

С КАКИХ КНИГ НАЧАТЬ СВОЮ КАРЬЕРНУЮ ПУТЬ АНАЛИТИКА SOC?

*Учитесь и читайте. Читайте
книги серьезные. Жизнь
сделает остальное.*

Достоевский Ф. М.

Часто студенты задают вопрос: “А что еще можно почитать, чтобы прокачать свои знания в Blue Team?”.

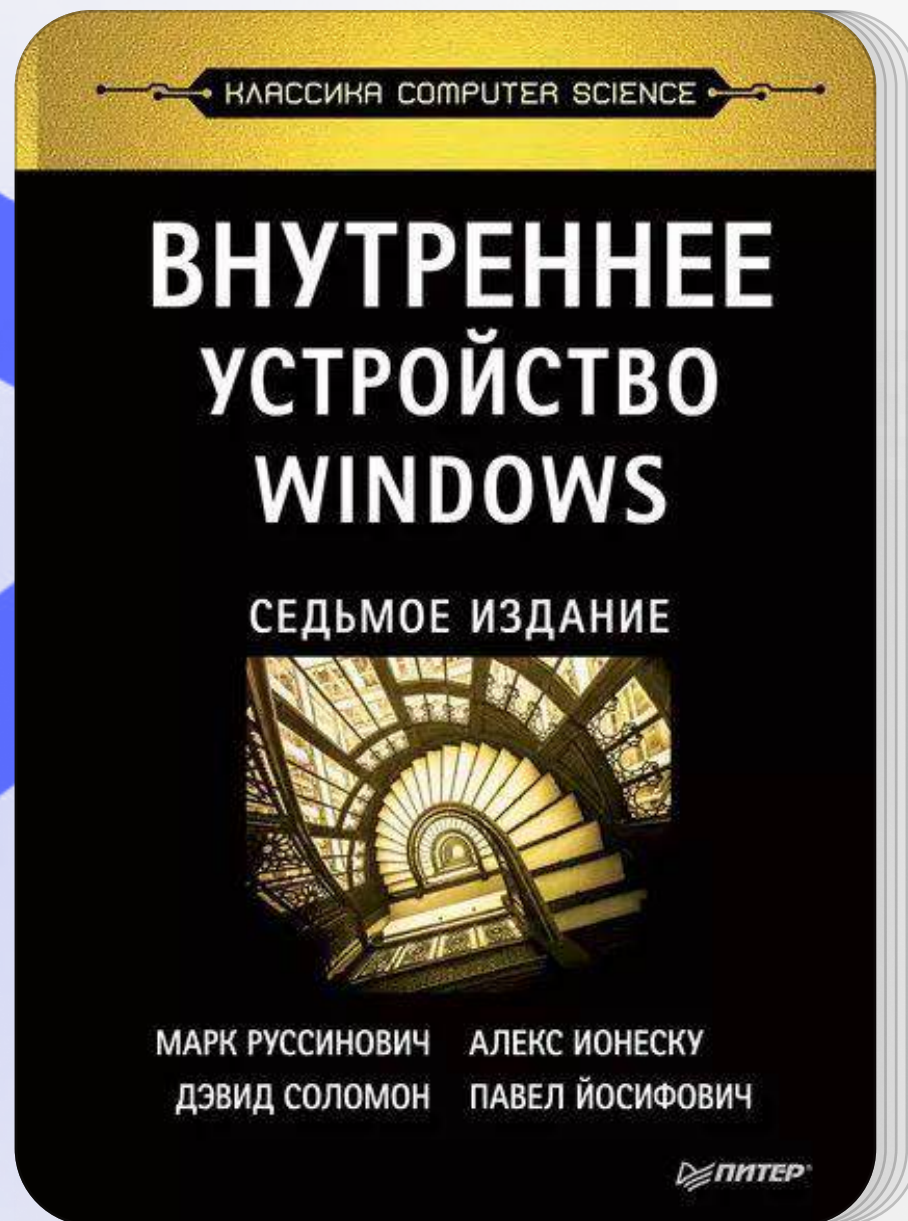
Действительно, существует очень много книг, статей и журналов на тему ИБ, поэтому выбрать с чего начать бывает непросто.

Ниже я описал несколько книг, которые на мой взгляд станут хорошей отправной точкой для освоения специальности.

ВНУТРЕННЕЕ УСТРОЙСТВО WINDOWS

М. РУССИНОВИЧ, Д. СОЛОМОН,
А. ИОНЕСКУ, П. ЙОЗИФОВИЧ

CyberED



Настольная книга всех, кто имеет дело с ОС Windows.

Оба тома описывают все, что нужно знать об этой операционке не только аналитику SOC, но и любому, кто взаимодействует с ней по работе. Можно назвать её в каком-то смысле энциклопедией.

Подход к чтению может быть разным: если читать от корки до корки трудно, то можно выбирать интересные в данный момент темы.

WINDOWS 10 PAVEL YOSIFOVICH SYSTEM PROGRAMMING

CyberED

Книга послужит отличной стартовой точкой в более глубоком освоении ОС Windows.

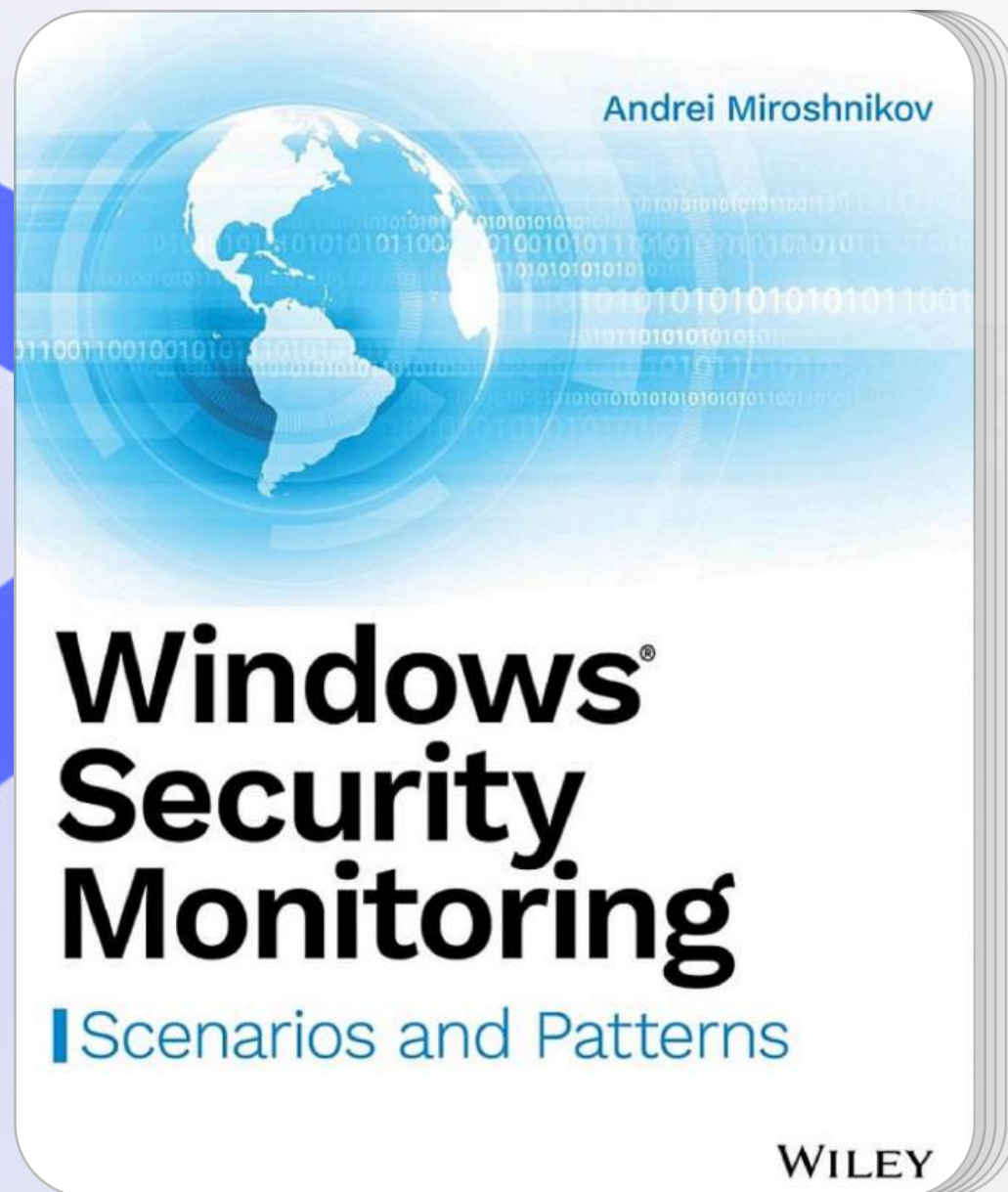
Практические примеры в этой книге позволят на собственном опыте узнать особенности операционной системы и работы с ней.



WINDOWS SECURITY MONITORING. SCENARIOS AND PATTERNS

CyberED

ANDREI MIROSHNIKOV



Из этой книги можно узнать многое о логировании в Windows: события, поля, настройка аудита и сценарии применения.

Поскольку знание и понимание логов очень важны для аналитиков SOC, рекомендую эту книгу к изучению.

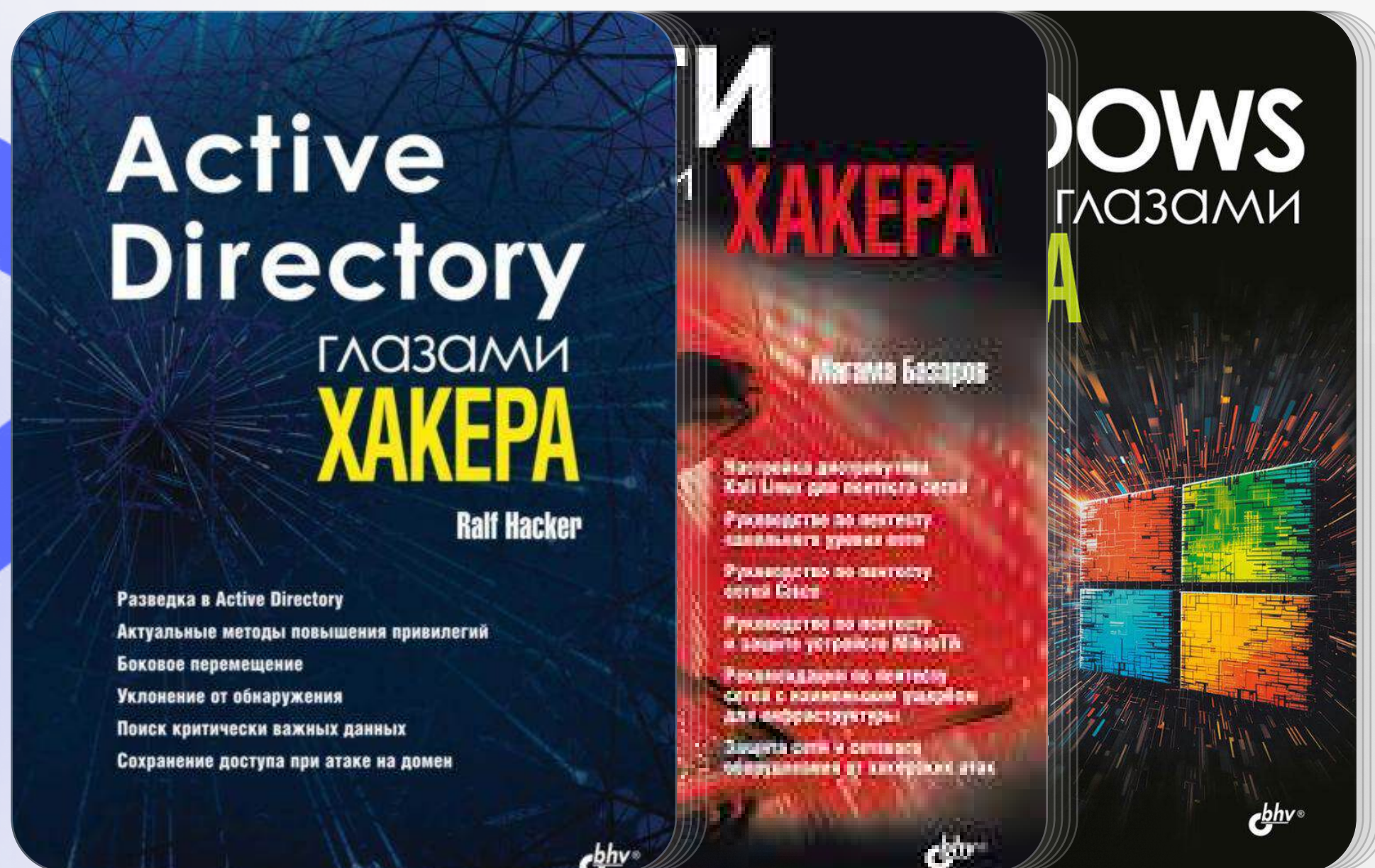
ОФИЦИАЛЬНОЕ РУКОВОДСТВО ПО ПОДГОТОВКЕ К СЕРТИФИКАЦИОННЫМ ЭКЗАМЕНАМ CISCO CCENT/CCNA ICND1 100–105

Из этой книги можно узнать многое о логировании в Windows: события, поля, настройка аудита и сценарии применения.

Поскольку знание и понимание логов очень важны для аналитиков SOC, рекомендую эту книгу к изучению.



СЕРИЯ КНИГ “ГЛАЗАМИ ХАКЕРА”



Сюда входят «Active Directory глазами хакера» Ralf’a Hacker’a, «Сети глазами хакера» Магамы Базарова и «Windows глазами хакера» Михаила Жмайло.

Замечательные книги, из которых можно почерпнуть знания и навыки в том как производятся атаки. Чтобы понимать как защищаться, необходимо сначала понимать от чего, то есть как происходит сама атака.

ВСКРЫТИЕ ПОКАЖЕТ!

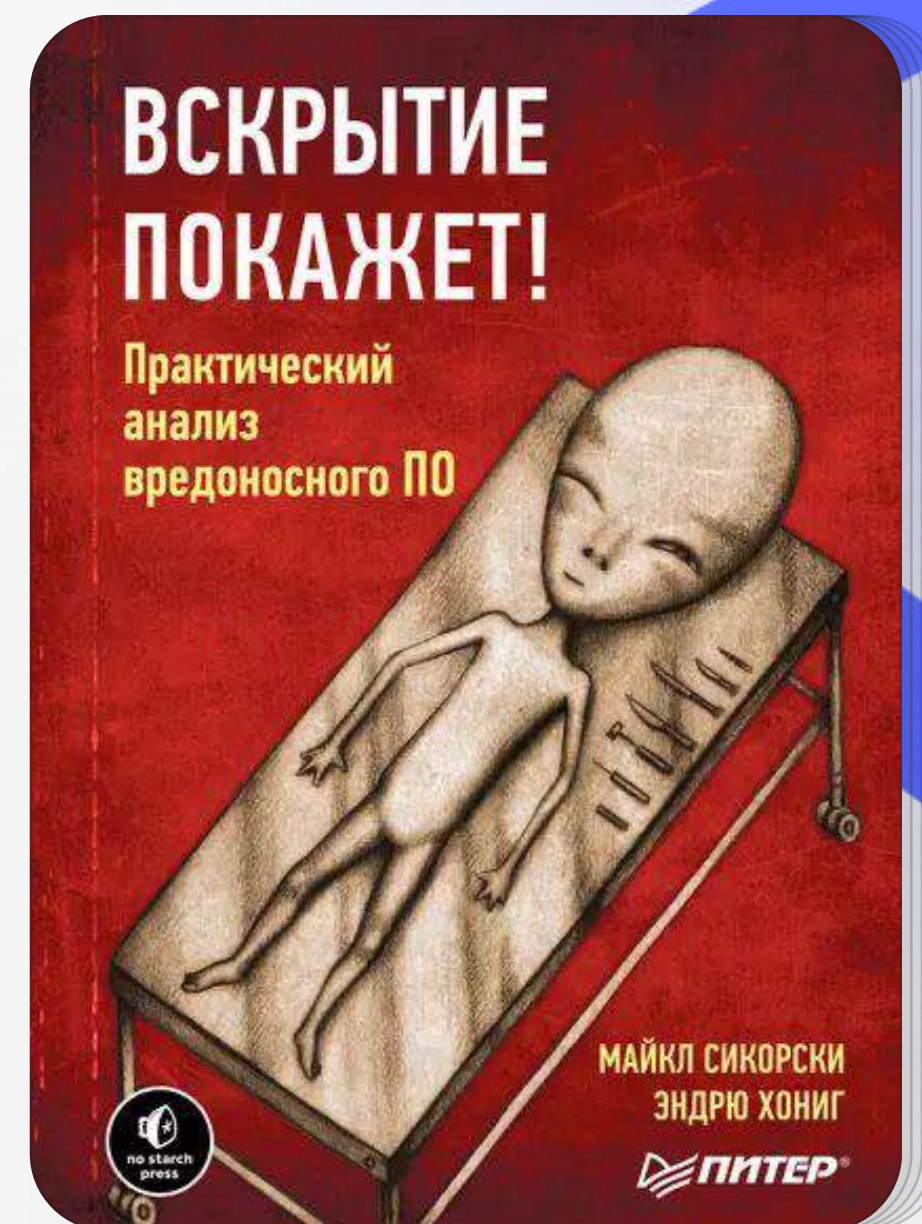
М. СИКОРСКИ

ПРАКТИЧЕСКИЙ АНАЛИЗ

ВРЕДОНОСНОГО ПО

В этой книге можно найти необходимые знания и навыки для того чтобы начать исследовать вредоносное ПО (реверс инжиниринг и malware analysis).

Книга написана понятным языком и без лишней «воды», так что подойдёт для изучения реверса даже если вы только начинаете.



ПОСТСКРИПТУМ

CyberED

Конечно, существует большое количество отличных книг, которые я не упомянул: «Идём по цифровому следу» Дмитрия Неверова, «Шифровальщики» Олега Скулкина, множество книг по разработке, сетям, ОС, реверсу, киберразведке и пр.

К сожалению, перечислить их все здесь нет возможности, однако рано или поздно вы встретите их на книжных полках полках или в подборках. Не судите о книге по обложке и развивайтесь, читая!