РЕЗЮМЕ

Швець В’ячеслав Віталійович
Дата народження: 21.07.1999 р.н.
Адреса: м. Біла Церква, бул. Олександрійський, 131
Телефон: +38(067) 181 67 44
Ел. пошта: more.zgraf@gmail.com

ПРОФЕСІЙНИЙ ПРОФІЛЬ

Інженер-програміст та фахівець з інформаційної безпеки з експертизою у захисті критичної інфраструктури та державного сектору. Маю глибокий технічний бекграунд у системному адмініструванні (Linux/Windows), мережевій інженерії та початковий рівень в Low-level розробці (C++/C#, Reverse Engineering). Спеціалізуюсь на виявленні складних кіберзагроз, аналізі цільового шпигунського ПЗ (Forensics) та використанні OSINT-методик для превентивного захисту.

ТЕХНІЧНІ НАВИЧКИ

- **Системне Адміністрування:** Windows xp/7/10/11. Linux (Ubuntu Server, Oracle, CentOS, засновані на *.deb), AD, EntraID, MS-365,.
- **Кібербезпека та інформаційна розвідка:** OSINT Frameworks (Maltego, Shodan, Google Dorks), Wazuh, Security Onion, Kali Linux, Metasploit, CrackMapExec.
- **Аналіз ШПЗ:** Пошук та аналіз Targeted Malware/Spyware (ручний аналіз реєстру, автозавантаження, дампу пам'яті), робота з Trend Micro Apex One, Digital Guardian DLP, Fortigate.
- **Мережа та Фаєрволи:** Fortigate (FortiOS, IPS/IDS), Mikrotik, pfSense, DNS Cloudflare, TCP/IP, VPN (IPsec, OpenVPN, WireGuard, FortiVPN), аналіз трафіку (Wireshark).
- **Хмари та Сервери:** Azure (AD/Entra ID), MS365, Proxmox VE, VMware ESXi.
- **Програмування:** C++, Python (Security Automation), Assembler (x86 basics), SQL, Bash.

ПРОФЕСІЙНИЙ ДОСВІД

6. Державна служба України з безпеки на транспорті, м. Київ
(01.10.2025 р. – по нині)
Посада: Головний спеціаліст Відділу критичної інфраструктури Управління інформаційної безпеки

- **Поглиблений аналіз (Forensics) робочих станцій:** виявлення та нейтралізація таргетованого шкідливого ПЗ (spyware, rootkits), розробленого спеціально для атаки на держслужбовців, яке не детектується стандартними антивірусами.

- Використання інструментів **OSINT** для моніторингу витоків даних (Leaked Credentials) та збору Threat Intelligence інформації щодо активності хакерських груп.
- Впровадження політик **DLP** (Microsoft Purview, Digital Guardian) для запобігання витоку конфіденційної інформації.
- Управління DNS-зонами в **Cloudflare**, налаштування WAF-Fortigate правил.
- Взаємодія з **CERT-UA**: аналіз індикаторів компрометації (IoC) та реагування на кіберінциденти.
- **Побудова внутрішньої VPN-мережі** на базі **Fortigate** для безпечного віддаленого доступу.
- Адміністрування гібридної хмарної інфраструктури (**Azure AD**, **MS365**) та віртуалізації (**Proxmox**, **VMware**).
- Міграція VM з "хмари" на "землю"
- Налаштування мережевого екранування та сегментація мережі для захисту критичних вузлів.
- Моніторинг подій безпеки через SIEM (**Wazuh**, **Security Onion, Fortigate EMS**).

(09.01.2025 р. – 30.09.2025)
Посада: Провідний фахівець відділу адміністрування інформаційно-комунікаційних систем

- Налаштування локальної мережі в Територіальних органах
- Налаштування, конфігурація, підтримка ПК та оргтехніки

(06.02.2024 р. – 08.01.2025)
Посада: Головний спеціаліст Відділу інформаційної безпеки

- Управління інфраструктурою відкритих ключів (КЕП), контроль засобів криптографічного захисту.
- Проведення внутрішніх пентестів та сканування вразливостей (Vulnerability Assessment) за допомогою **Kali Linux**.
- Розробка інструкцій та навчання персоналу методам протидії фішингу та соціальній інженерії.

(12.05.2023 р. – 05.02.2024)
Посада: Провідний фахівець Відділу інформаційної безпеки

- Реагування на інциденти безпеки, аналіз підозрілих файлів та посилань.
- Адміністрування антивірусного захисту **Trend Micro, Fortigate**.
- Написання та впровадження КСЗІ.
- Налаштування мережевого шлюзу PfSense
- Локалізація, налаштування та обслуговування Fortimail.
- Адміністрування хмарної інфраструктури Azure
- Налаштування SIEM Wazuh

5. ТОВ «Бінотел», м. Київ
(01.08.2022 р. – 01.05.2023)
Посада: Програмний інженер

- Експертна підтримка VoIP-інфраструктури. Глибока діагностика SIP/RTP трафіку (**Wireshark**, tcpdump) на рівні пакетів.
- Налаштування мережевого обладнання клієнтів (**Mikrotik**) для проходження голосового трафіку (NAT, QoS).
- Вирішення аварійних та складних питань в роботі телефонії клієнтів.

- Написання конфігураційних файлів для інтеграції різних клієнтських систем (CRM, API, сервіс подачі показників з лічильників за допомогою IVR, тощо.) з SIP-сервером

4. ТОВ «КНАЙПА ПРО СЕРВІС», м. Київ
(01.11.2021 р. – 01.04.2022)
Посада: Програмний інженер

- Розгортання комплексних систем автоматизації (POS).
- Технічна підтримка клієнтів, та консультація працівників стосовно роботи касового/бухгалтерського/офіціантського ПЗ.
- Побудова захищених VPN-тунелів між філіями закладів.
- Адміністрування баз даних SQL, забезпечення резервного копіювання.
- Супровід клієнтських серверів на баз Windows Server 2003-2018

3. ТОВ «Бінотел», м. Київ
(01.09.2020 р. – 29.10.2021)
Посада: Програмний інженер

- Технічний супровід клієнтів хмарної АТС.
- Комунікація з клієнтами в телефонному режимі.
- Налаштування програмних та фізичних IP-телефонів

2. Навчальний центр «Перспектива», м. Київ
(27.06.2019 р. – 07.09.2020 р.)
Посада: Молодший системний адміністратор

- консультування працівників з питань використання комп'ютерів
- здійснення інсталяції, настроюванню й оптимізації системного програмного забезпечення, впровадження прикладних програм
- підключення й заміна зовнішніх обладнань, проведення тестування засобів обчислювальної техніки, забезпечення ведення комп'ютерних баз даних, проведення комп'ютерних антивірусних заходів
- адміністрування локальної обчислювальної мережі організації; усунення аварійних ситуацій, пов'язаних з ушкодженням програмного забезпечення й баз даних.
- Контроль графіку навчання, та уроків навчального центру

1. Магазин «Reima», м. Київ
(27.07.18 р. – 01.09.18 р.)
Посада: Касир торговельного залу

- ведення обліку грошових коштів
- оформлення первинних касових документів
- проведення розрахункових операцій через РРО
- ведення книги обліку розрахункових операцій та складання звітів про використання РРО
- ведення касової книги

ДОДАТКОВІ НАВИЧКИ ТА ПРОЕКТИ (REVERSE ENGINEERING & R&D)

Single Player Project (World of Warcraft Emulation)

- Розробка ядра сервера на **C++**.
- Написання аддонів та модулів ядра сервера на **LUA**.
- **Reverse Engineering:** Аналіз бінарних протоколів та структури пам'яті клієнта гри.
- Робота з MySQL та оптимізація високонавантажених систем.

Nexus Forever (WildStar Emulation)

- Розробка емулятора на **C# (.NET Core)**.
- Дослідження пропрієтарних алгоритмів шифрування та мережевої взаємодії.

Security Research

- **CrackMapExec:** Розробка модулів на **Python** для аудиту безпеки Active Directory.
- Практичний досвід використання відлагоджувачів (x64dbg, IDA Pro) для аналізу коду.

ОСВІТА

- **Магістр:** Білоцерківський національний аграрний університет (20.09.2024 – 31.12.2025). Спеціальність: Публічне управління та адміністрування.
- **Бакалавр:** НТУУ «Київський політехнічний інститут імені Ігоря Сікорського» (2016 - 2020). Спеціальність: Метрологія та інформаційно-вимірювальна техніка.

ОСОБИСТІ ЯКОСТІ

Аналітичний склад розуму, уважність до деталей (критично для форензіки), стресостійкість при реагуванні на інциденти, постійне самонавчання у сфері кібербезпеки.