МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
В.о. декана факультету комп'ютерних інформаційних технологій
_____Ігор ЯКИМЕНКО
«___» _____ 20___р.

ЗАТВЕРДЖУЮ
В.о. проректора з науково-педагогічної роботи
_____Віктор ОСТРОВЕРХОВ
«___» _____ 20___р.

ЗАТВЕРДЖУЮ:
Директор навчально-наукового інституту новітніх освітніх технологій
_____Святослав ПИТЕЛЬ
«___» _____ 20___р.

РОБОЧА ПРОГРАМА
з дисципліни
«АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ»

Ступінь вищої освіти – **магістр**
Галузь знань – **12 Інформаційні технології**
Спеціальність – **125 Кібербезпека та захист інформації**
Освітньо-професійна програма – **Кібербезпека**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лаборат. (семін.) (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	Іспит (сем)
Денна	1	1	30	15	5	4	96	150	1
Заочна	1	1,2	8	4			138	150	2

Тернопіль – 2023

Робоча програма складена на основі освітньо-професійної програми підготовки магістра за спеціальністю 125 - Кібербезпека та захист інформації галузі знань 12 - Інформаційні технології, затвердженої Вченої радою ЗУНУ
протокол № 10 від 23.06.2023 р.

Робочу програму склав доцент кафедри кібербезпеки, к.т.н., доцент Івасьєв Степан Володимирович.

Робоча програма затверджена на засіданні кафедри кібербезпеки,
протокол № 1 від 28.08.20223р.

Завідувач кафедри
кібербезпеки Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності кібербезпека та захист інформації, протокол № 1 від 30.08.2023 р.

Керівник групи
забезпечення спеціальності Василь ЯЦКІВ

Гарант ОП Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Аналіз шкідливого програмного забезпечення»

Дисципліна – «Аналіз шкідливого програмного забезпечення»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	Галузь знань 12 Інформаційні технології	Статус дисципліни – обов'язкова Мова навчання - українська
Кількість залікових модулів – 4	Спеціальність 125 – Кібербезпека та захист інформації	Рік підготовки ДФН – 1, ЗФН– 1 Семестр: ДФН – 1; ЗФН – 1,2
Кількість змістових модулів –2	Ступінь вищої освіти – магістр	Лекції: ДФН - 30 год., ЗФН – 8 год. Лабораторні заняття: ДФН - 15 год.; ЗФН – 4 год.
Загальна кількість годин – 150		СРС: ДФН - 100 год., в т.ч. тренінг – 4год.; ЗФН – 138 год.Індивідуальна робота -5 год.
Тижневих годин:10 год., з них аудиторних –3 год.		Вид підсумкового контролю – іспит

2. Мета й завдання вивчення дисципліни

2.1. Мета вивчення дисципліни

Мета вивчення дисципліни «Аналіз шкідливого програмного забезпечення» полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного машинного навчання, необхідних для подальшої роботи та навчити застосуванню методів та засобів аналізу шкідливого програмного забезпечення в умовах широкого використання сучасних інформаційних технологій.

2.2 Завдання вивчення дисципліни

В результаті вивчення курсу «Аналіз шкідливого програмного забезпечення» студенти повинні:володіти методиками проведення зворотної розробки програмного забезпечення та апаратних пристроїв; засвоїти основні фундаментальні поняття і закони методів реверс інжинірингу для їх використання в сучасних умовах; знати принципи побудови сучасного програмного забезпечення; вміти використовувати основний математичний апарат та закони декомпіляції програмного забезпечення; вміти використовувати програмні засоби, які реалізують основні методи реверс інжинірингу. Завдання проведення лекцій полягає у розгляді найкращих практик динамічного та статичного аналізу шкідливого ПЗ, проведенні декомпіляції та дебагінгу коду. Завдання проведення практичних занять, як одна з основних форм навчального процесу, передбачає набуття практичних навиків з виявлення, ідентифікації, статичного та динаміного аналізу, декомпіляції та дебагінгу шкідливого програмного забезпечення.

2.3.Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни

Здатність до абстрактного мислення, аналізу та синтезу.

Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог

Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації..

2.4 Передумови для вивчення дисципліни.

Вивчення курсу «Аналіз шкідливого програмного забезпечення» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Тестування комп'ютерних систем на проникнення», «Дослідження і проектування систем захисту інформації», «Моніторинг мережевої безпеки»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

2.5. Результати навчання

Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації

3. Програма навчальної дисципліни

Змістовний модуль 1. Реверс інжиніринг.

Тема 1. Основні статичні методики

Програмне забезпечення, основи статичного аналізу. Проектування та зворотнє проектування ПЗ. Фази проектування ПЗ. Програмний продукт.

Література: 1, 5, 11.

Тема 2. Упаковане і обфуційоване шкідливе ПЗ.

Методології проектування запакованого ПЗ. Пакувальники. Архіватори.

Література: 2, 8.

Тема 3. Аналіз шкідливих програм в віртуальних машинах.

Технології віртуалізації. Дослідження змін в реєстрі. Дослідження змін в файловій системі.

Література: 4, 7.

Тема 4. Використання віртуальної машини для аналізу безпеки.

Сканери вразливостей. Сервери DCOM. Аналіз відкритих портів та вразливостей ОС.

Література: 3, 6.

Тема 5. Основи динамічного аналізу.

Основні поняття динамічного аналізу. Структурування систем. Моделі управління програм. Модульна декомпозиція. Проблемно-залежні архітектури ПЗ. Шаблони проектування ПЗ.

Література: 5, 8.

Тема 6. Прискорений курс по асемблеру для архітектури x86.

Поняття асемблера. Архітектури операційної системи. Набори інструкцій. Шкідливі програми в середині спеціального ПЗ.

Література: 4, 9.

Тема 7. Розпізнавання конструкцій мови С в асемблері.

Дизасемблювання. Аналіз двійкового коду.Розпізнавання конструкцій мови С в асемблері.

Література: 3, 11.

Тема 8. Аналіз шкідливих програм для Windows.

Основні поняття об'єктного підходу. Об'єкти і класи об'єктів. Ієрархія класів. Процес розпізнавання об'єктно-орієнтованого коду. Визначення об'єктів. Моделі архітектури. Модифікація системної архітектури.

Література: 2, 10.

Тема 9. Порівняння налагодження на рівні вихідного і дизасемблювати коду. Аналізатор на рівні асемблера OllyDbg.

Аналізатор на рівні асемблера OllyDbg. Вихідне налагодження. Низхідне налагодження. Дизасемблювання коду.

Література: 1, 5, 8.

Змістовий модуль 2. Відлагодження та дизасемблювання ПЗ.

Тема 10. Відлагодження ядра з допомогою WinDbg.

Драйвери і код ядра. Відлагоджувальні символи Microsoft. Особливості ядра Windows Vista,7,10. Робота з WinDbg.

Література: 1, 5, 11.

Тема 11. Антидизассемблювання.

Асемблер для архітектури x86. Технологія IDA Pro. Розпізнавання конструкцій С та їх приховування в асемблері. Аналіз шкідливих програм для Windows.

Література: 1, 2, 6.

Тема 12. Антивідладка.

Відлагоджування. Технологія OllyDbg. Відлагодження ядра з допомогою WinDbg/

Література: 2, 3, 9.

Тема 13. Методи протидії віртуальним машинам.

Поведінка шкідливого ПЗ. Скритий запуск шкідливого ПЗ. Кодування даних. Мережеві сигнатури. Виявлення віртуальної машини.

Література: 4, 7, 10.

Тема 14. Пакувальники і розпакування.

Антидизасемблювання. Антивідладка. Пакувальники та де пакувальники.

Література: 1, 3, 8.

Тема 15. Аналіз коду командної оболонки.

Аналіз коду командної стрічки. Аналіз коду C++. Шістдесятчотирьохбітні шкідливі програми.

Література: 3, 5, 9.

4. Структура залікового кредиту дисципліни

ДФН	Кількість годин				
	Лекції	Лабор. заняття	Самост. робота	Індив. робота	Контрольні заходи
Змістовий модуль 1. Реверс інжиніринг					
Теми 1. Основні статичні методики	2		6		Поточне опитування
Тема 2. Упаковане і обфуційоване шкідливе ПЗ.	2		6		Поточне опитування
Тема 3. Аналіз шкідливих програм в віртуальних машинах.	2		6	1	Поточне опитування
Тема 4. Використання віртуальної машини для аналізу безпеки.	2		6		Поточне опитування
Тема 5. Основи динамічного аналізу.	2		6	1	Поточне опитування
Тема 6. Прискорений курс по асемблеру для архітектури x86.	2	1	6		Поточне опитування
Тема 7. Розпізнавання конструкцій мови С в асемблері.	2		6		Поточне опитування
Тема 8. Аналіз шкідливих програм для Windows.	2	2	6	1	Поточне опитування
Тема 9. Порівняння налагодження на рівні вихідного і дизасемблювати коду. Аналізатор на рівні асемблера OllyDbg.	2		6		Поточне опитування
Змістовий модуль 2. Відлагодження та дизасемблювання ПЗ.					
Тема 9. Порівняння налагодження на рівні вихідного і дизасемблювати коду. Аналізатор на рівні асемблера OllyDbg.	2	2	6		Поточне опитування
Тема 10. Відлагодження ядра з допомогою WinDbg.	2	2	6		Поточне опитування
Тема 11. Антидизассемблювання.	1		6	1	Поточне опитування
Тема 12. Антивідладка.	1	2	6		Поточне опитування
Тема 13. Методи протидії віртуальним машинам.	2	2	8		Поточне опитування
Тема 14. Пакувальники і розпакування.	2	2	8		Поточне опитування
Тема 15. Аналіз коду командної оболонки.	4	2	8	1	Поточне опитування

Тренінг			4		КПІЗ
Разом	**30**	**15**	**100**	**5**	

ЗФН	Кількість годин				
	Лекції	Лабор. заняття	Самост. робота	Індив. робота	Контрольні заходи
Змістовий модуль 1. Реверс інжиніринг.					
Теми 1. Основні статичні методики	0,5	0,25	6		Поточне опитування
Тема 2. Упаковане і обфуційоване шкідливе ПЗ.	0,5	0,25	6		Поточне опитування
Тема 3. Аналіз шкідливих програм в віртуальних машинах.	0,5	0,25	6		Поточне опитування
Тема 4. Використання віртуальної машини для аналізу безпеки.	0,5	0,25	6		Поточне опитування
Тема 5. Основи динамічного аналізу.	0,5	0,25	6		Поточне опитування
Тема 6. Прискорений курс по асемблеру для архітектури x86.	0,5	0,25	8		Поточне опитування
Тема 7. Розпізнавання конструкцій мови С в асемблері.	0,5	0,25	10		Поточне опитування
Тема 8. Аналіз шкідливих програм для Windows.	0,5	0,25	10		Поточне опитування
Тема 9. Порівняння налагодження на рівні вихідного і дизасемблювати коду. Аналізатор на рівні асемблера OllyDbg.	0,5	0,25	10		Поточне опитування
Змістовий модуль 2. Відлагодження та дизасемблювання ПЗ.					
Тема 9. Порівняння налагодження на рівні вихідного і дизасемблювати коду. Аналізатор на рівні асемблера OllyDbg.	0,5	0,25	10		Поточне опитування
Тема 10. Відлагодження ядра з допомогою WinDbg.	0,5	0,25	10		Поточне опитування
Тема 11. Антидизассемблювання.	0,5	0,25	10		Поточне опитування
Тема 12. Антивідладка.	0,5	0,25	10		Поточне опитування
Тема 13. Методи протидії віртуальним машинам.	0,5	0,25	10		Поточне опитування
Тема 14. Пакувальники і розпакування.	0,5	0,25	10		Поточне опитування
Тема 15. Аналіз коду командної оболонки.	0,5	0,25	10		Поточне опитування
Разом	**8**	**4**	**138**		

5. Тематика лабораторних занять.

Лабораторна робота №1.

Тема: Основи визначення технологій реверсної інженерії.

Мета: Вміти виявляти упаковане шкідливе ПЗ. Вміти досліджувати заголовки і розділи PE-файла. Знаходити та виділяти використання хеш функцій.

Питання для обговорення: 1. Технологія хешування. 2. Упаковане шкідливе ПЗ. 3. Заголовки і розділи PE-файла.

Література:1-11.

Лабораторна робота № 2.

Тема: Основи динамічного аналізу.

Мета: Навчитися розв’язувати задачі динамічного аналізу. Досліджувати вплив шкідливого ПЗ на Windows. Виявляти підозрілу мережеву активність.

Питання для обговорення: 1. Запуск шкідливих програм. 2. Моніторинг з допомогою Process Explorer 3. Порівняння знімків реєстра. 4. Симуляція мережі.5 Перехоплення пакетів з

допомогою Wireshark.

Література:1-11.

Лабораторна робота № 3.

Тема: Робота з IDAPro.

Мета: Навчитися працювати з системами для реверс інженерії програмного забезпечення. Вміти використовувати системи дизасемблювання, такі як IDAPro.

Питання для обговорення:

1. Інтерфейс IDAPro. 2. Використання перехресних посилань. 3. Підвищення швидкодії дизасемблювання. 4. Плагіни IDAPro.

Література: 1-11.

Лабораторна робота № 4.

Тема: Дослідження додатків Windows.

Мета: Навчитися використовувати Windows API для відслідковування шкідливого ПЗ. Навчитися виявляти зміни в режимах ядра системи.

Питання для обговорення:

1. Windows API. 2. API для роботи з мережею. 3. Відслідковування запущених програм. 4. Порівняння режимів ядра.

Література: 1-11.

Лабораторна робота № 5.

Тема: Відлагодження.

Мета: Навчитися використовувати системи відлагодження для зворотного проектування. Навчитися керувати виконанням програми з допомогою відладника.

Питання для обговорення:

1. Порівняння процесі від лагодження на рівні від лагодження. 2. Виключні ситуації. 3.Керування виконанням з допомогою відладника.

Література: 1-11.

Лабораторна робота № 6.

Тема: Використання OllyDbg.

Мета: Навчиттися працювати зі стеками. Виявляти незахищені виключні ситуації. Використовувати відлагодження з використанням скриптів.

Питання для обговорення: 1. Завантаження шкідливого ПЗ. 2. Робота зі стеками.3. Обробка виключень. 4. Відлагодження з використанням скриптів.

Література: 1-11.

Лабораторна робота № 7.

Тема: Відлагоджувальні системи Microsoft.

Мета: Мати загальне уявлення про драйвери і код ядра. Вміти застосовувати відлагоджувальні символи Microsoft. Вміти працювати з WinDbg.

Питання для обговорення: 1. Драйвери і код ядра. 2. Відлагоджувальні символи Microsoft. 3. Особливості ядра Windows Vista,7,10. 4. Робота з WinDbg.

Література: 1-11.

Лабораторна робота № 8.

Тема: Поведінка шкідливих програм.

Мета: Вміти виявляти взлом облікових записів Microsoft. Вміти виявляти та знешкоджувати руткіти в користувацькому режимі. Виявляти зміну привілегій облікових записів.

Питання для обговорення: 1. Взлом облікових записів. 2. Підвищення привілегій. 3. Механізми постійної присутності. 4. Руткіти в користувацькому режимі.

Література: 1-11.

6. Комплексне практичне індивідуальне з дисципліни.

Індивідуальна робота студента передбачає виконання комплексного практичного індивідуального завдання, яке виконується кожним студентом одноосібно. Студенти повинні провести аналіз наданого ПЗ та провести за одним з варіантів:

1. Динамічний аналіз.
2. Статичний аналіз.
3. Виявлення C++ коду.
4. Декомпіляція шкідливого ПЗ.
5. Аналіз дій з реєстром.

6. Виявлення змін в файловій системі.
7. Спостереження за мережевою активністю.

7. Самостійна робота

№ п/п	Тематика
1	Завантаження коду командної оболонки для аналізу
2	Позиційно-незалежний код
3	Визначення адреси виконання
4	Пошук символів вручну
5	Остаточна версія програми Hello World
6	Кодування коду командної оболонки
7	NOP-ланцюжка
8	Пошук коду командної оболонки
9	Аналіз коду на C ++
10	Об'єктно-орієнтоване програмування
11	Звичайні та віртуальні функції
12	Створення і знищення об'єктів
13	64-бітні шкідливі програми
14	Особливості архітектури x64
15	WOW64
16	Ознаки шкідливого коду на платформі x64

8. Тренінг з дисципліни.

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі студентів.

Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Рекомендується наступне проведення тренінгу:

№	Вид роботи	Порядок проведення тренінгу
1	Огляд сучасних середовищ моделювання комп'ютерних програм	1. розгляд сучасних середовищ моделювання програм фірм Visual Paradigm, Microsoft; 2. дослідження мови графічного опису для об'єктного моделювання на основі UML діаграм
2	Розгляд процесу моделювання комп'ютерних програм	- постановка задачі; - опис технічного завдання; - моделювання програмної розробки на основі UML діаграм
3	Програмна реалізація проектованого додатку	– Реалізація розробленої програми на об'єктна-орієнтованій мові програмування; – реалізація графічного інтерфейсу користувача.
4	Тестування розробленого програмного додатку	1. вибір та обґрунтування тестової вибірки; 2. опис вхідних та вихідних даних; 3. перевірка правильності роботи реалізованого програмного додатку

9. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; практичні роботи, індивідуальні заняття; робота в Інтернет.

10. Засоби оцінювання та методи демонстрування результатів навчання.

У процесі вивчення дисципліни «Аналіз шкідливого програмного забезпечення» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування;
- залікове модульне тестування та опитування;
- оцінювання результатів КПІЗ;
- завдання на лабораторному обладнанні, тренажерах, реальних об’єктах тощо;
- ректорська контрольна робота;ю

11. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Аналіз шкідливого програмного забезпечення» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Семестр 1 - екзамен

Заліковий модуль 1	Заліковий модуль 2 (ректорська контрольна робота)	Заліковий модуль 3 (підсумкова оцінка за КПІЗ враховуючи поточне опитування)	Заліковий модуль 4 (письмовий екзамен)
20%	20%	20%	40%
1. Теоретичні питання – max 40 балів. 2. Практичне завдання: 2 практичні завдання по 30 балів – max 60 балів.	1. Теоретичні питання – max 40 балів. 2. Практичне завдання: 2 практичні завдання по 30 балів – max 60 балів.	1. Підготовка КПІЗ – max 40 балів. 2. Захист КПІЗ – max 40 балів. 3. Участь у тренінгах – max 20 балів	1. Теоретичні питання: 3 питання по 20 балів - max 60 балів. 2. Практичне завдання - max 40 балів

Шкала оцінювання

За шкалою університету	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75–84		C (добре)
65–74	задовільно	D (задовільно)
60–64		E (достатньо)
35–59	незадовільно	FX (незадовільно з можливістю повторного складання)
1–34		F (незадовільно з обов’язковим повторним курсом)

12. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна.

№	Найменування	Номер теми
1	Мультимедійний проектор та проєкційний екран	1 -15
2	Персональні комп’ютери	1 -15
3	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1 -15
4	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1 -15
5	Наявність доступу до мережі Інтернет	1 -15
6	DrWeb Cure it, FoxitReader, WinZip, Total Commander, Dev C++, MASM32, SQL Server Community Editions, OllyDbg 1.0, WinDbg.	1-15

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Mishra A. Mobile App Reverse Engineering: Get started with discovering, analyzing, and exploring the internals of Android and iOS apps. Birmingham: Packt Publishing, 2022. - 165 p.
2. Omar M. Defending Cyber Systems through Reverse Engineering of Criminal Malware.

Springer, 2022. - 59 p.
3. Додонов А.Г. та ін. Комп'ютерна конкурентна розвідка. Додонов А.Г., Ланде Д.В., Прищепа В.В., Путятін В.Г. - Київ: ТОВ Інжиніринг, 2021. - 355 с.
4. Belous A., Saladukha V. Viruses, Hardware and Software Trojans: Attacks and Countermeasures. Springer, 2020. - 838 p.
5. Alrabaee S., Debbabi M., Shirani P., Wang L., Youssef A., Rahimian A., Nouh L., Mouheb D., Huang H., Hanna A. Binary Code Fingerprinting for Cybersecurity: Application to Malicious Code Fingerprinting. Springer, 2020. - 264 p.
6. Basant Vidya. Hacking Mastery With Kali Linux. Independently published, 2021. - 200 p.
7. Mohanta Abhijit, Saldanha Anoop. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware. Apress Media LLC, 2020. — 948 p.
8. Budgen David. Software Design: Creating Solutions for Ill-Structured Problems. 3rd edition. — Routledge, 2021. — 365 p.
9. Martins Luiz Eduardo, Gorschek Tony. Requirements Engineering for Software and Systems. River Publishers, 2022. — 230 p.
10. Wardle Patrick. The Art of Mac Malware: The Guide to Analyzing Malicious Software. No Starch Press, 2022. — 320 p
11. Kohnfelder Loren. Designing Secure Software. No Starch Press, 2022. — 332 p.