КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

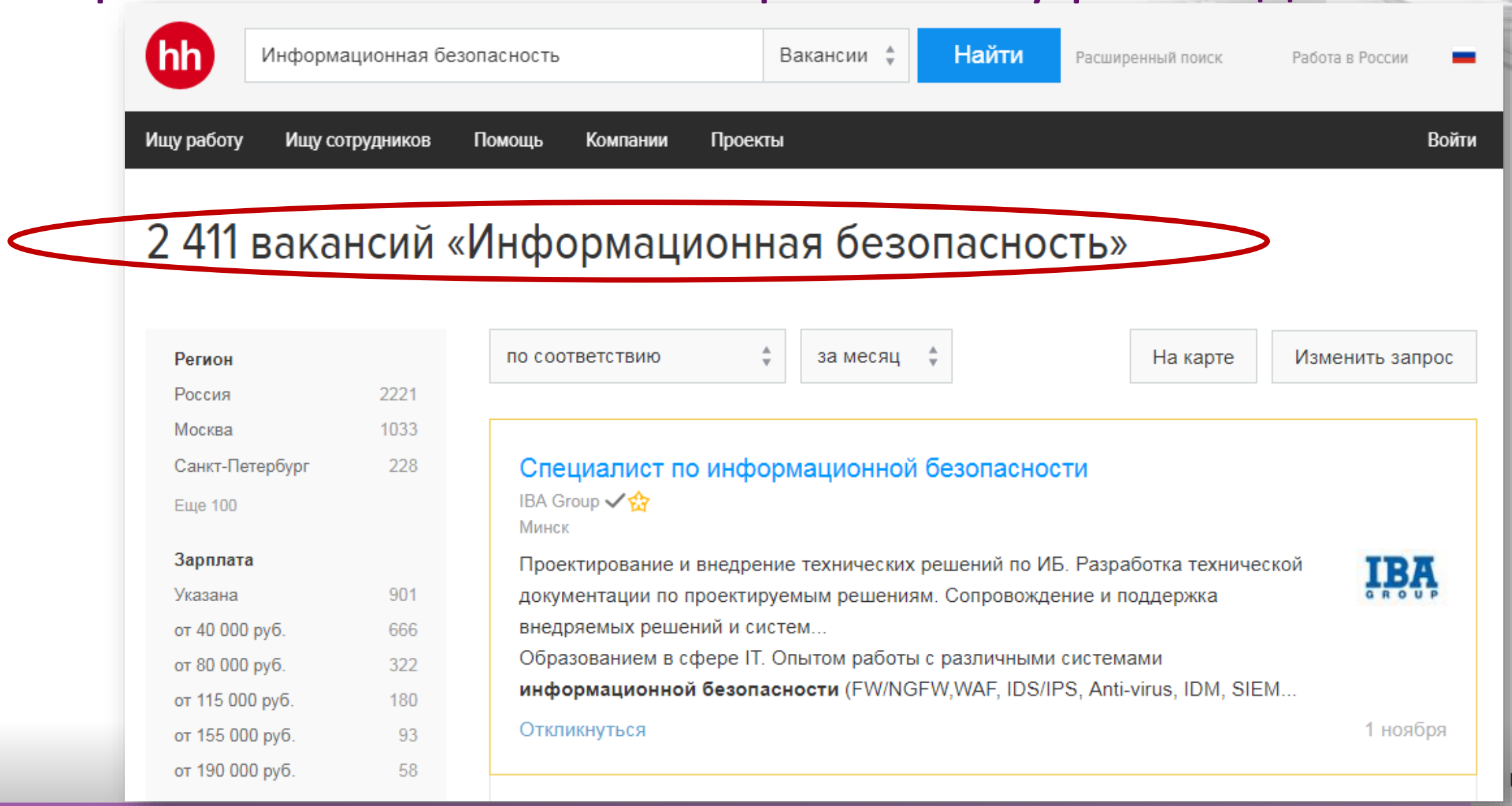
Информзащита
Учебный центр

Карьера безопасника – к чему стремиться и чему учиться?

Андрей Степаненко, директор
a.stepanenko@itsecurity.ru

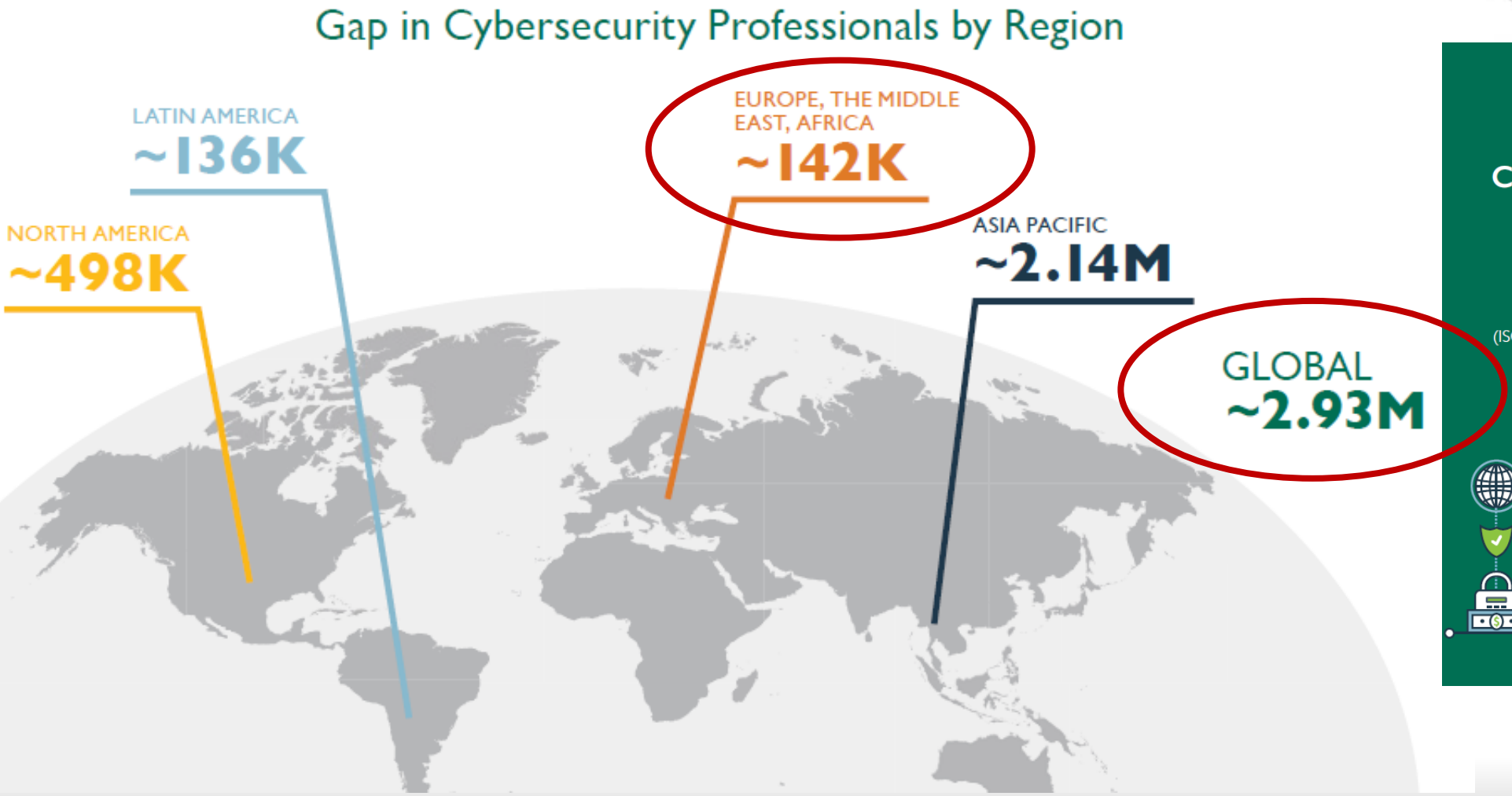
Нужны и мы вообще?

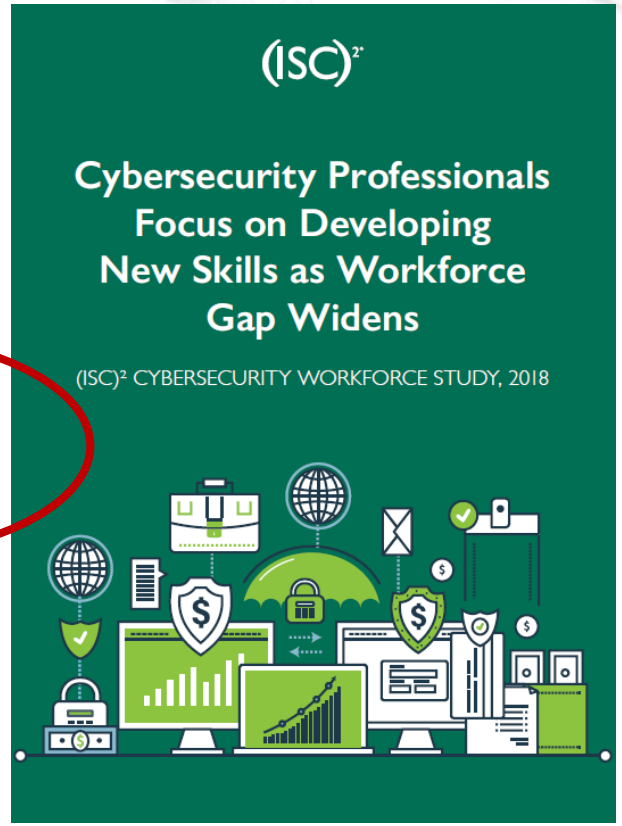
Хорошие новости: Есть потребности у работодателей



Информзащита
Учебный центр

Хорошие новости: Глобальный дефицит безопасников





Информзащита
Учебный центр

Оборотная сторона медали

Плохие новости: Много соискателей работы

hh | Информационная безопасность | Резюме | Найти | Расширенный поиск | Работа в России

Ищу работу | Ищу сотрудников | Помощь | Компании | Проекты | Войти

Найдено **141 458** соискателей с **158 159** резюме

Регион

Россия	140710
Москва	45621
Санкт-Петербург	17615

Еще 385

Профобласть

IT, телеком	65482
Безопасность	52355
Начало карьеры	12507

Еще 25

За весь период ▾ Сортировать по соответствию ▾ Изменить запрос

Руководитель подразделения по информационной безопасности

36 лет

Опыт работы

13 лет и 6 месяцев

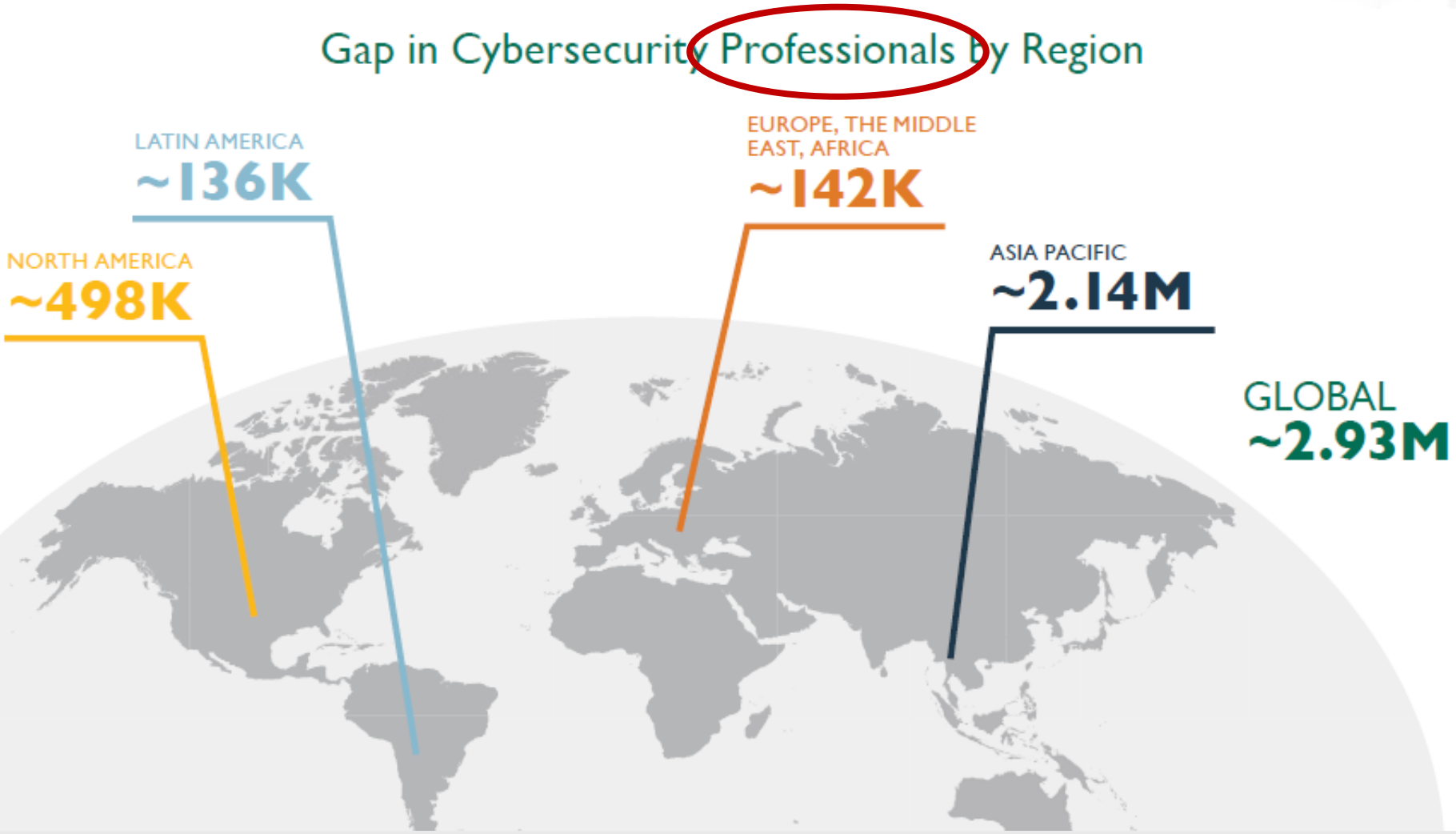
Последнее место работы

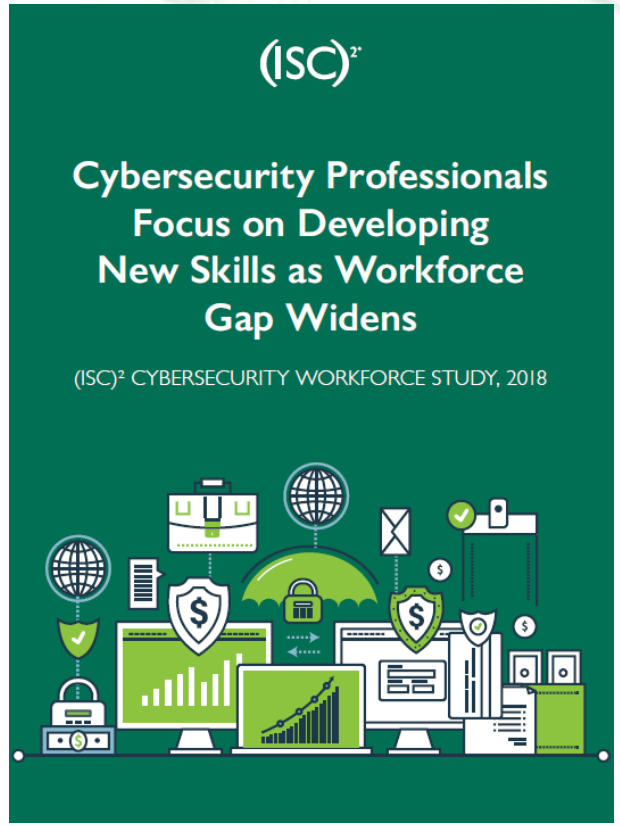
Начальник службы информационной безопасности,
iQ-Solutions, Июль 2016 — Декабрь 2017

Обновлено 6 ноября, 06:32

Информзащита
Учебный центр

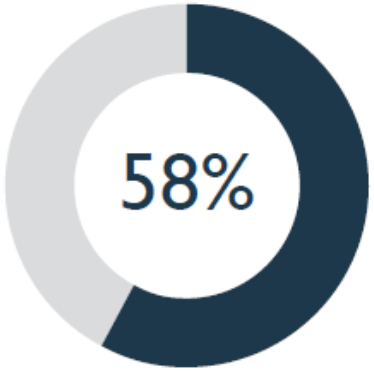
Плохие новости: Ложка дегтя – нужны профессионалы ☹





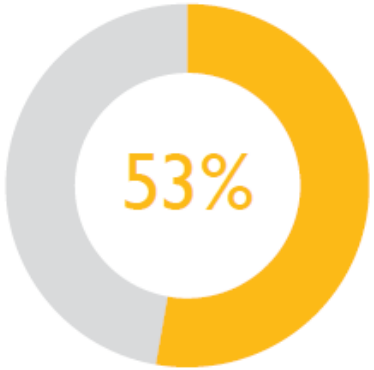
Информзащита
Учебный центр

Какие знания должны быть у **профессионала**?

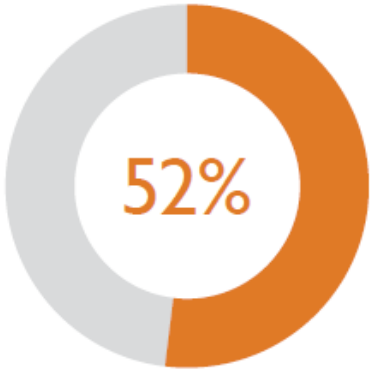


Security awareness

Risk assessment, analysis & management

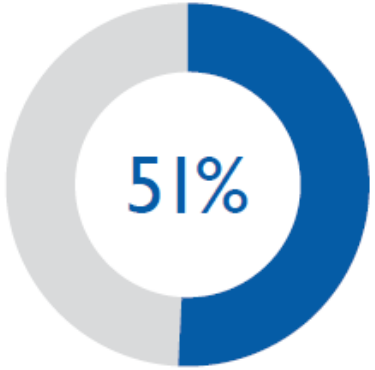


Security administration



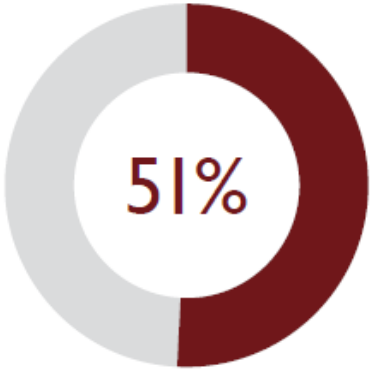
Network monitoring

Incident investigation and response

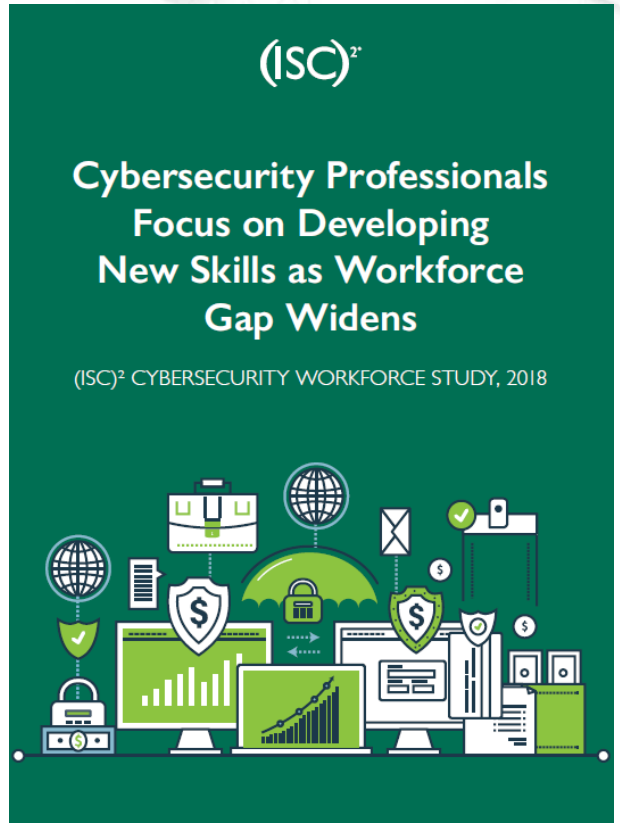


Intrusion detection

Cloud computing security



Security engineering



Процент отражает количество респондентов, назвавших конкретные знания «**Критически важными**»

Информзащита
Учебный центр

Типовые роли безопасников

- Руководитель
  - отвечает за организацию работ по созданию системы защиты и состояние безопасности
- Аналитик
  - отвечает за определение требований к защищенности и разработку необходимых НМД по вопросам защиты информации
- Аудитор
  - контролирует текущее состояние системы защиты на предмет соответствия ее заявленным целям
- Администратор средств защиты
  - отвечает за сопровождение штатных и дополнительных средств защиты
- Специалист по работе с конечными пользователями
  - отвечает за реализацию и контроль исполнения регламентов

Откуда берутся специалисты по ИБ

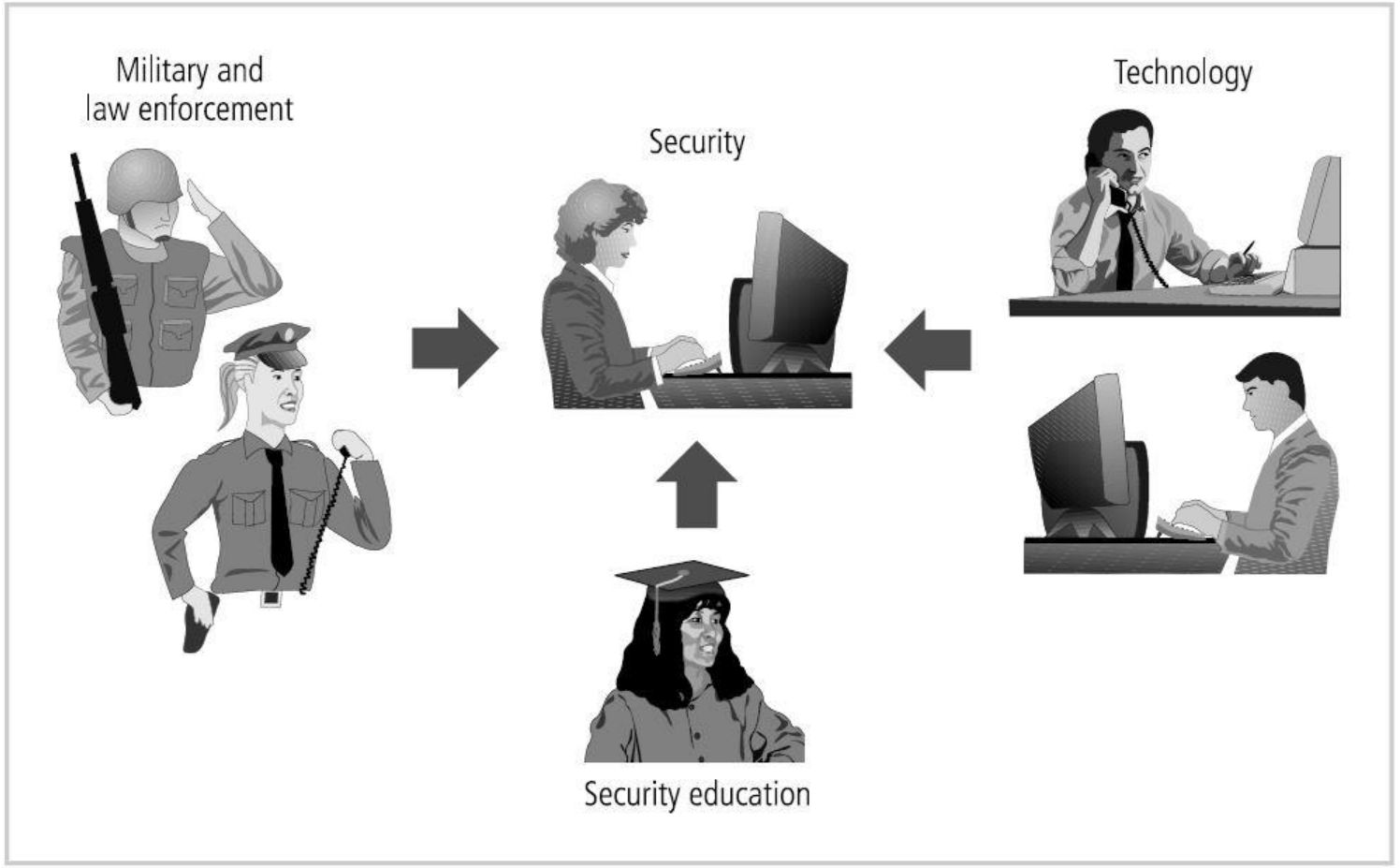
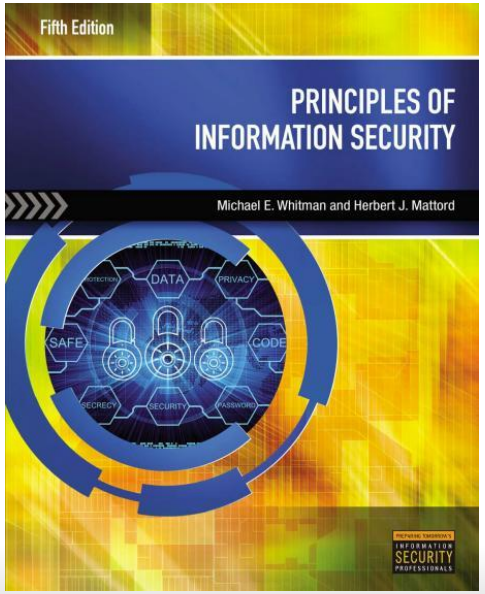


Figure 11-1 Career Paths to Information Security Positions

Иллюстрация из книги «Principles of Information Security»

M.Whitman, H.Mattord

1-е издание, 2003 г.



Информзащита
Учебный центр

Чему учат специализированные вузы

СПЕЦИАЛЬНОСТИ ВЫСШЕГО ОБРАЗОВАНИЯ – СПЕЦИАЛИТЕТА

- 2.10.05.01 Компьютерная безопасность
- 2.10.05.02 Информационная безопасность телекоммуникационных систем
- 2.10.05.03 Информационная безопасность автоматизированных систем
- 2.10.05.04 Информационно-аналитические системы безопасности
- 2.10.05.05 Безопасность ИТ в правоохранительной сфере
- 2.10.05.06 Криптография
- 2.10.05.07 Противодействие техническим разведкам

Общероссийский классификатор специальностей ОК 009-2016 (ОКСО)

Чему учат специализированные вузы

ОСНОВНЫЕ ДИСЦИПЛИНЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Основы информационной безопасности
- Организационное и правовое обеспечение информационной безопасности
- Криптографические методы защиты информации
- Техническая защита информации

Общие дисциплины из базовой части ФГОС 3+

Информзащита
Учебный центр

Чему учат специализированные вузы

ДОПОЛНИТЕЛЬНЫЕ ДИСЦИПЛИНЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Защита в операционных системах
- Основы построения защищенных баз данных
- Основы построения защищенных компьютерных сетей
- Разработка и эксплуатация автоматизированных систем в защищенном исполнении
- Управление информационной безопасностью

Чего хотят работодатели (пример вакансии с hh.ru)

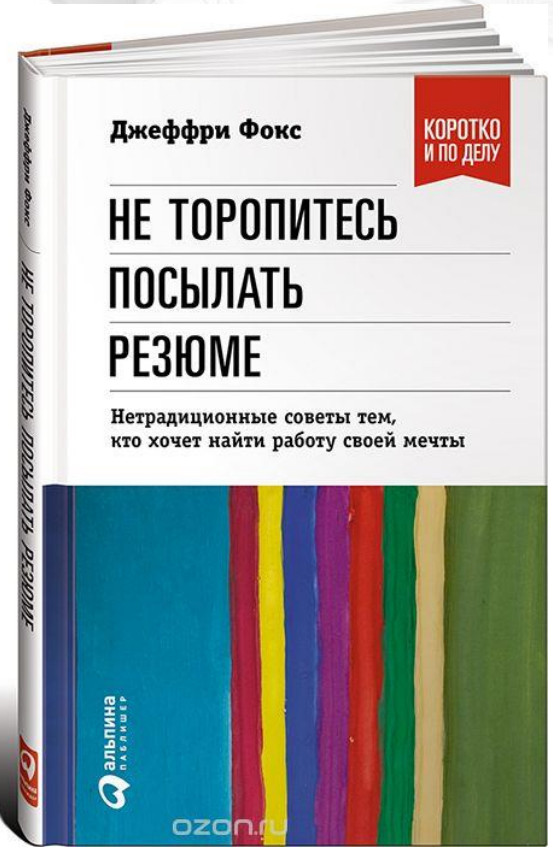
- Участие в реализации требований 382-П, комплекса стандартов СТО БР ИББС
- Разработка нормативных документов по информационной безопасности
- Проведение внутренних аудитов по ИБ
- Контроль соблюдения требований информационной безопасности
- Выявление и расследование инцидентов ИБ
- Проведение обучения и проверки знаний сотрудников по вопросам ИБ
- Эксплуатация системы выявления утечек информации
- Эксплуатация средств СКЗИ, защиты от вредоносного ПО
- Управление межсетевым экраном, ключевой инфраструктурой PKI

Чего хотят работодатели (пример вакансии с hh.ru)

- Анализ информационных рисков компании
- Выявление возможных каналов утечки
- Разработка организационно-распорядительных документов
- Организация и координация работ, проводимых в рамках обеспечения ИБ
- Проведение аудита состояния ИБ
- Установка, настройка и сопровождение технических средств защиты
- Защита локальных компьютерных сетей от вирусных атак и взломов

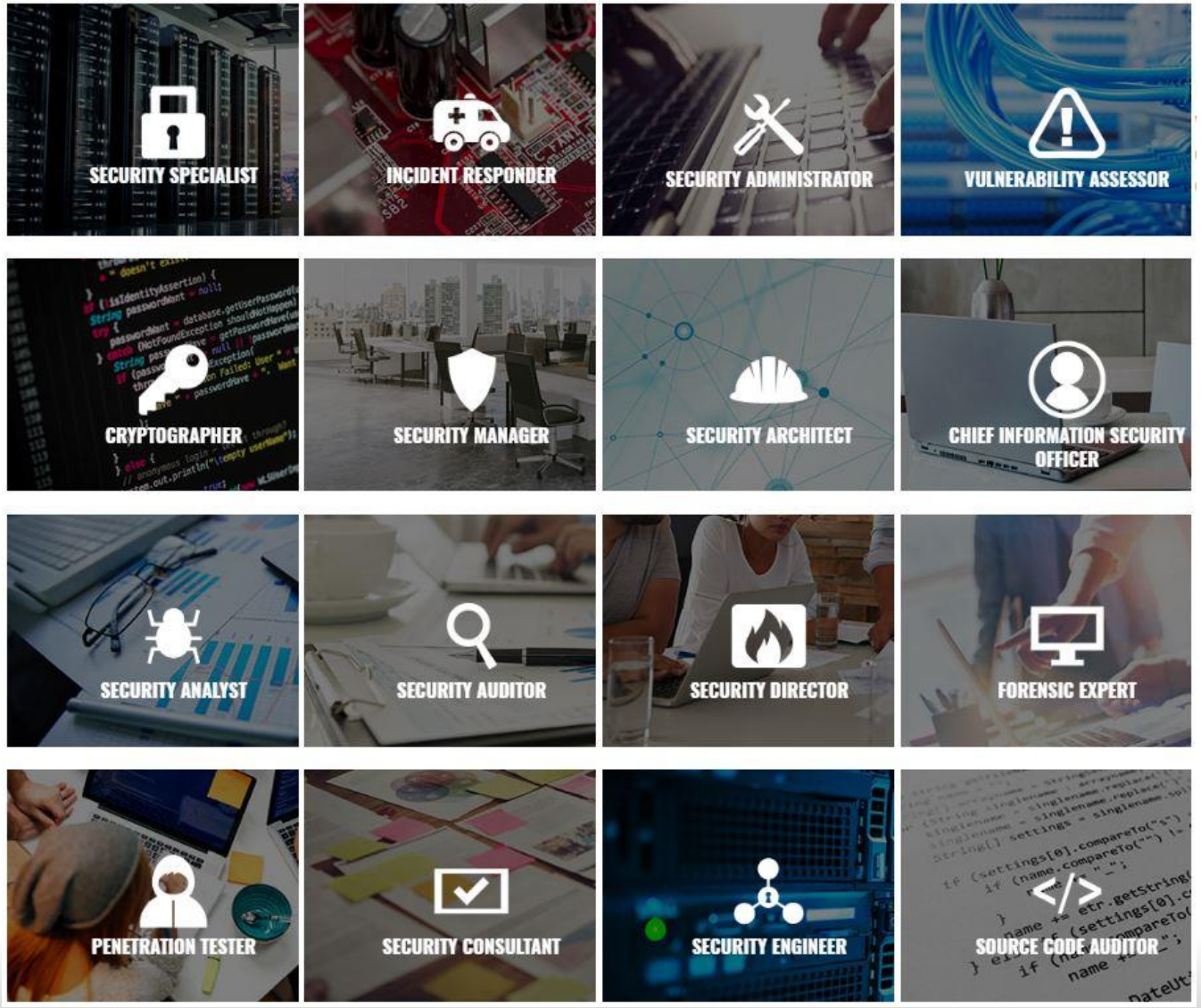
Пошаговая инструкция ☺

- Определить долгосрочную цель
- Трезво оценить свои текущие знания и умения
- Определить ближайшую цель
- Составить список недостающих знаний
- Начать учиться и набирать опыт
- По достижении ближайшей цели – повторить с начала ☺



Информзащита
Учебный центр

Интересные зарубежные ресурсы



CYBER SECURITY EDUCATION

www.cybersecurityeducation.org

Информзащита
Учебный центр

Почти готовый план ☺

HOW TO BECOME A SECURITY SPECIALIST

Everyone and most every thing needs some type of protection. You protect your home with locks or alarm systems; you protect your car with insurance, and you protect your health by going to the doctor. A major corporation or organization uses a security specialist to protect their software and network security system. A security specialist is smart career path to take to begin your career in cyber security, as you'll be the go-to person responsible for the overall safety of your employer's data.

CYBER SECURITY EDUCATION

Информзащита
Учебный центр

Следующие ступеньки

CAREER PATH AS A SECURITY SPECIALIST

Since a security specialist is essentially an entry level position in the large world of cyber security, there are positions you can start out in at first and then, you can work your way up the ladder into a management role. It is a great career to enter as there are several roads to travel toward executive-level roles.

CYBER SECURITY EDUCATION

Entry-Level	Senior-Level	Executive-Level
System Administrator	IT Project Manger	Chief Information Security Officer
Security Administrator	Security Manager	Security Director
Network Administrator	Security Consultant	
	Security Architect	

Информзащита
Учебный центр

Подсказки по требуемым знаниям

JOB REQUIREMENTS

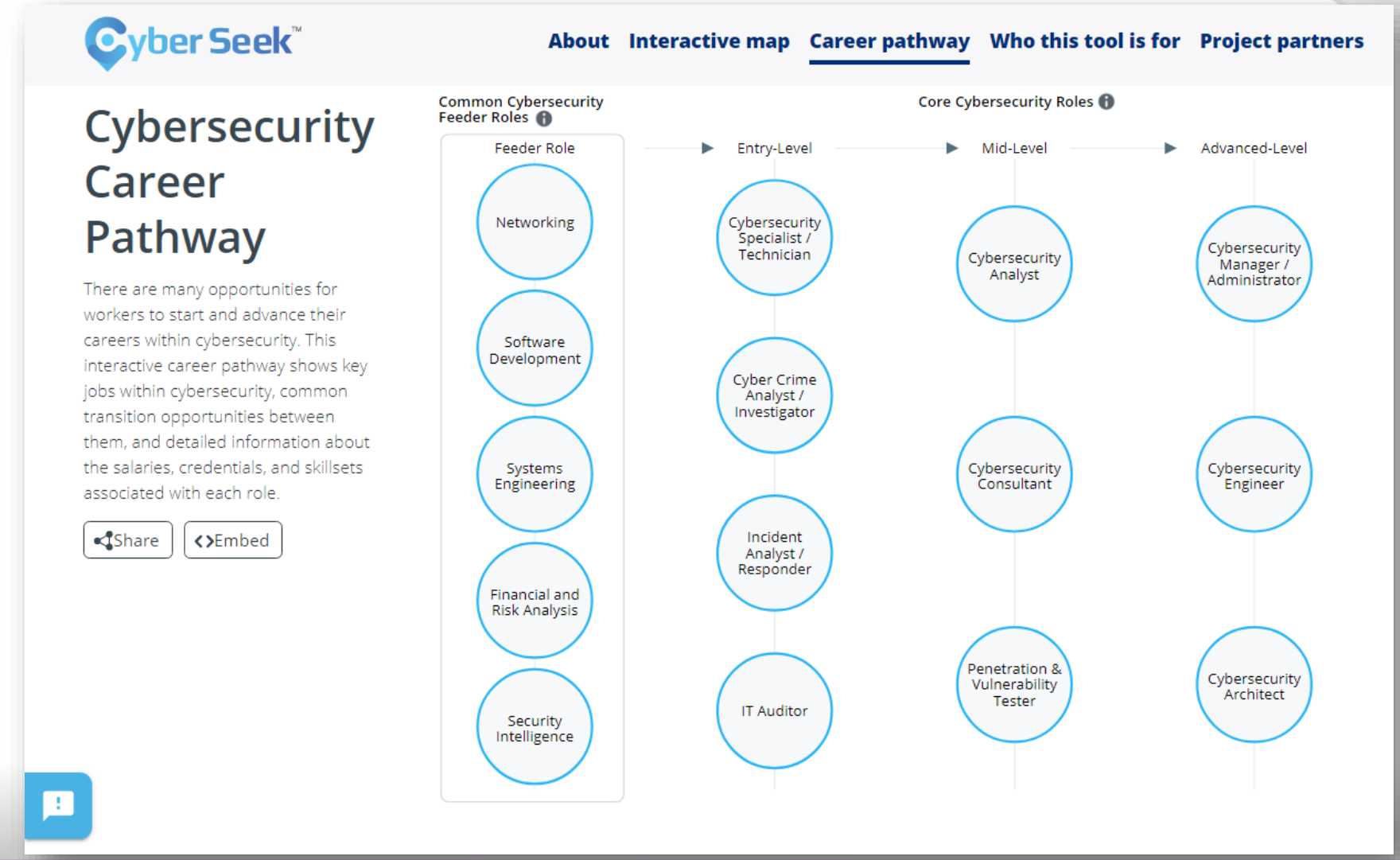
Hard Skills

- Knowledgeable in SIEM—Security Information and Event Management
- Ability to perform vulnerability and penetrations tests
- Understand computer protection programs and software such as anti-malware, anti-virus and firewall
- Fluent in programming languages like PHP, Java, C++, C# or C
- Comfortable working with UNIX, Windows, and Linux systems
- Confident in threat modeling, coding practices and ethical hacking
- Understanding of Load Balancer, Proxy Server and Packet Shaper

CYBER SECURITY EDUCATION

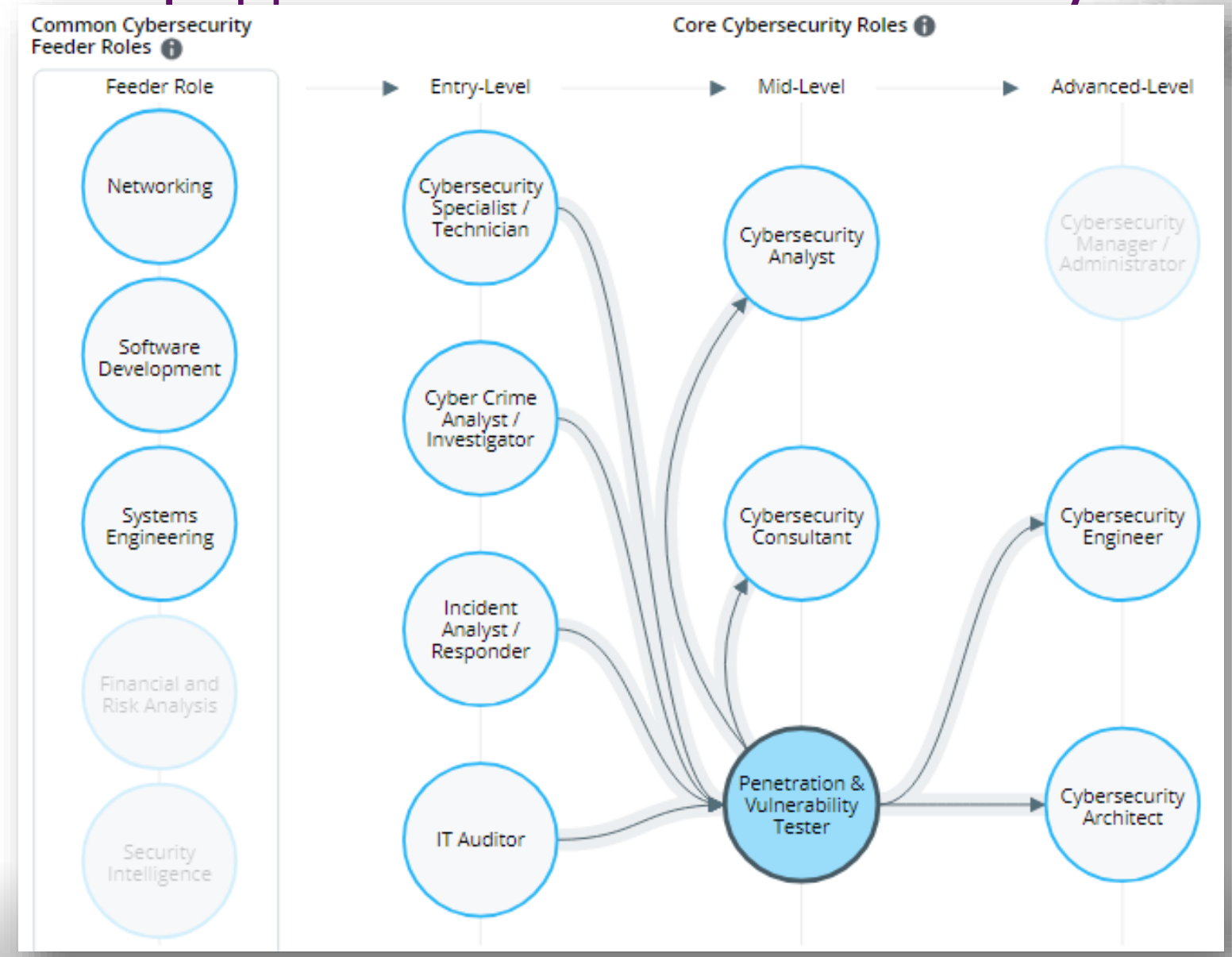
Информзащита
Учебный центр

Хороший ресурс для планирования карьеры www.cyberseek.org



Информзащита
Учебный центр

Наглядное представление возможных путей



Информзащита
Учебный центр

Дополнительная информация для планирования

Penetration & Vulnerability Tester

AVERAGE SALARY

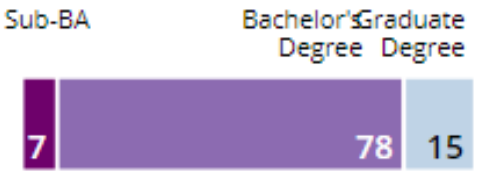
$97,000

Penetration & Vulnerability Tester

COMMON JOB TITLES

- Application Security Engineer
- Penetration Tester
- Security Analyst II
- Application Security Architect
- Application Security Analyst

REQUESTED EDUCATION (%)



TOP SKILLS REQUESTED

1. Information Security
2. LINUX
3. JAVA
4. Python
5. Information Systems
6. UNIX
7. Scanners
8. Software Development
9. SQL

TOTAL JOB OPENINGS

10,929

Penetration & Vulnerability Tester

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

- Analyze
- Protect and Defend

TOP CERTIFICATIONS REQUESTED

- GIAC
- CISA
- CISM
- Cisco Certified Network Associate
- Certified Ethical Hacker

Информзащита
Учебный центр

Что еще может быть полезно для карьеры

Информзащита
Учебный центр

Чему нужно учиться

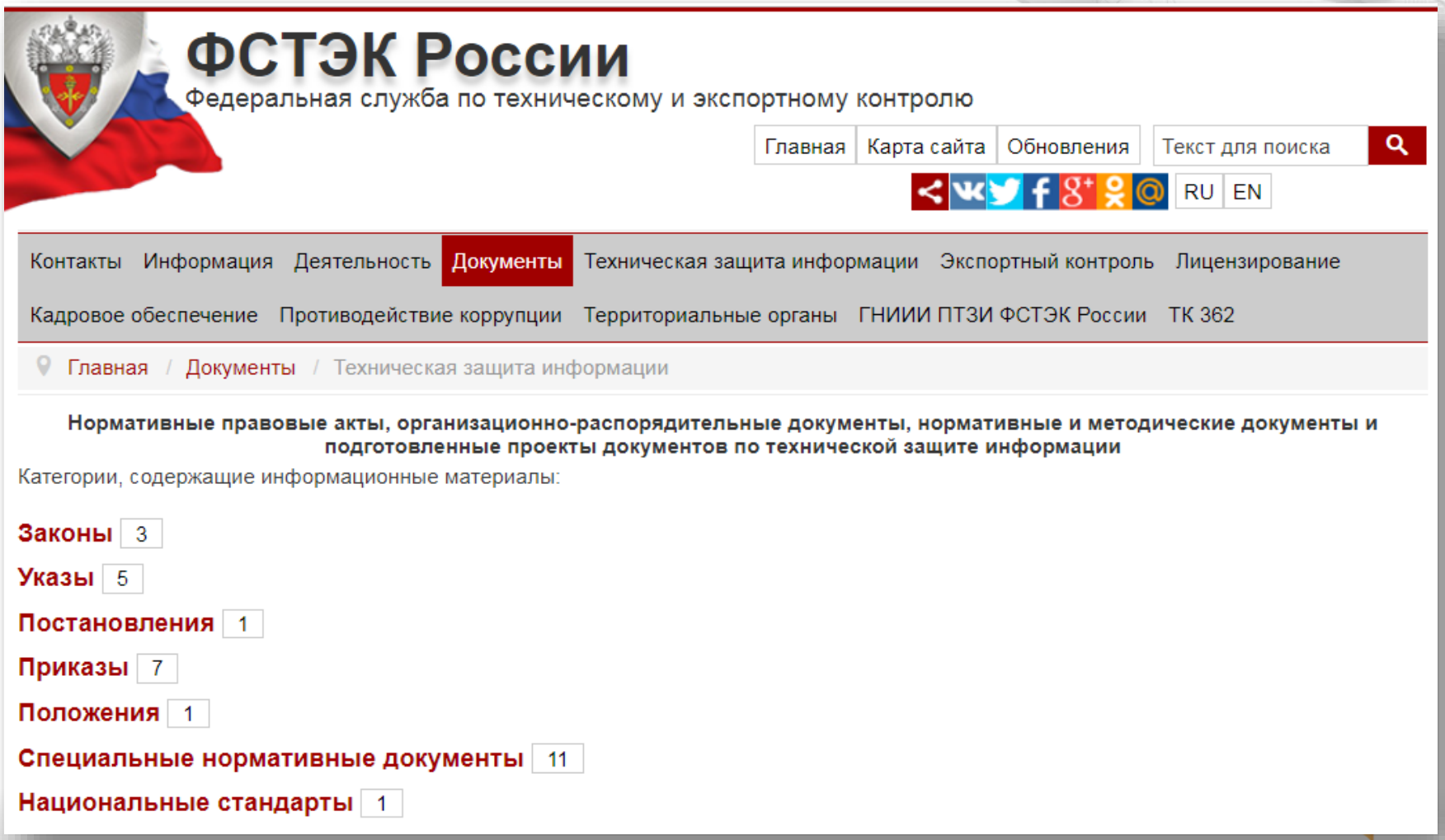
- Администрирование ОС и СУБД
- Администрирование доступных СЗИ
- Российские нормодоки
- Международные стандарты и лучшие практики
- Базовые знания по максимально широкому кругу технологий ИБ и ИТ
- Программирование (как минимум, на уровне скриптов для автоматизации)
- + Следить за актуальным состоянием отрасли

Осваивайте самые распространенные продукты

Группы мер обеспечения безопасности (на примере Приказа ФСТЭК России от 25 декабря 2017 г. N 239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации")	Айдеко	Акронис	Актив	Аладдин Р.Д.	Амикон	Газинформсервис	Гарда Технологии	Доктор Веб	Инфовотч	Инфотекс	Код Безопасности	Конфидент	Крипто-Про	Лаборатория Касперского	НИИ СОКБ	НПО РусБИТех	ОКБ САПР	Позитив Технолоджиз	СёрчИнформ	Сигнал-КОМ	С-Терра	Фактор-ТС	ЦБИ	Элвис-Плюс	Эшелон
I. Идентификация и аутентификация (ИАФ) II. Управление доступом (УПД) III. Ограничение программной среды (ОПС) IV. Защита машинных носителей информации (ЗНИ)			*	*		*					*	*				*	*								*
V. Аудит безопасности (АУД)																		*					*		*
VI. Антивирусная защита (АВЗ)								*			*			*											
VII. Предотвращение вторжений (компьютерных атак) (СОВ)	*								*	*	*											*			*
VIII. Обеспечение целостности (ОЦЛ)																							*		*
IX. Обеспечение доступности (ОДТ)		*																							
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)																									
ЗИС.2,4,5 Защита периметра, сегметирование, DMZ	*				*					*	*										*	*		*	*
ЗИС.16 Защита от спама	*							*						*											
ЗИС.17 Защита информации от утечек							*		*										*						
ЗИС.19 Защита информации при ее передаче по каналам связи					*					*	*										*	*		*	
ЗИС.28-29 Исключение возможности отрицания отправки/приема информации													*							*					
ЗИС.34 Защита от угроз отказа в обслуживании (DOS, DDOS-атак)							*		*					*				*							
ЗИС.38 Защита информации при использовании мобильных устройств											*			*	*										
ЗИС.39 Управление перемещением виртуальных машин											*						*								
XII. Реагирование на компьютерные инциденты (ИНЦ)																		*	*						*

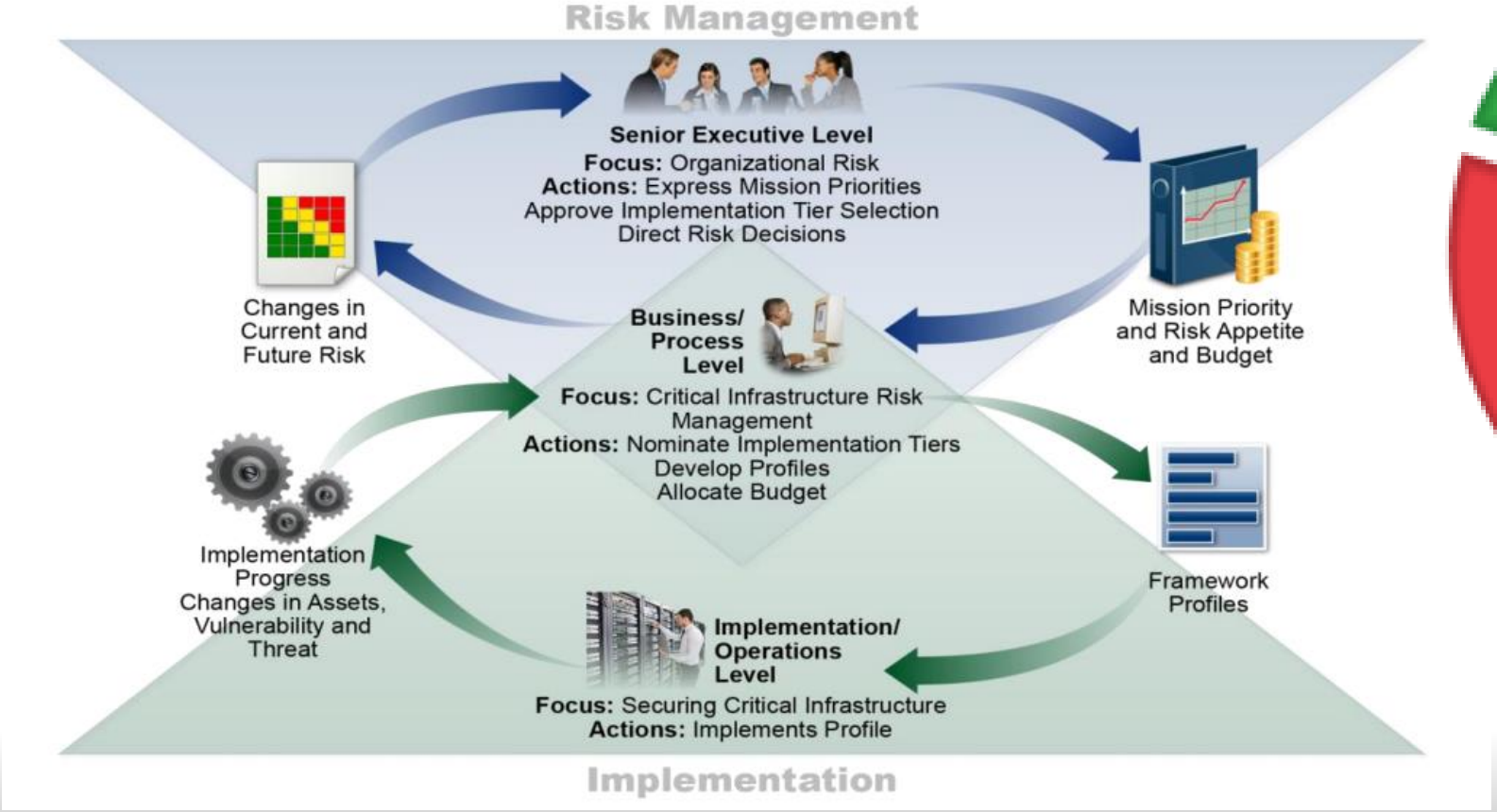
Следите за изменением законодательства

- Сайт ФСТЭК России
  - https://fstec.ru/



Изучайте международные документы

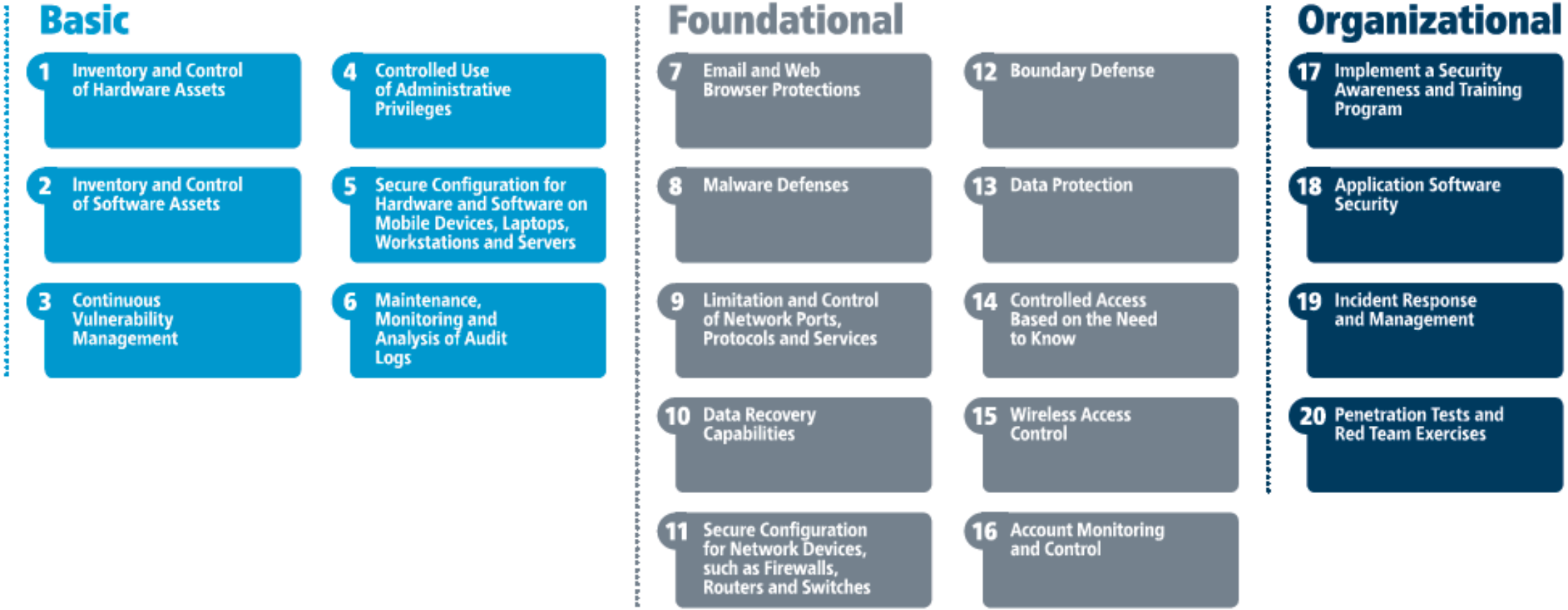
- NIST Cybersecurity Framework
  - https://www.nist.gov/cyberframework



Информзащита
Учебный центр

Используйте лучшие практики

- CIS Critical Security Controls for Effective Cyber Defense
  - https://www.sans.org/critical-security-controls



Информзащита
Учебный центр

Очень полезный источник знаний

- Серия стандартов BSI 100 IT-Grundschutz https://www.bsi.bund.de/EN/
  - 100-1 Information Security Management Systems
  - 100-2: IT-Grundschutz Methodology
  - 100-3: Risk Analysis based on IT-Grundschutz
  - 100-4: Business Continuity Management
  - IT-Grundschutz Catalogues

IT-Grundschutz Catalogues

Content

Полезные ресурсы для поддержания тонуса

- Новостные ленты по ИБ
  - Security Lab https://www.securitylab.ru/
  - Threatpost https://threatpost/
  - Anti-Malware https://www.anti-malware.ru/
  - Сайт ассоциации BISA https://bis-expert.ru/
  - Dark Reading http://www.darkreading.com/
  - Help Net Security https://www.helpnetsecurity.com/

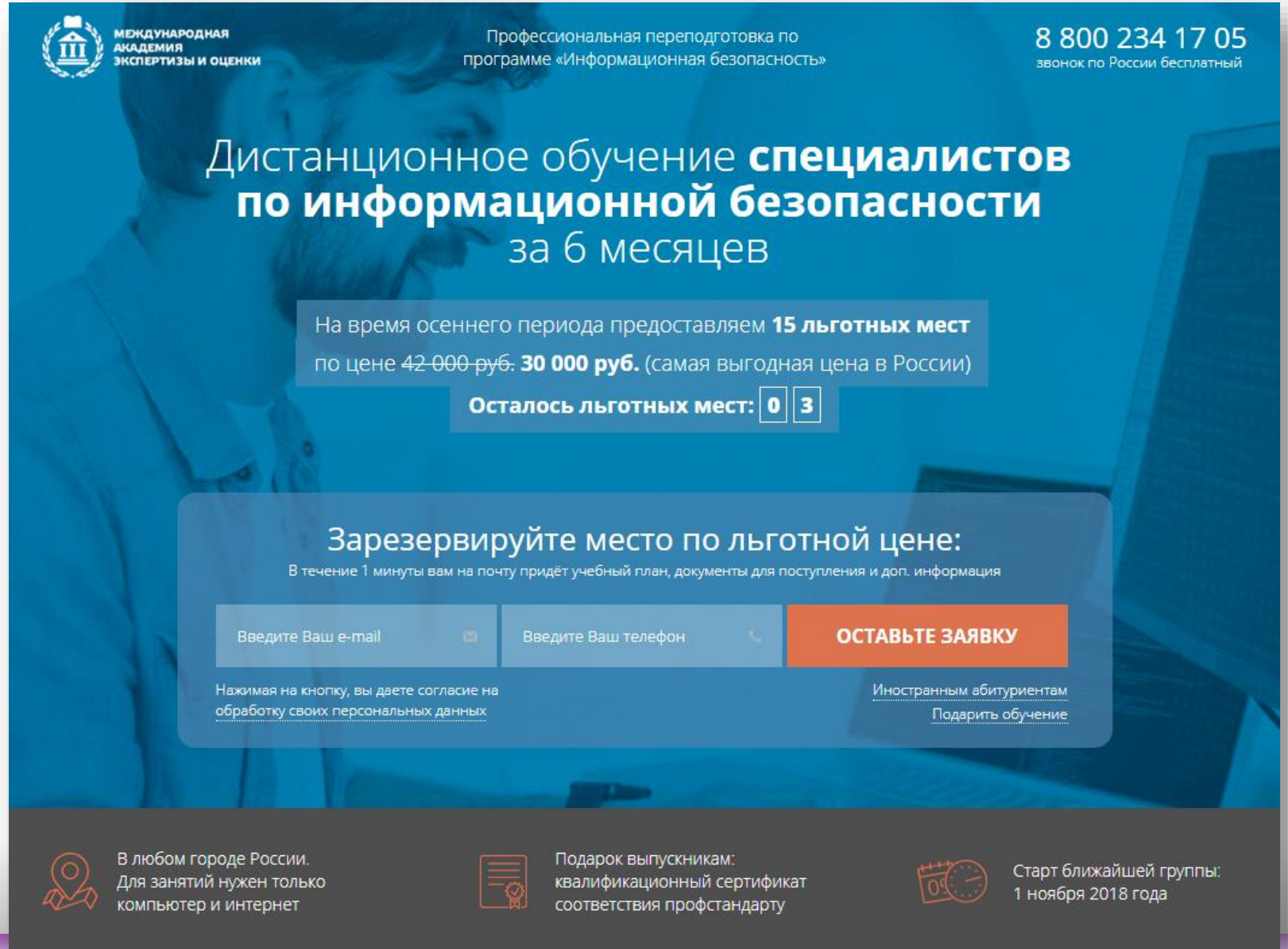
Полезные ресурсы для поддержания тонуса

- Личные блоги экспертов
  - Лукацкий Алексей https://lukatsky.blogspot.com/
  - Емельянников Михаил http://emeliyannikov.blogspot.com/
  - Борисов Сергей http://sborisov.blogspot.ru/
  - Комаров Алексей https://blog.zlonov.ru/
  - Царев Евгений http://www.tsarev.biz/
  - Группа «Безопасность КИИ» в Facebook https://www.facebook.com/groups/kii187fz/

Чему еще учиться

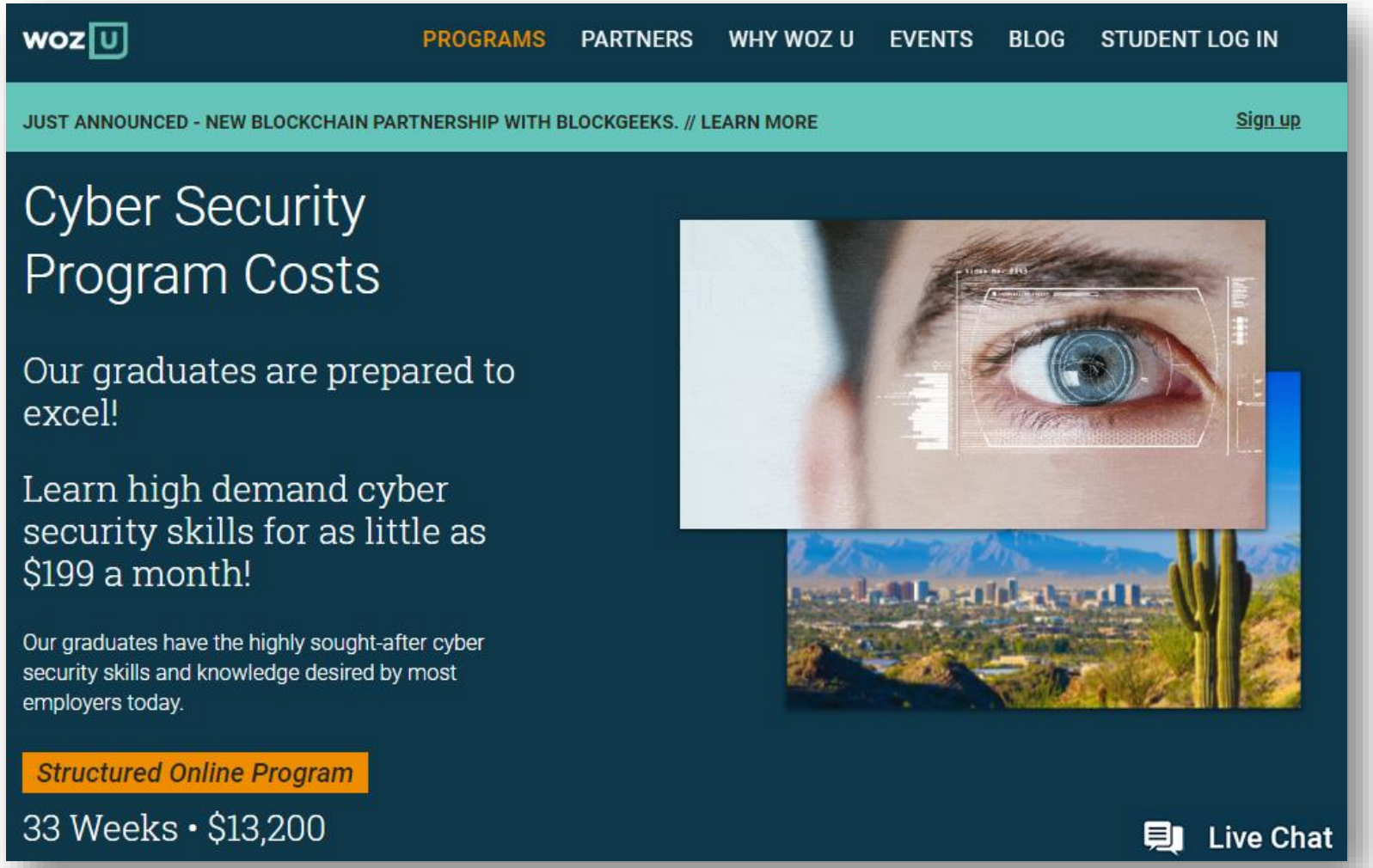
- Самосовершенствование
  - Личностные навыки
    - Коммуникационные навыки
    - Презентационные навыки
    - Навыки работы в команде
  - Управление проектами и тайм-менеджмент
  - Английский язык
  - Русский язык ☺
- Хорошая физическая форма

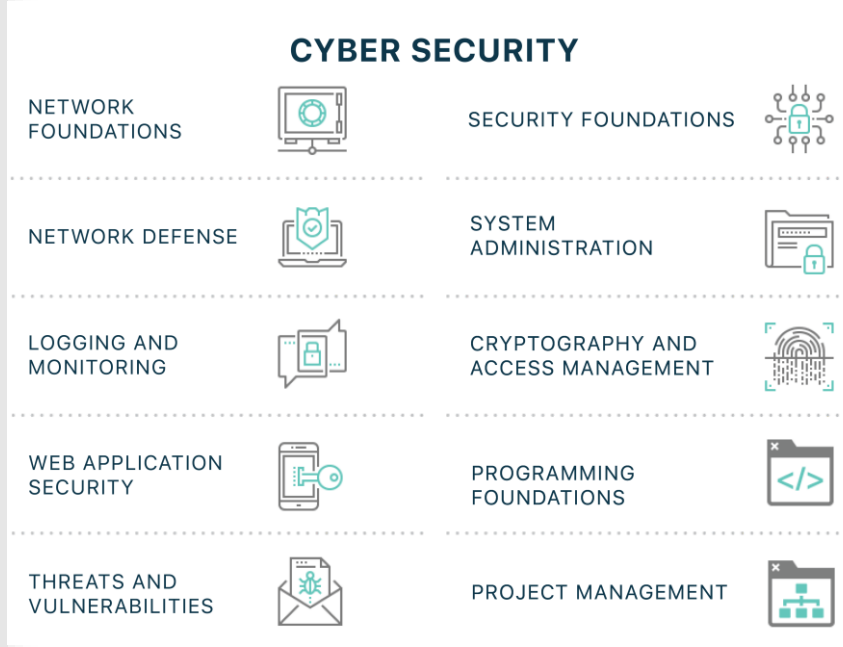
Про меркантильное



Информзащита
Учебный центр

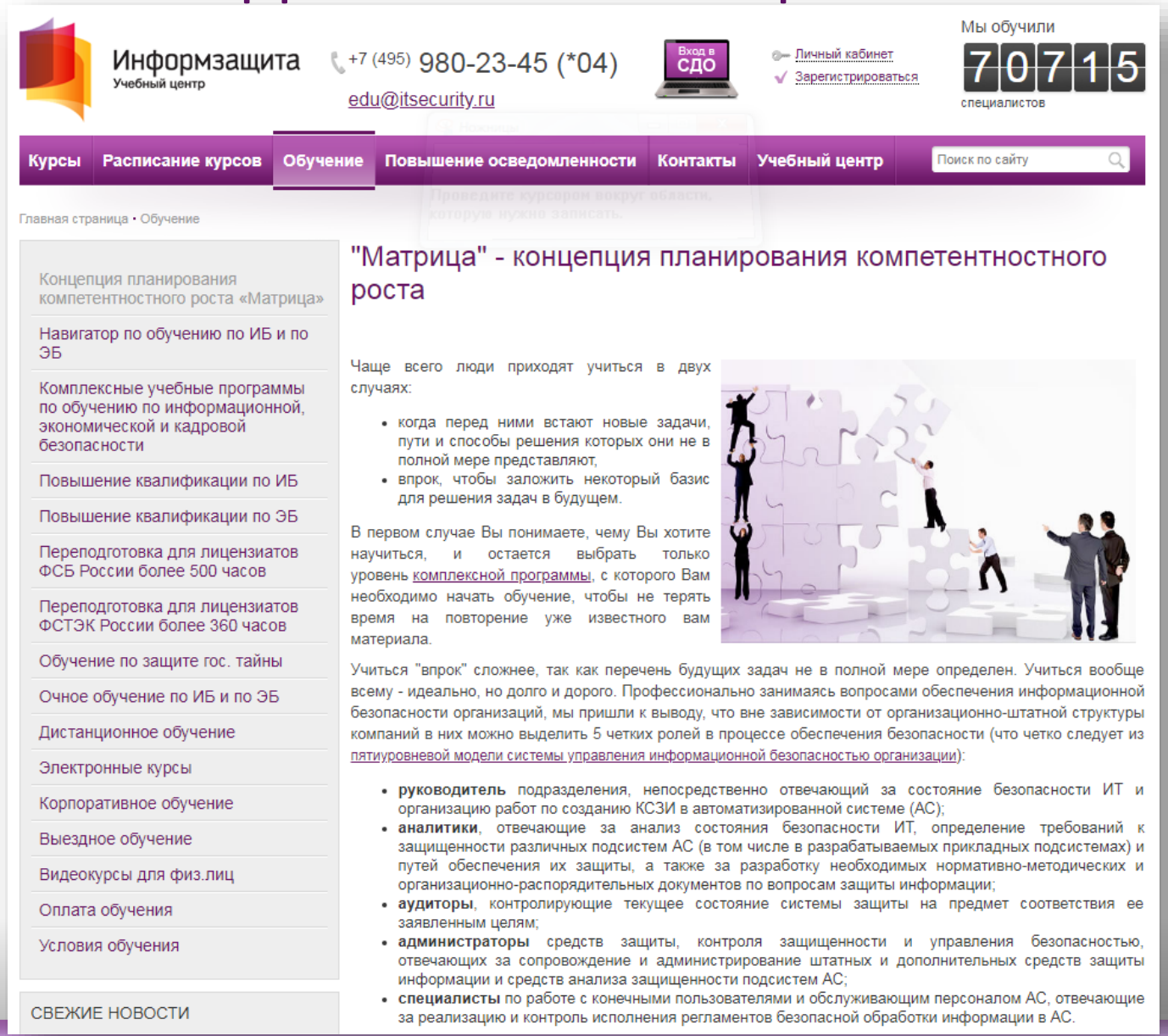
Про меркантильное





Информзащита
Учебный центр

Ваш надежный помощник ☺



www.itsecurity.ru

Информзащита
Учебный центр

Основы

- БТ01 Безопасность информационных технологий (5 дней)
- БТ05 Основы TCP/IP (1 день)
- БТ03 Безопасность компьютерных сетей (4 дня)
- БТ06 Защита сетевого периметра (3 дня)
- БТ07 Безопасность Web-приложений (2 дня)
- БТ09 Безопасность беспроводных сетей (3 дня)
- КП17 Безопасность систем электронной почты (2 дня)
- КП20 Анализ защищенности сетей (3 дня)

Углубленное изучение нормативки

- КП32 Защита персональных данных (2 дня)
- БТ25 Обеспечение безопасности и меры защиты информации в государственных информационных системах (2 дня)
- БТ187 Обеспечение безопасности объектов критической информационной инфраструктуры (2 дня)
- КП62 Защита информации в Национальной платежной системе (1 день)
- КП30 Реализация режима коммерческой тайны на предприятии (2 дня)
- КП31 Организация конфиденциального делопроизводства (2 дня)
- КП06 Использование ЭП и PKI (3 дня)

Информзащита
Учебный центр

Специализация

- БТ31 Безопасность Windows 7/8.1/10/2012R2/2016 (5 дней)
- БТ12 Безопасность сетей на базе Linux (Unix) (5дней)
- БТ19 Безопасность IP-телефонии (2 дня)
- КП21 Обнаружение атак (2 дня)
- КП22 Организация защиты от DDoS-атак (2 дня)
- КП05 Расследование компьютерных инцидентов (4 дня)
- БТ15 Антология хакинга (5 дней)

Информзащита
Учебный центр

Специализация

- КП43 Система управления инцидентами как основа обеспечения информационной безопасности организации (3 дня)
- КП44 Управление рисками безопасности информационных систем организаций (2 дня)
- КП45 Методы и средства аудита информационной безопасности (3 дня)
- БТ16 Компьютерная криминалистика (5 дней)
- Т012 Порядок развертывания и применения PKI на основе ПАК «КриптоПро УЦ» 2.0 (3 дня)

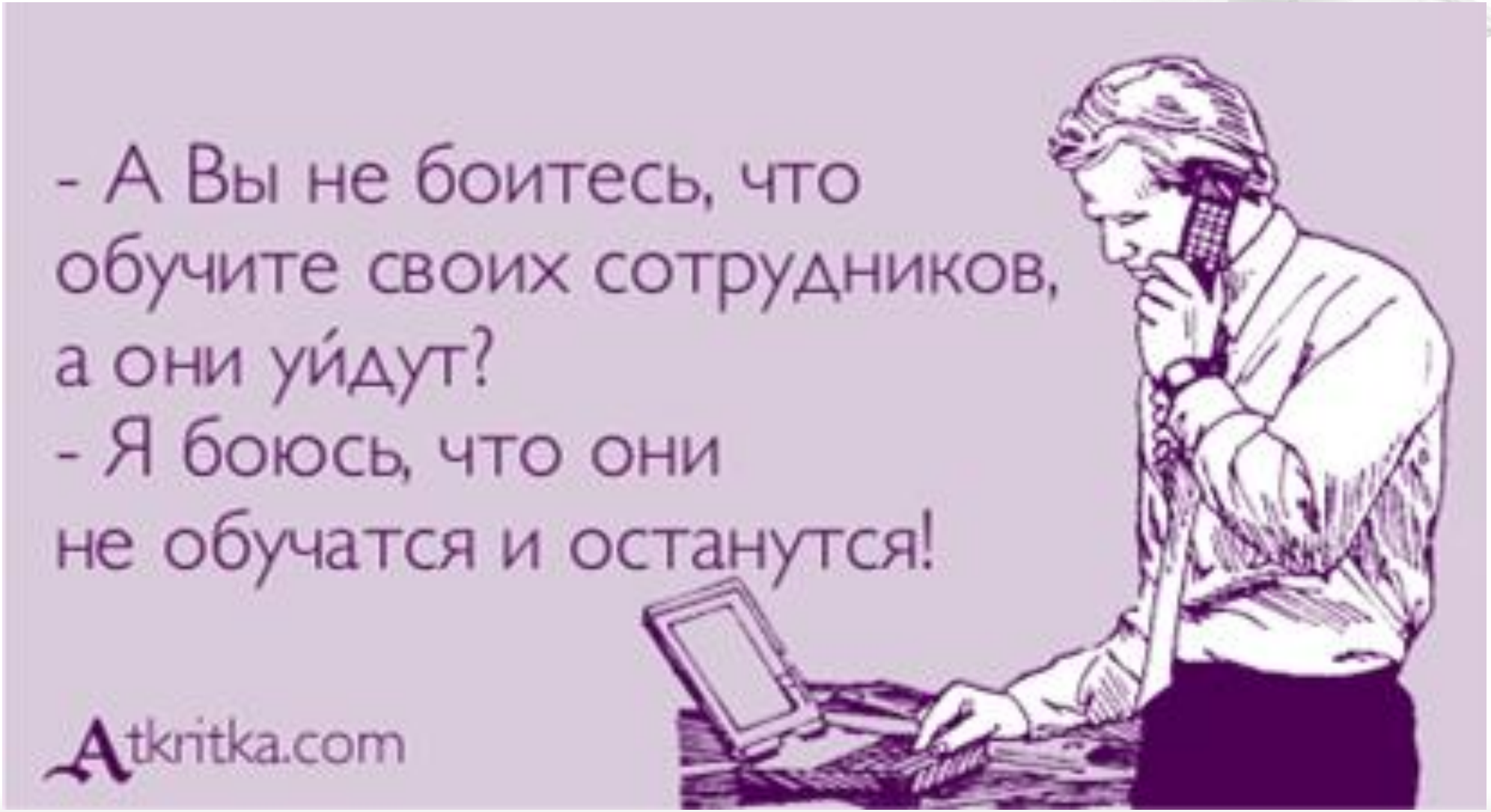
Информзащита
Учебный центр

Курсы вендоров

- Позитив Технолоджис
- Лаборатория Касперского
- Код Безопасности
- Крипто Про
- Аладдин Р.Д.
- HP ArcSight
- Microsoft
- CheckPoint
- Cisco

Информзащита
Учебный центр

Вместо заключения



Информзащита
Учебный центр

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информзащита
Учебный центр

Спасибо!

Андрей Степаненко
a.stepanenko@itsecurity.ru
(495) 980-2345 доб. 826
www.itsecurity.ru