АСИЕ-ГРУПП

Как обеспечить информационную безопасность при ограниченных ресурсах — используя Open Source-решения

*как с минимальным бюджетом и ограниченными ресурсами построить эффективную систему защиты: закрыть ключевые векторы угроз

Основные векторы угроз

1. Вредоносное ПО (вирусы, трояны, шифровальщики)
2. Сетевые атаки (сканирование, вторжения, DDoS)
3. Утечки данных (внутренние/внешние каналы)
4. Несанкционированный доступ (привилегии, слабые пароли)
5. Несанкционированный доступ (привилегии, слабые пароли)

** При ограниченном бюджете важно сосредоточиться на наиболее вероятных и критичных векторах, чтобы не распыляться.*

Принципы построения ИБ при ограниченных ресурсах

1. Приоритет на критичные активы
2. Максимум автоматизации и удобства администрирования
3. Использование Open Source решений
4. Интеграция между инструментами
5. Постепенное развитие, не пытаться сразу охватить всё — начать с малого, расширяться.

NGFW IDS/IPS при ограниченных ресурсах

1. Класс решения: Межсетевой экран / UTM / IDS/IPS
   - OPNsense / pfSense — https://opnsense.org/
   - Suricata / Snort — https://suricata.io/
2. Векторы:
   - Защита периметра
   - Обнаружение вторжений
   - Контроль трафика
3. Пример настройки:

   https://habr.com/ru/companies/jetinfosystems/articles/732778/

DLP и контроль данных

1. Класс решения: DLP (Data Loss Prevention)

2. Решения:
   - OpenDLP — https://github.com/iknowjason/OpenDLP
   - MyDLP — https://sourceforge.net/projects/mydlp/

3. Векторы:
   - Предотвращение утечек данных
   - Контроль каналов передачи (почта, USB, сеть)

**Открытые DLP требуют адаптации под конкретную инфраструктуру.*

PAM (управление привилегиями)

1. Класс решения: PAM (Privileged Access Management)
   - HashiCorp Vault — https://www.vaultproject.io/
   - Teleport — https://goteleport.com/
2. Векторы:
   - Централизованное управление привилегиями
   - Аудит и контроль доступа
3. Пример применения
   - Vault для хранения API-токенов и паролей с разграничением ролей.

Антивирус и EDR

1. Класс решения: PAM (Privileged Access Management)
   - ClamAV — https://www.clamav.net/
   - OSSEC / Wazuh Agent
2. Векторы:
   - Обнаружение вредоносных файлов
   - Мониторинг активности на хостах
3. Пример:
   - ClamAV с почтовым шлюзом, интегрированный в Wazuh.

Резервное копирование и восстановление

1. Класс решения: Backup / Recovery

2. Решения:

   Restic — https://restic.net/

3. Векторы:

   - Защита от потери данных
   - Восстановление после атак

4. Пример настройки:

   - https://habr.com/ru/companies/selectel/articles/768014/
   - https://habr.com/en/articles/540096/

Организационные меры

Разработка политики безопасности

Обучение персонала

Регулярный аудит и тестирование

Разграничение прав доступа

**Эти меры не требуют больших инвестиций, но значительно повышают уровень ИБ.*

Пример комплексной схемы

Итоги

1. Можно построить зрелую систему ИБ без лицензий.

2. Open Source решения обеспечивают высокий уровень безопасности при грамотной настройке.

3. Главное — приоритет, дисциплина, постоянный контроль.