УДК 004.382
ББК 32.973-018
Э61

Энсон С.

Э61 Реагирование на компьютерные инциденты. Прикладной курс / пер. с англ. Д. А. Беликова. – М.: ДМК Пресс, 2021. – 436 с.: ил.

ISBN 978-5-97060-484-7

Эта книга написана практиками и для практиков, которым необходимо ежедневно выявлять действия злоумышленников в сетях и сдерживать кибератаки. Опираясь на свой опыт расследования вторжений, а также консультирования глобальных клиентов и разработки средств для цифровой криминалистики, автор предлагает наиболее эффективные методы борьбы с киберпреступниками.

Реагирование на инцидент информационной безопасности рассматривается в книге как непрерывный цикл, а не разовая процедура. Представлено несколько моделей реагирования на инциденты с учетом специфики современных киберугроз; обсуждаются меры по их предупреждению. В первой части речь идет о подготовке к реагированию на компьютерные атаки, затем подробно рассматриваются практические действия по обнаружению злоумышленника и устранению последствий взлома.

Подчеркивая, что хакерские тактики непрерывно обновляются, автор приводит ссылки на сторонние ресурсы, где можно найти самую свежую информацию по теме компьютерной безопасности.

УДК 004.382
ББК 32.973-018

ISBN 978-1-119-56026-5 (англ.)
ISBN 978-5-97060-484-7 (рус.)

Содержание