

Шамиль Ичакаев

Инженер по информационной безопасности (сетевая безопасность, NGFW)

Москва, удалённо · Telegram: @shvmqa (t.me/shvmqa) · Телефон: +7 (926) 999-93-86

О СЕБЕ

Инженер по информационной безопасности с фокусом на сетевую и инфраструктурную защиту. В компании внедрил и администрирую шесть систем защиты: межсетевой экран нового поколения PT NGFW с интеграцией в Active Directory, WAF на базе ModSecurity с OWASP CRS, SIEM на базе Wazuh, EDR и антивирусную защиту на 254 хоста, облачную Anti-DDoS-защиту Qrator и собственную DLP-платформу. Спроектировал DMZ, перевёл маршрутизацию между VLAN на L3-коммутатор Cisco, разработал PoC защищённого удалённого доступа (IPsec IKEv2 / SSL VPN), политику ИБ и обучение сотрудников в LMS. Разработал коммерческий VPN-сервис на Xray-core: 11 серверов в 8 странах.

КЛЮЧЕВЫЕ НАВЫКИ

Сетевая безопасность: NGFW (PT NGFW), межсетевые экраны, WAF (ModSecurity, OWASP CRS), IDS/IPS, Anti-DDoS (Qrator), VPN (IPsec IKEv2, SSL VPN), DMZ, сегментация сети, коммутаторы Cisco (L3), маршрутизация между VLAN, VLAN, TCP/IP

Доступ и PKI: Active Directory, LDAP, strongSwan, PKI, SSL/TLS, разграничение доступа (RBAC)

Мониторинг и анализ: SIEM (Wazuh), CEF, Syslog, Grafana, Prometheus, Nmap, Wireshark

Защита рабочих мест и данных: EDR, антивирусная защита, DLP, контроль съёмных носителей, TLS-инспекция, цифровые отпечатки документов

Разработка: Python, FastAPI, SQLAlchemy, PostgreSQL, Redis, React, TypeScript, pytest

Инфраструктура: Linux, Docker, Docker Compose, nginx, Caddy, HAProxy, Xray-core, ufw, fail2ban, Bash

ОПЫТ РАБОТЫ

ООО «ЮНИПРО» — Специалист по информационной безопасности

Июль 2025 — настоящее время

Отвечаю за сетевую и инфраструктурную безопасность компании: аудит, внедрение и сопровождение средств защиты информации (СЗИ), сегментация сети, удалённый доступ, защита данных.

- Провёл аудит инфраструктуры и текущего состояния ИБ, выявил ключевые технические риски, сформировал и согласовал с руководством квартальный план изменений по периметру, удалённому доступу и сегментации сети.
- Разработал политику информационной безопасности компании и внедрил LMS для обучения сотрудников: обязательное ознакомление с требованиями ИБ и тестирование знаний, материалы по цифровой гигиене.
- Обосновал потребность и внедрил PT NGFW (Positive Technologies) с нуля: требования, архитектура интеграции с Active Directory, компактная политика из 28 правил на основе групп AD, журналирование, контроль приложений и URL-фильтрация; администрирую в продуктиве.
- Внедрил WAF на базе ModSecurity с OWASP CRS для защиты внутренних веб-сервисов, опубликованных наружу: подключил приложения, настроил правила и исключения под легитимный трафик, чтобы убрать ложные срабатывания; администрирую в продуктиве.
- Развернул SIEM на базе Wazuh: централизованный сбор и анализ событий безопасности, включая инциденты DLP-платформы, оповещения о подозрительной активности; сопровождаю и разбираю события.
- Внедрил EDR и антивирусную защиту на 254 хоста (рабочие станции и серверы): развёртывание агентов, политики защиты, централизованное управление; администрирую и разбираю срабатывания.
- Подключил облачную защиту от DDoS-атак Qrator для внешних сервисов компании: перевёл публичные ресурсы под фильтрацию и закрыл прямой доступ к серверам в обход защиты (входящий трафик — только с адресов Qrator).
- Спроектировал и внедрил DMZ-сегмент, изолировав внешние сервисы от внутренней сети: снизил риск несанкционированного доступа и сделал межсегментное взаимодействие управляемым.
- Перевёл терминирование трафика на L3-коммутатор Cisco: шлюзы сегментов и маршрутизация между VLAN на ядре сети; настраиваю и администрирую коммутаторы Cisco (VLAN, транки, порты доступа).

- Заменял небезопасную схему удалённого доступа: разработал и протестировал PoC защищённого подключения (IPsec IKEv2 на strongSwan с собственной PKI, SSL VPN) с разграничением доступа по группам AD.
- Разработал собственную DLP-платформу и вывел её в прод: контроль USB, веб-загрузок, облачных папок и мессенджеров на рабочих станциях, детектирование персональных данных и секретов, политики и расследование инцидентов.
- Автоматизировал инвентаризацию поверхности атаки: Nmap → нормализация → SQLite → Grafana, развёртывание через Docker Compose; сравнение сканов сократилось примерно с 3 часов ручной работы до 15 минут.

ПРОЕКТЫ

DLP-платформа (2026, собственная разработка) — система предотвращения утечек для парка Windows-рабочих станций: сервер политик и инцидентов (Python, FastAPI, PostgreSQL), консоль безопасности (React, TypeScript), Windows-агент и браузерное расширение Manifest V3.

- Каналы: USB и съёмные носители, загрузки и веб-формы в браузере (расширение + локальный TLS-прокси), облачные папки, мессенджеры.
- Детектирование: ПДн РФ (паспорт, СНИЛС, ИНН, банковские реквизиты, карты с проверкой Луна), секреты и ключи, цифровые отпечатки документов, OCR.
- Политики с режимами block / monitor / audit и симуляцией; инциденты со скриншотом и теневой копией файла; интеграция с SIEM (Wazuh, CEF) и AD/LDAP.
- Защита агента: обновления с проверкой подписи Authenticode и canary-раскаткой, пиннинг TLS-сертификата сервера, watchdog и защита службы от остановки; журнал аудита с SHA-256-цепочкой.
- Около 5 900 автотестов (pytest), 80 миграций БД. Разработано с применением AI-ассистированной разработки (Claude Code).

VPN-сервис (2026, разработка коммерческого проекта) — разработал сервис: инфраструктура из 11 серверов в 8 странах под управлением панели Remnawave, Telegram-бот для продаж (Python, aiogram 3) и веб-кабинет.

- Xray-core: VLESS + REALITY, транспорты XHTTP, WebSocket, gRPC; CDN-фронтинг и L4-релеи на HAProxy; выбор узла по сети клиента.
- Безопасность: проверка платёжных вебхуков, rate limiting на Redis, 2FA (TOTP), шифрование секретов AES-256-GCM, ufw и fail2ban, собственный anti-DDoS слой (iptables).
- Надёжность: ежеминутная проверка каждого узла реальным клиентским конфигом с алертами в Telegram, почасовые зашифрованные бэкапы PostgreSQL; более 200 автотестов бота.

Attack Surface Inventory Pipeline — результаты сканирований Nmap приводятся к единой схеме (хосты, порты, сервисы, версии), история хранится в SQLite, сравнение сканов показывает новые, закрытые и изменённые сервисы, дашборды Grafana используются для triage; стек запускается через Docker Compose. Сравнение сканов — примерно 15 минут вместо 3 часов.

ОБРАЗОВАНИЕ

Дагестанский государственный технический университет, Махачкала — неоконченное высшее, 2026

Безопасность автоматизированных систем в сфере связи, информационных и коммуникационных технологий

КУРСЫ

2026 — PT Application Security, Positive Technologies

2025 — PT Data Security: инвентаризация, классификация и контроль данных, Positive Technologies

2024 — Информационная безопасность (полный курс), HackTheBox Academy: Linux Fundamentals, Bash Scripting и другие модули

2022 — Основы программирования на Python, Яндекс Лицей

ДОПОЛНИТЕЛЬНО

Формат: полная занятость, удалённо; возможна работа как самозанятый.

Языки: русский — родной.

Рекомендация: Павел, руководитель отдела информационных технологий ЮНИПРО — контакты по запросу.