стійких і нестійких даних з Windows комп'ютерів.
109. Аналіз пам'яті і реєстру Windows.
110. Огляд кешу, куків, історії веб-браузерів, файлів і метаданих в Windows.
111. Аналіз журналів подій Windows і Linux систем.
112. Здобуття і огляд стійких і нестійких даних з Linux комп'ютерів.

3.2. Практичні завдання

1. Із наведеного фрагменту заголовку електронного поштового листа визначте ймовірну IP-адресу терміналу, з якого його було відправлено (вказується на екзамені)?
2. Якій організації належить IP-діапазон (вказується на екзамені)?
3. Визначити банк емітент платіжної картки (вказується на екзамені)?
4. Стало відомо, що підозрювана особа здійснювала комунікації через HTTP проксі-сервер (вказується на екзамені). Вкажіть, на ім'я якого провайдера (назва) потрібно надіслати запит про збереження інформації щодо з'єднань абонента до оформлення відповідного міжнародного запиту?
5. За допомогою сервісу Shodan дізнатися IP-адреси вузлів заражених шкідливим програмним забезпеченням у місті (вказується на екзамені).

6. За допомогою утиліт командного рядка в системі Windows знайти рядок (вказується на екзамені) у текстовому файлі (написати команду).

7. Вкажіть хоча б один файл, який було завантажено з мережі Інтернет у поточному році з IP-адреси (вказується на екзамені).

8. Визначити тип (Visa чи MasterCard) платіжної картки (вказується на екзамені).

9. Отримати обліковий запис (зареєструватися) на сайті (вказується на екзамені) без наявної SIM-картки в телефоні.

10. Під час здійснення первинних заходів зі встановлення інформації про володільця облікового запису Skype за допомогою програми WireShark оперативний працівник дійшов попереднього висновку, що шукана особа може перебувати з ним в одній будівлі. На підставі чого міг бути зроблений такий висновок?

11. Під час розслідування кримінального провадження за ознаками вчинення злочину, передбаченого ст. 361 Кримінального кодексу України, було вилучено комп'ютерну техніку підозрюваного. Значна частина пристроїв була прив'язана до одного облікового запису. Яким чином можна дізнатися повну історію користування цим обліковим записом?

12. Під час розслідування кримінального провадження за ознаками вчинення злочину, передбаченого ст. 303 Кримінального кодексу України, було встановлено контактну електронну поштову скриньку особи, яка може бути причетною до вчинення розслідуваного злочину. Знайдіть фото, прив'язане до облікового запису та місця, які володілець облікового запису відмітив на карті.

13. Під час розслідування кримінального провадження за ознаками вчинення злочину, передбаченого ст. 363 Кримінального кодексу України, було встановлено контактну електронну поштову скриньку особи, яка може бути причетною до вчинення розслідуваного злочину. Знайдіть принаймні три ресурси, на яких під час реєстрації використовувалася встановлена електронна пошта.

14. Створити мультимедіа-контент, який не буде виявлятися системами розпізнавання слідів роботи штучного інтелекту.

15. Під час огляду засобу комп'ютерної техніки на ньому було виявлено банк даних у вигляді неструктурованого текстового файлу. Привести фрагмент тексту до визначеної структури. Імпортувати приведені дані до СУБД.

16. Під час огляду засобу комп'ютерної техніки на ньому було виявлено банк даних у вигляді неструктурованого текстового файлу розміром 3 Тб. За допомогою вбудованих в операційну систему утиліт знайти у відповідному файлі текстовий фрагмент (вказується на екзамені).

17. Під час вивчення зв'язків фігурантів виникла потреба у використанні програми Maltego. Додати один із локальних перетворювачів, вказаних викладачем та протестувати його функціональність.

18. Під час вивчення зв'язків фігурантів виникла потреба у використанні програми Maltego. Додати в програму перетворювач за відомою Seed URL.

19. Під час моніторингу мережі Інтернет працівниками поліції було виявлено протиправний контент на одному з сайтів. Визначити для сайту

застосовувані сертифікати, існуючі субдомени, історію функціонування, рекламні метрики для проведення подальшого аналізу.

20. Скласти запитову частину відповідного процесуального документу для одержання інформації про належність IP-адреси конкретному користувачеві у визначений час, якщо IP-адреса належить великому оператору мобільного зв'язку.

21. Налаштувати віддалене SSH підключення з ОС Windows до ОС Kali Linux із використанням автентифікації за допомогою RSA ключів.

22. 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.

23. За наданим доменним ім'ям ресурсу, який використовує послуги Cloudflare, встановити його справжню IP адресу.

24. За наданим доменним ім'ям ресурсу і програми Web data extractor здійснити збір даних із сайту.

25. За наданим доменним ім'ям ресурсу зібрати DNS інформацію про ресурс із використанням robtex.com.

26. За наданим доменним ім'ям ресурсу знайти перелік сайтів, які розміщуються на тому ж самому сервері, що й цільовий.

27. За наданим доменним ім'ям ресурсу знайти перелік субдоменів цільового домену.

28. Здійснити пошук та аналіз каталогів і файлів для вебсайту на віртуальній машині metasploitable2.

29. За наданим доменним ім'ям ресурсу за допомогою metagoofil знайти і завантажити для аналізу метаданих доступні файли.

30. З визначеного ресурсу за допомогою Theharvester і Infoga зібрати доступні записи електронної пошти, імен користувачів, вузлів та субдоменів.

31. Визначити доступні мережні сервіси (відкриті порти) для scanme.nmap.org.

32. Визначити наявні вразливості віртуальної машини metasploitable2.

33. Продемонструвати налаштування iptables (міжмережного екрану) в ОС Kali Linux.

34. Продемонструвати створення та застосування бекдору для ОС Windows 10.

35. Продемонструвати експлуатацію вразливості вебзастосунку для віртуальної машини Five86:1 (Vulnhub).

36. Для здобуття потенційних доказів отримана ухвала суду щодо тимчасового доступу до речей і документів, а саме до файлів журналів провайдера послуг Інтернету (оператора мобільного зв'язку), файлів відеозапису системи відеоспостереження, тощо. Створити копії електронних документів, які будуть визнані судом як оригінальні.

37. При огляді місця вчинення кримінального правопорушення (обшуку) були виявлені носії цифрової інформації – картки пам'яті, флеш-накопичувачі. Здобути з носіїв цифрової інформації потенційні електронні докази вчинення кримінального правопорушення.

38. При огляді місця вчинення кримінального правопорушення (обшуку) було виявлено включений комп'ютер з ОС Windows. Здобути з включеного комп'ютеру з ОС Windows нестійкі дані, що можуть бути доказами вчинення кримінального правопорушення.

39. Оперативному працівнику Національної поліції надійшло доручення від слідчого оглянути смартфон з ОС Android, який було вилучено у підозрюваного на місці вчинення злочину. Здобути з включеного смартфону потенційні електронні докази вчинення кримінального правопорушення.

40. При огляді наживо Windows і Linux комп'ютерів підозрюваного було виявлено теки із файлами без розширень. Визначити типи знайдених файлів.

41. При огляді наживо Windows комп'ютеру підозрюваного було виявлено файли без розширень. Встановити метадані знайдених файлів.

42. Продемонструвати стеганографічне приховування та виявлення файлів за допомогою утиліти OpenPuff.

43. Продемонструвати приховування та виявлення файлів із використанням альтернативного потоку даних NTFS.

4. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Criminal Intelligence. Manual for Analysts. United Nations, 2011. 96 c.

2. Handbook of Digital Forensics and Investigation / edited by Eoghan Casey. Elsevier Academic Press, 2010. 567 p.

3. Online Investigative Principles for Federal Law Enforcement Agents. November 1999.

4. Бандурка О. М. Теорія і практика оперативно-розшукової діяльності: монографія. Харків : Золота миля, 2012. 620 с.

5. Богинський О. В. Деякі методи, що застосовуються для підготовки аналітичних висновків, в межах інституту кримінальної розвідки. Legea si Viata. 2018. № 3. С. 11-15.

6. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. К., 2017. 148 с.

7. Манжай О. В. Аналіз методології кримінальної розвідки в зарубіжних країнах. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. 2016. № 3(75). С. 256-265.

8. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. Вісник Харківського національного університету внутрішніх справ. 2016. № 3(74). С. 111-120.

9. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. Право і безпека. 2009. № 4 (31). С. 215–219.

10. Методика розкриття злочинів, вчинених у сфері функціонування платіжних карток та електронних розрахунків: наук.-метод. рек. / О. І. Безпалова, Д. Т. Карпізін, В. В. Носов, О. В. Манжай, В. І. Стреляний. Х. : Харк. нац. ун-т. внутр. справ. 2013. 79 с.

11. Незаконні дії з банківськими платіжними картками: методичні рекомендації. К. : МВС України, 2013. 28 с.

12. Петрович Л., В'ятов Н. Пошук та вилучення доказів: тренінг для тренерів з викладання тематики розслідування кіберзлочинів для представників навчальних закладів МВС України. К. : Проект ОБСЄ «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні»), 2014. 60 с.

13. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016. URL: http://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення: 12.06.2019).

14. Носов В.В. Кібербезпека // Курс дистанційного навчання. URL: https://kursant.univd.edu.ua (дата звернення: 13.04.2020).

15. Носов В.В. Цифрова криміналістика // Курс дистанційного навчання. URL: https://kursant.univd.edu.ua (дата звернення: 13.04.2020).

16. ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. На заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT) ; Чинний від 2019-01-01. Київ : УкрНДНЦ, 2018. VI, 31 с. : рис., табл. (Національний стандарт України).

Допоміжна

17. Manzhai O .V. Special Investigation Activity Comparative Studies // *Internal Security*. 2015. № 1(7). pp. 19-37.

18. Marshall A. M., Miller P. CaseNote: Mobile phone call data obfuscation & techniques for call correlation. *Digital Investigation*. 2019. Vol. 29. pp. 82-90 (DOI: 10.1016/j.diin.2019.03.004).

19. Бандурка О. М., Перепелиця М. М., Манжай О. В., Шендрик В. В. Оперативно-розшукова компаративістика: монографія. Х. : Золота миля, 2013. 352 с., іл.

20. Вакутин Ю. А. Способы маскировки преступного поведения: учеб. пособие. Омск : Высшая школа милиции МВД СССР. 1987. 132 с.

21. Збереження і отримання записів від провайдерів Інтернет-послуг в Сполучених Штатах Америки: довідник для правоохоронних органів іноземних країн. 2014. 33 с.

22. Перепелиця М.М., Манжай О.В., Шендрик В.В. Використання комп'ютерних технологій в оперативно-розшуковій діяльності: навчальний-посібник / за заг. ред. О.М. Бандурки. Одеса : ОДУВС, 2011. 146 с., іл.

23. Про основні засади забезпечення кібербезпеки України: Закон України : від 05.10.2017 : [із змінами і доповненнями] // Відомості Верховної Ради України. 2017. № 45 (10.11.2017). Ст. 403.

24. Про телекомунікації : Закон України від 18.11.2003 : [із змінами і доповненнями]. *Офіційний вісник України*. 2003. № 51 (02.01.2004). Ч. 1. Ст. 2644.

25. Реєстр методик проведення судових експертиз. URL: http://rmpse.minjust.gov.ua (дата звернення: 13.02.2020).

26. Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. 2019. Вип. 146. С. 179–191.

Інформаційні ресурси в Інтернеті

27. http://www.court.gov.ua/vscourt – веб-портал судової влади в Україні
28. http://www.gp.gov.ua – веб-сайт Генеральної прокуратури України.
29. http://www.kmu.gov.ua – веб-сайт Кабінету Міністрів України.
30. http://www.minjust.gov.ua – веб-сайт Міністерства юстиції України.
31. http://www.mvs.gov.ua – веб-сайт Міністерства внутрішніх справ України.
32. http://www.portal.rada.gov.ua – веб-сайт Верховної Ради України.
33. http://www.president.gov.ua – веб-сайт Президента України.
34. http://www.reyestr.court.gov.ua – єдиний реєстр судових рішень в Україні.
35. http://www.sbu.gov.ua – веб-сайт СБУ.
36. http://www.scourt.gov.ua – веб-сайт Верховного Суду України.
37. https://www.npu.gov.ua/ – веб-сайт Національної поліції України.
38. https://securityonline.info/category/forensics.
39. https://resources.infosecinstitute.com/category/forensics-2.
40. http://www.dfrws.org.
41. https://www.forensicmethods.com.
42. http://www.hackerhighschool.org.
43. https://securityonline.info.
44. https://gbhackers.com.
45. https://securityonline.info.
46. https://www.hackingarticles.in.