Анализ источников по теме «информационная безопасность»

1. Эриксон Джон «Искусство эксплоита» // Санкт-Петербург: Питер. 2018. - 496 с.

Данная книга не содержит в себе каких-то готовых рецептов взлома чего-либо. Она даёт читателю необходимую базу для понимания основных направлений хакинга, например, реверс-инжиниринг и эксплуатацию уязвимостей, безопасность веб-приложений, криптографию и беспроводные сети. Кроме того, в книге даны основы языка Си и ассемблера.

2. А. А. Бирюков «Информационная безопасность. Защита и нападение» // ДМК-Пресс. 2017. - 434 с.

Во многих книгах по ИБ освещаются либо только технические аспекты, либо нормативные акты, связанные с обеспечением ИБ. Но данное учебное пособие стремится избавиться от однобокого разбора этой темы, и поэтому в ней приводятся как техническая информация, описывающая атаки и защиту от них, так и рекомендации по обеспечению информационной безопасности с соответствующими примерами.

3. Adrian Mouat «Docker Security» // O'Reilly Media. 2016.

Чтобы безопасно использовать Docker, необходимо знать о потенциальных проблемах безопасности, а также об основных инструментах и методах обеспечения безопасности систем на базе контейнеров. Автор этой книги Эдриан Муат (Adrian Mouat) даёт в ней рекомендации для разработки политик и процедур безопасности контейнеров.
В книге рассматриваются такие угрозы, как эксплойты ядра, DoS-атаки, разрывы контейнеров и заражённые изображения. Хоть книга и выпущена в 2016 году, многие методы, приведенные в ней, по-прежнему актуальны.

4. Jason Andress, Ryan Linn «Coding for Penetration Testers» // Syngress. 2011 - 320 с.

Данная книга познакомит читателей со скриптовыми языками, которые используются в инструментах для тестов на проникновение, а также с примерами того, как их использовать и в каких ситуациях.

5. Nicholas Marsh «Nmap Cookbook: The Fat-Free Guide to Network Security Scanning» // CreateSpace Independent Publishing Platform. 2015 - 226 с.

Данная книга обеспечивает упрощённый охват функций сетевого сканирования, доступных в наборе утилит Nmap. Каждая функция Nmap проиллюстрирована наглядными примерами, которые помогут быстро понять их назначение.

6. Родичев Ю. А. «Нормативная база и стандарты в области информационной безопасности. Учебное пособие» // Санкт-Петербург: Питер. 2021 - 256 с.

Учебное пособие, выпущенное в 2017 году, является одним из самых последних изданий по защите информации. В нем рассмотрены наиболее важные нормативные документы ФСТЭК, а также международные и национальные стандарты Российской Федерации в области информационной безопасности.

7. В. Бондарев «Введение в информационную безопасность автоматизированных систем» // Издательство МГТУ им. Н. Э. Баумана. 2021 - 252 с.

В книге рассмотрена законодательная база информационной безопасности, приведен перечень основных возможных угроз, а также описываются подходы к созданию систем защиты информации. Также приводится классификация предупредительных мер. Изучены вопросы программно-аппаратных механизмов обеспечения информационной безопасности.

8. С. А. Нестеров «Основы информационной безопасности» // Лань. 2022 - 324 с.

В этой книге основательно и последовательно излагаются основы информационной безопасности, описываются практические аспекты ее реализации. Читатель изучит:

1) теоретические основы защиты информации;
2) основы криптографии;
3) защиту информации в IP-сетях;
4) анализ и управление рисками в сфере информационной безопасности.

Теоретический материал сопровождается лабораторными работами, выделенными в отдельный раздел.

9. Николай Скрабцов «Аудит безопасности информационных систем» // Санкт-Петербург: Питер. 2017 - 272 с.

В книге Никиты Скабцова (магистр CS, опыт работы инженером по информационной безопасности – 10 лет, преподаватель «компьютерные сети, операционные системы», сертификаты: CEH, CCSA, LPIC, MCITP) рассматриваются методы

обхода систем безопасности сетевых сервисов и проникновения в открытые информационные системы.

10. Алексей Милосердов, Данил Гриднев «Тестирование на проникновение с Kali Linux»

Полный Гид по Kali Linux : тестирование на проникновение, книгу, пригодную для использования как новичками так и уже опытным администраторам и экспертам ИБ для целей проведения аудита безопасности ИТ-инфраструктуры. Книга состоит из 8 частей, в которые входят 62 главы с подробным описанием используемых инструментов и методик тестирования.

Книга является систематизированным сборником, включающим переводы англоязычных ресурсов, книг и веб-сайтов, посвящённых теме penetration testing, а также собственный опыт авторов.

11. Kimberly Graves «Certified Ethical Hacker Review Guide» // Sybex. 2010 - 432 с.

Официальное руководство по подготовке к экзаменам на сертификацию CEH поможет выявить риски сетей и компьютеров в плане безопасности. Руководство охватывает весь спектр вопросов хакинга современных систем.

12. Jack Koziol, David Litchfield, Dave Aitel, Chris Anley «The Shellcoder’s Handbook» // Wiley. 2007 - 744 с.

Группа ведущих экспертов в области информационной безопасности написала одну из лучших книг о том, как найти дыры в любой операционной системе или приложении. В книге описываются методы написания шелл-кодов Windows, атаки на переполнение стека, а также нарушения корректного функционирования ядра открытых систем.

13. «OWASP TestingGuide v4»

OWASP (The Open Web Application Security Project) — открытый проект, объединяющий десятки компаний и специалистов, стремящихся сделать безопасность приложений более прозрачной, чтобы любой разработчик был в курсе потенциальных уязвимостей или слабых мест в его приложении.

OWASP Testing Guide — сборник статей от множества авторов, включающий «лучшие практики» для пентестов и описание техники тестирования в веб-приложениях и веб-сервисах.

14. А. А. Бирюков «Собираем устройства для тестов на проникновение» // ДМК-Пресс. 2018 - 378 с.

Многообразие и доступность различных недорогих аппаратных платформ, таких как Arduino, Raspberry Pi и др., простота их программирования, и при этом практически полное отсутствие средств защиты от них делают хакерские устройства мощным и опасным средством реализации компьютерных атак. В книге рассматриваются как теоретические основы информационной безопасности, так и практические аспекты создания собственных устройств с исходными кодами, схемами и примерами реализации. Также рассматриваются механизмы защиты от данного вида атак.

15. Брюс Шнайер «Прикладная криптография. Протоколы, алгоритмы и исходный код на С» // Диалектика. 2022 - 1040 с.

До появления настоящей монографии практикам приходилось тратить многие часы на поиск и изучение научной литературы, прежде чем они могли приступить к разработке криптографических приложений. Именно этот пробел восполняет книга "Прикладная криптография". Начав с целей засекречивания передачи данных и простейших примеров программ для достижения этих целей, Брюс Шнайер разворачивает перед читателем всю панораму практических результатов 20 лет исследований. В книге Брюса Шнайера "Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С(Си)" в деталях описаны принципы работы, реализации и примеры использования криптографических алгоритмов, является самой читаемой книгой по криптографии в мире!

16. Хабр «Фундаментальные законы информационной безопасности» // URL: https://habr.com/ru/post/325382/

17. Хабр «Системы классификации и оценки уязвимостей информационных систем» // URL: https://habr.com/ru/company/bastion/blog/706884/

В статье рассказывается о видах уязвимостей, где они появляются и как их классифицировать

18. Хабр «Разбор вредоносных файлов APT Kimsuky» // URL: https://habr.com/ru/company/rvision/blog/706046/

В статье показан процесс анализа вредоносного ПО на основе реальных сэмплов, используемых APT-группировками

19. Хабр «Лучшие практики безопасности Node.js» // URL: https://habr.com/ru/company/otus/blog/706000/

В статье перечислены различных угрозы для приложений, написанных на Node.js, их описание и способы устранения

20. Хабр «Тестирование Wi-Fi и ананасы из Китая» // URL: https://habr.com/ru/company/gaz-is/blog/687696/

В статье описывается процесс простого пентеста Wi-Fi и исследование устройства под названием Pineaplle. Pineapple (или, пайнеп) используется для различных атак на Wi-Fi сети.

Анализ состояния изученной проблемы:

Информационная безопасность - перспективная область, включающее в себя множество различных направлений, таких как форензика (расследование кибер инцидентов), тестирование на проникновение (пентест), аудит безопасности, мониторинг ИБ системы (SOC - security operation center) и др. Но в каждом из этих направлений необходимо разбираться в базовых вещах, таких как криптография, ОС и сети. В эпоху ежедневных взломов систем и приложений рассматриваемая область ещё надолго останется востребованной.