БЕЗОПАСНОСТЬ ПЛАТФОРМ ВИРТУАЛИЗАЦИИ:
КЛЮЧЕВЫЕ КРИТЕРИИ ПРИ ВЫБОРЕ

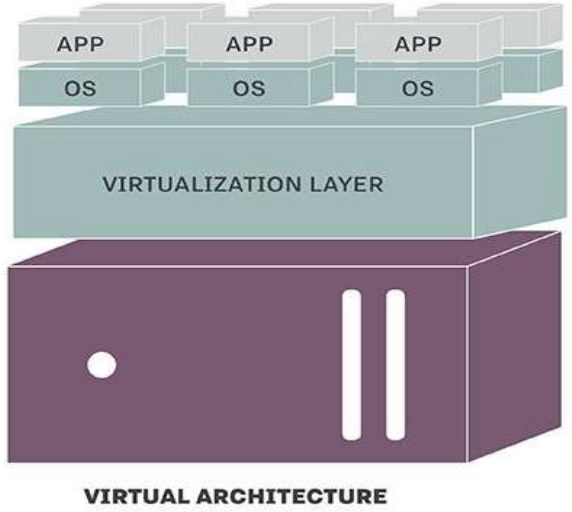
О СЕБЕ

МОЛОДЕНОВА АЛЕКСАНДРА

Руководитель направления архитектуры ИБ

СТОИТ ЛИ ЗАДУМЫВАТЬСЯ О БЕЗОПАСНОСТИ?

Сложность анализа



Высокий ущерб при наступлении риска

Рост количества уязвимостей

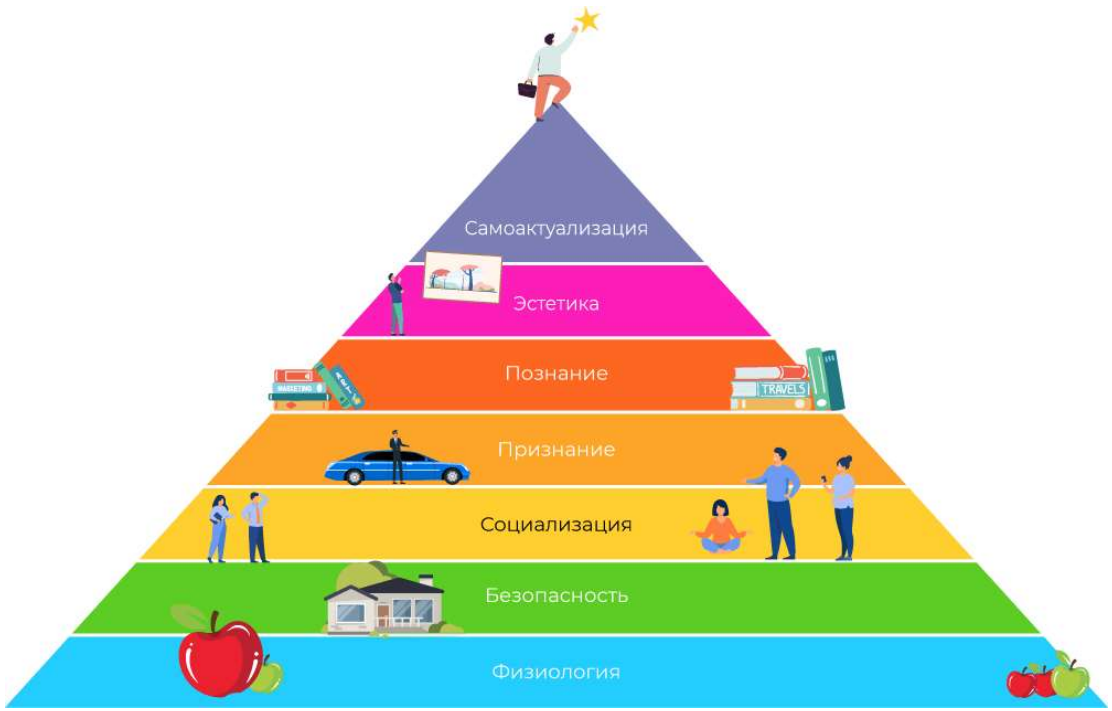
Search Results

There are **1262** CVE Records that match your search.

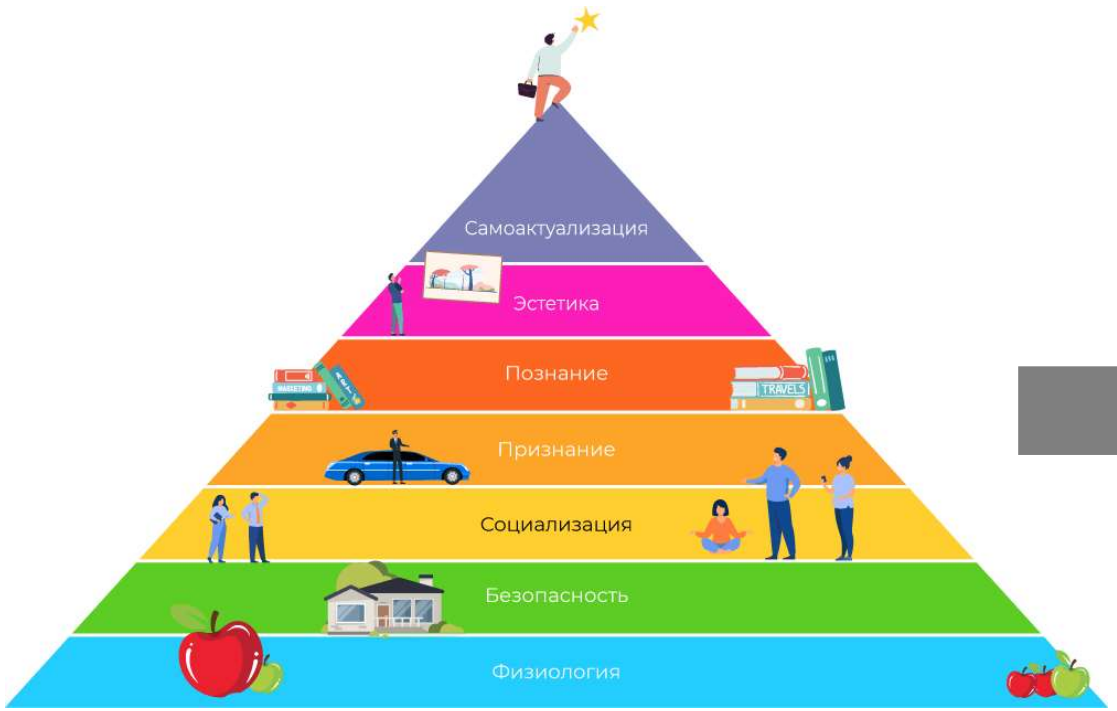
Name	
CVE-2025-22226	VMware ESXi, Workstation, and Fusion contain an information disclosure vuln process.
CVE-2025-22225	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with
CVE-2025-22224	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Us machine's VMX process running on the host.
CVE-2025-22222	VMware Aria Operations contains an information disclosure vulnerability. A ma
CVE-2025-22221	VMware Aria Operation for Logs contains a stored cross-site scripting vulnera delete action in the Agent Configuration.
CVE-2025-22220	VMware Aria Operations for Logs contains a privilege escalation vulnerability.
CVE-2025-22219	VMware Aria Operations for Logs contains a stored cross-site scripting vulner user.
CVE-2025-22218	VMware Aria Operations for Logs contains an information disclosure vulnerabi
CVE-2025-22217	Avi Load Balancer contains an unauthenticated blind SQL Injection vulnerabili specially crafted SQL queries to gain database access.
CVE-2025-22215	VMware Aria Automation contains a server-side request forgery (SSRF) vulne
CVE-2025-21862	In the Linux kernel, the following vulnerability has been resolved: drop_moni <none>/-1, .owner_cpu: 0 CPU: 1 PID: 7995 Comm: syz-executor.0 Tainted:

КЛЮЧЕВЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОДУКТОВ

«Потребности ИБ»



«Потребности ИБ»



«Потребности ИБ»

ВЕНДОРСКОЕ ИЛИ OPENSOURCE

- Юридическая защищенность
- Сертификация, внешние проверки
- Закрытость кода и документации

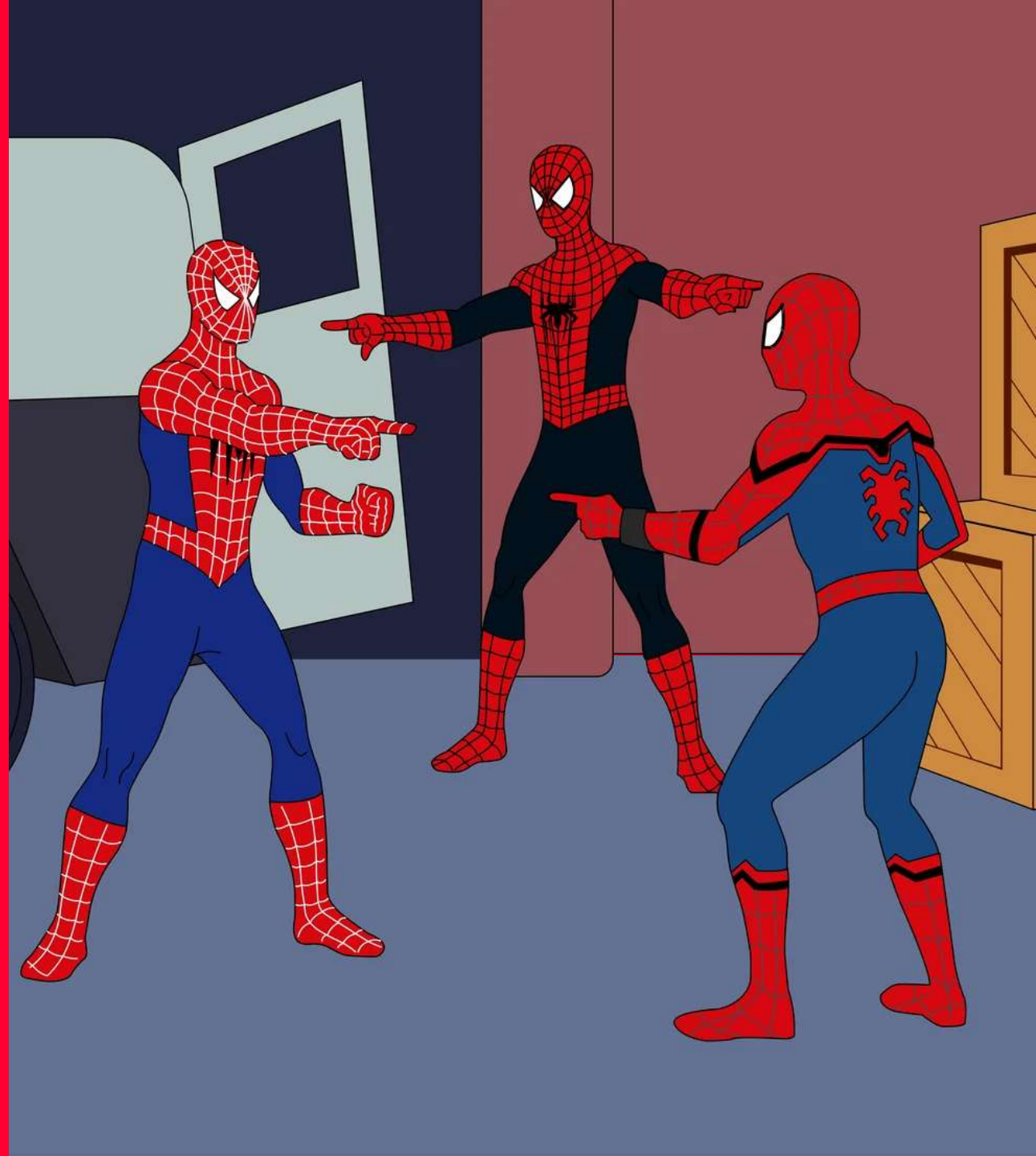
- Код открыт сообществу
- Возможность доработок под специфику ИС

ПРИ СОСТАВЛЕНИИ ТЗ УЧТЕМ И ПУНКТЫ ОТ ИБ

Четкая фиксация требований к продукту и зон ответственности за обеспечение безопасности ПО

ПРОРАБОТКА ПОТЕНЦИАЛЬНЫХ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОПРЕДЕЛЕНИЕ ЗОН ОТВЕТСТВЕННОСТИ, СРОКОВ УСТРАНЕНИЯ И КОМПЕНСАЦИОННЫХ МЕР

В том числе при выборе OpenSource



ШАБЛОН ТРЕБОВАНИЙ

- Возможность изоляции компонентов
- Поддержка ролевой модели доступов
- Аутентификация, авторизация, парольные политики
- Аудит и логирование, события ИБ
- Поддержка интеграции с СЗИ
- Сканирование компонентов
- Механизмы резервирования

КОНТАКТЫ

МОЛОДЕНОВА АЛЕКСАНДРА

Руководитель направления архитектуры ИБ
@solinenarany