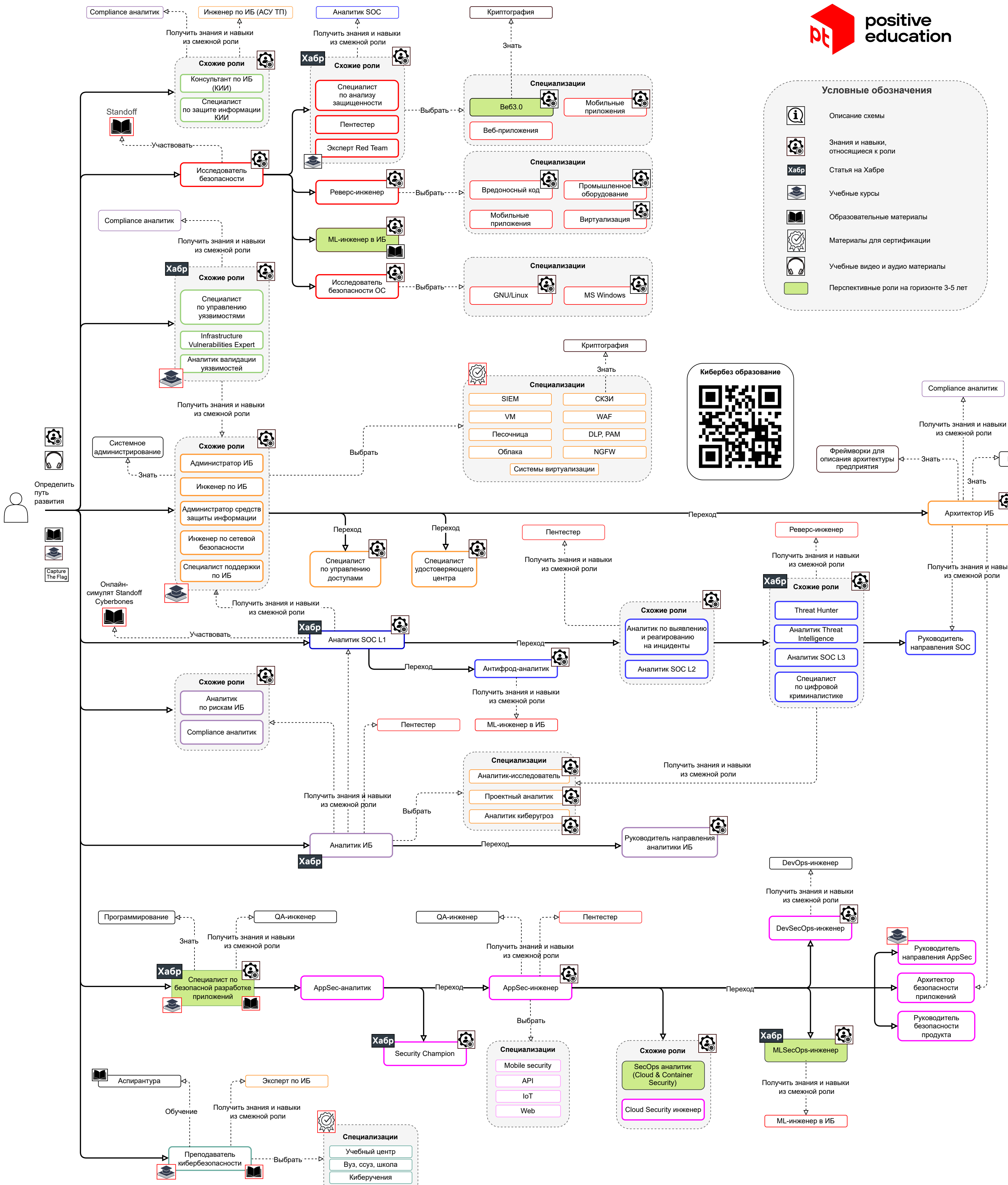


Схема карьерных треков в кибербезопасности

cybersecurity-roadmap.ru



Области компетенций в области кибербезопасности



Архитектура ПК	
Язык ассемблера	
x86	ARM MIPS AMD64

Операционные системы			
Управление учетными записями и привилегиями	MacOS	VMware vSphere	Hyper-V KVM
Администрирование	iOS	Виртуализация	Kubernetes
MS Windows	GNU/Linux	Android	Контейнеризация
Внутреннее устройство ОС	Системное программирование	Механизмы безопасности ОС	
Язык C	Механизмы аутентификации и авторизации	Анализ журналов событий	
Как работает переполнение			

Компьютерные сети			
Microsoft AD	GPO	DNS	DHCP
LDAP	tcpdump	Wireshark	VK Cloud
Принципы построения корпоративных сетей	Анализ сетевого трафика	Микросервисы	Облачные решения
Диагностика сетевых проблем	L2TP	IPSec	GRE
Стек протоколов TCP/IP (Модель OSI)	SOAP	SMB	NTPM
	Kerberos	SSH	HTTP(S)
			TLS/SSL

Автоматизация задач (программирование)			
Умение читать код на популярных языках	Python	C/C++	bash
Языки программирования	PowerShell	PowerShell	GitLab
Языки программирования	git	Docker	Terraform
Принципы разработки ПО	Ansible	Регулярные выражения	
Алгоритмическая сложность	ООП	Алгоритмы и структуры данных	SAST
			DAST
			O/S/SCA
			DevSecOps

Системы управления базами данных			
Механизмы безопасности	Управление учетными записями и привилегиями	Глубокое обучение	Типы атак
Администрирование	PostgreSQL	MSSQL	Oracle
MySQL	NoSQL	SQL	
Принципы разработки ПО	Алгоритмы и структуры данных	Безопасная разработка	
Алгоритмическая сложность	ООП	Алгоритмы и структуры данных	SAST
			DAST
			O/S/SCA
			DevSecOps

Практическая кибербезопасность			
Атаки по уровням модели OSI	YARA	Угроза	Экспloit
Поверхность атаки	Уязвимость	Риск	Аутентификация
Типы атак	Шифрование	Хеширование	PGP
	Криптографические примитивы и концепции	Volatility	Форензика
Этический хакинг	метasploit	Kali Linux	Атаки на беспроводные устройства
OWASP TOP 10	CWE Top 25	Байткод	IL
		Java	PE
		ELF	DEX
		IDA Pro	Ghidra
		Radare2	WinDbg
			gdb

Стандарты / методологии / фреймворки по ИБ			
ГОСТ Р 57580.1-2017	ГОСТ Р 57580.3-2022	PC БР ИББС 2.2	ISO 27001
ISO 27005	Результативная кибербезопасность (ПКБ)		
Методики управления рисками ИБ			
ISO/IEC 270XX	CobIT	PCI DSS	Модели угроз
152-ФЗ	MITRE ATT@CK	187-ФЗ	CyberKillChain
149-ФЗ	Zero Trust		
			ФСТЭК РФ 17, 21, 239

Средства защиты информации			
iptables	Suricata	Zeek	Snort
FW/NGFW	NTA	IDS/IPS	AV
Сканыеры безопасности	Управление уязвимостями	Метрики	Криптографические средства защиты информации
Nessus	MaxPatrol	Разновидности уязвимостей	Анализ журналов событий
nmap	Burp Suite	CVE	Облачные СЗИ
OpenVAS	ZAP	CWE / CVSS	БДУ ФСТЭК
		БДУ ФСТЭК	