Федеральные законы, рекомендуемые к прочтению:

* ФЗ от 21.07.1993 №5485-1 «О государственной тайне»
* ФЗ №149 «Об информации, информационных технологиях и о защите информации»
* ФЗ №152 «О персональных данных»
* ФЗ №63 «Об электронной подписи»
* ФЗ №98 «О коммерческой тайне»
* Указ Президента №250

Информация – любые сведения вне зависимости от их представления.

SIEM – SIM (управление информацией о безопасности) + SEM (управление событиями безопасности) 🡪 Система управление событиями безопасности

DLP – Data Loss Prevention 🡪 Предотвращение утечек информации

IDS/IPS – IDS (Intrusion Detection System) + IPS (Intrusion Prevention System) 🡪 системы обнаружения и предотвращения вторжений

SOC – Security Operation Center 🡪 операционный центр безопасности

EDR – Endpoint Detection and Response 🡪 агентское решение для обнаружения, расследования и реагирования на сложные киберугрозы

VPN – Virtual Private Network 🡪 виртуальная частная сеть

WAF – Web Application Firewall 🡪межсетевой экран для веб-приложений, инструмент для фильтрации трафика, работающий на прикладном уровне.

Pentest – тестирование на проникновение и безопасность, анализ системы на наличие уязвимостей (моделирование кибератаки для выявления уязвимостей). Крупные компании должны проводить его не реже 3 раз в год.

Firewall – межсетевой экран 🡪 программный/программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

0-day (zero-day) – уязвимость нулевого дня, термин, обозначающий уязвимости и вредоносные программы, против которых ещё не разработаны защитные механизмы.