КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ИТОГИ

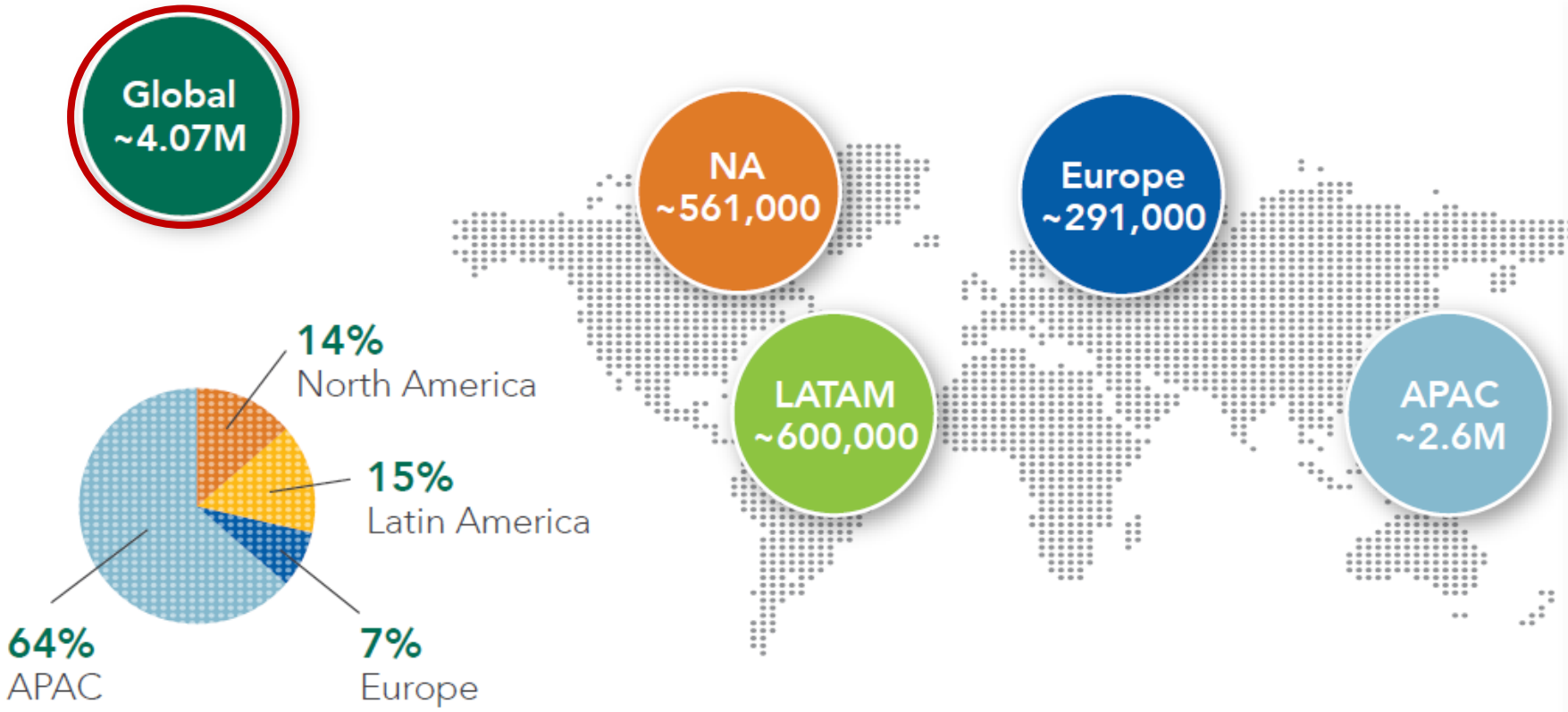
Тенденции рынка ИБ-кадров: кто виноват и что делать?

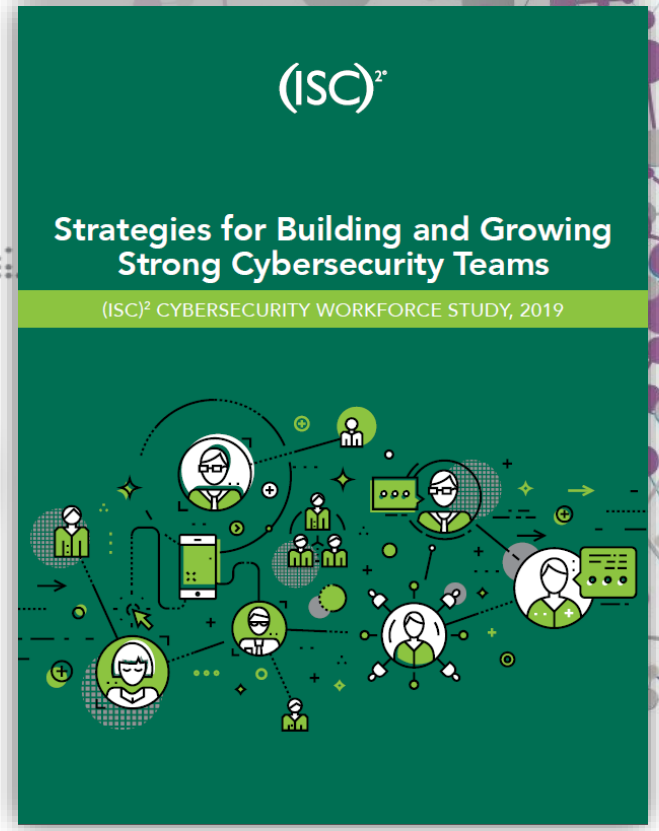
Андрей Степаненко, директор

Информзащита
Учебный центр

Глобальный дефицит безопасников

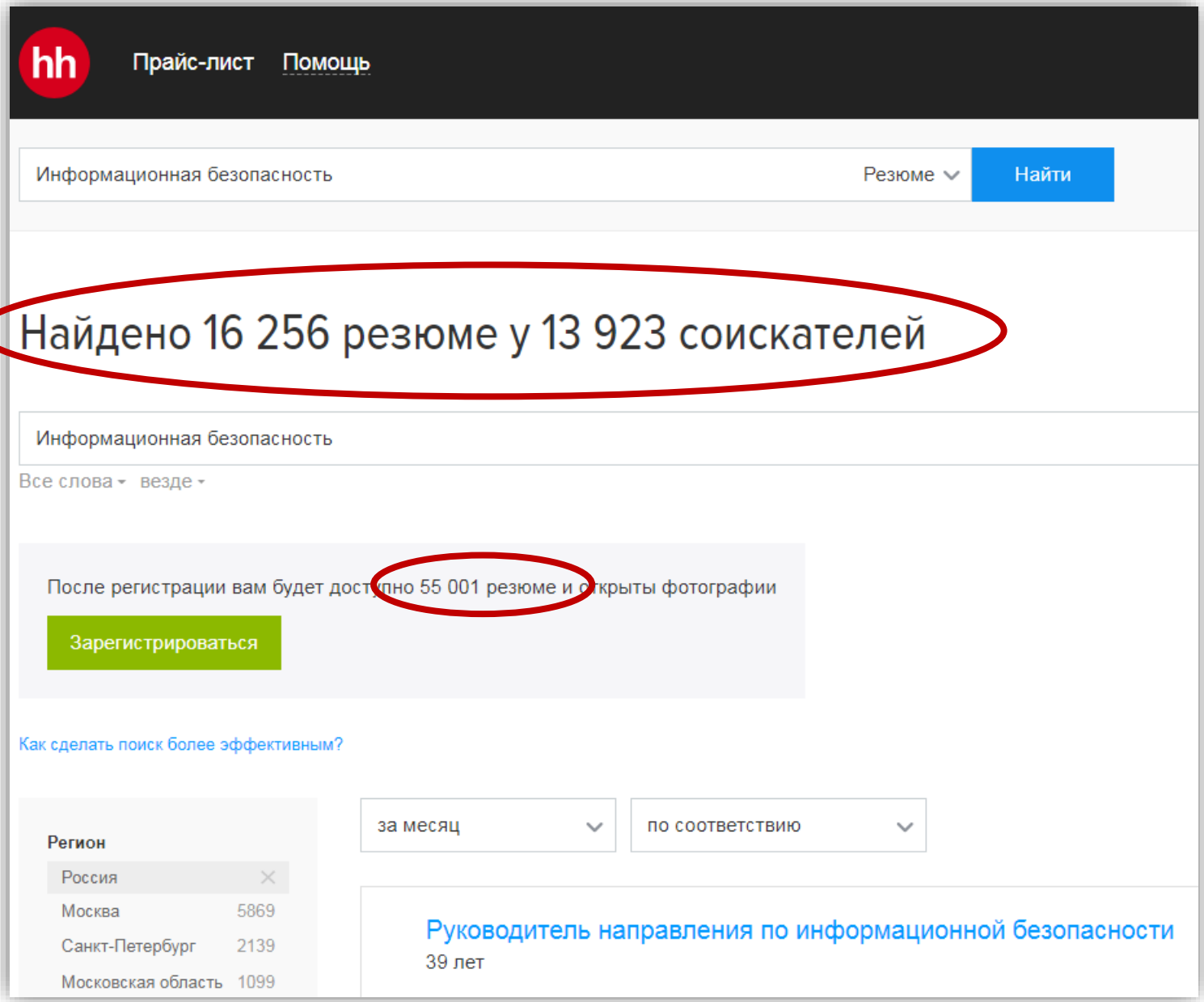
The Cybersecurity Workforce Gap by Region





Информзащита
Учебный центр

Российские реалии



Информзащита
Учебный центр

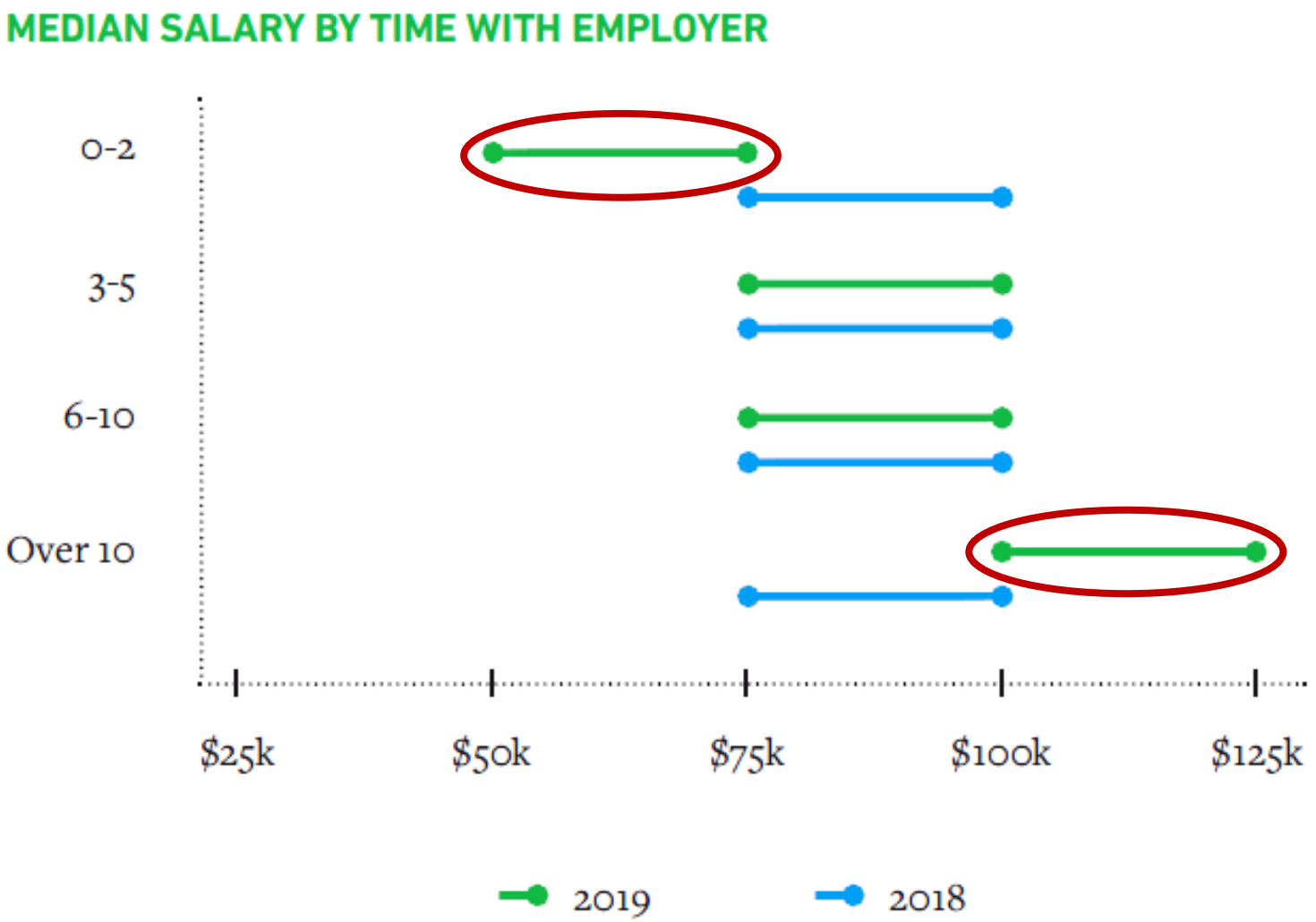
Как ищем (если мы не Сбербанк и т.п.)

Приоритеты кадровика:

- Профессионализм
- Желание работать за маленькую заплату

Информзащита
Учебный центр

Наметившаяся тенденция



Информзащита
Учебный центр

Откуда берутся безопасники

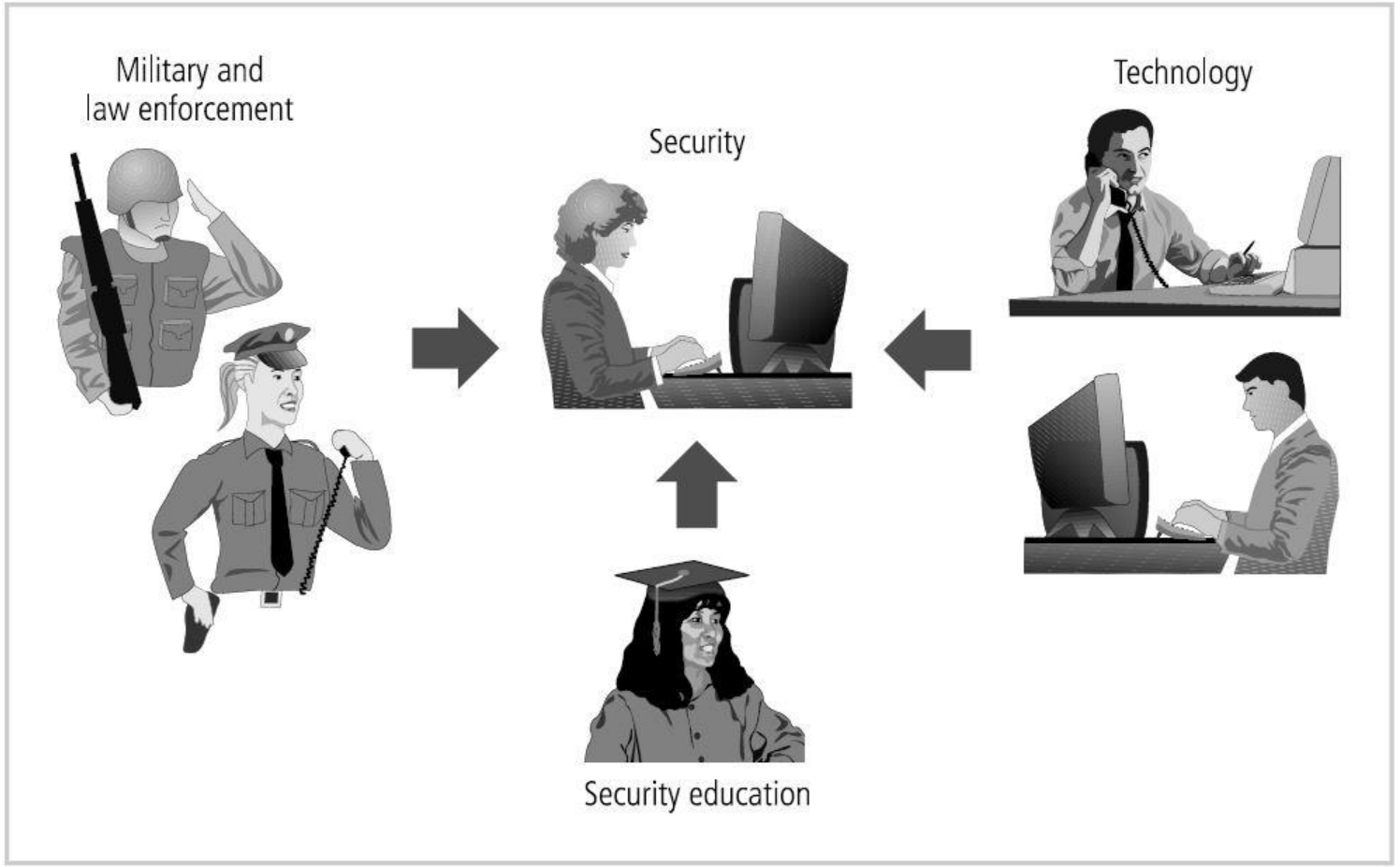
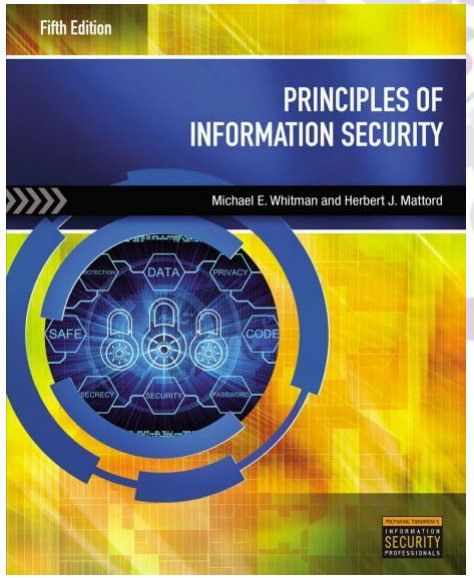


Figure 11-1 Career Paths to Information Security Positions

Иллюстрация из книги «Principles of Information Security»
M. Whitman, H. Mattord
1-е издание, 2003 г.



Информзащита
Учебный центр

Перспективы

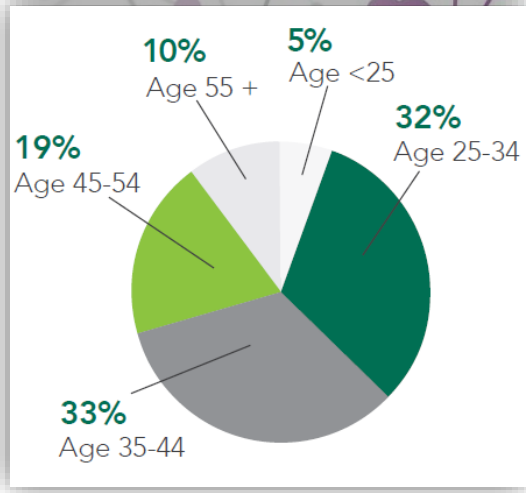
Контрольные цифры приема по УГНПС 10.00.00 «Информационная безопасность» на 2018-21 гг.

Уровни высшего образования	2018	2019	2020	2021*
Бакалавриат	2 379	2 673	2 918	3 039
Магистратура	999	606	808	680
Специалитет	3 264	3 812	3 743	3 858
ИТОГО:	**6 642**	**7 091**	**7 469**	**7 628**
Будет выпущено* (75%)	4 982	5 318	5 602	5 721
Пойдет работать по специальности* (70%)	3 487	3 723	3 921	4 005

Информзащита
Учебный центр

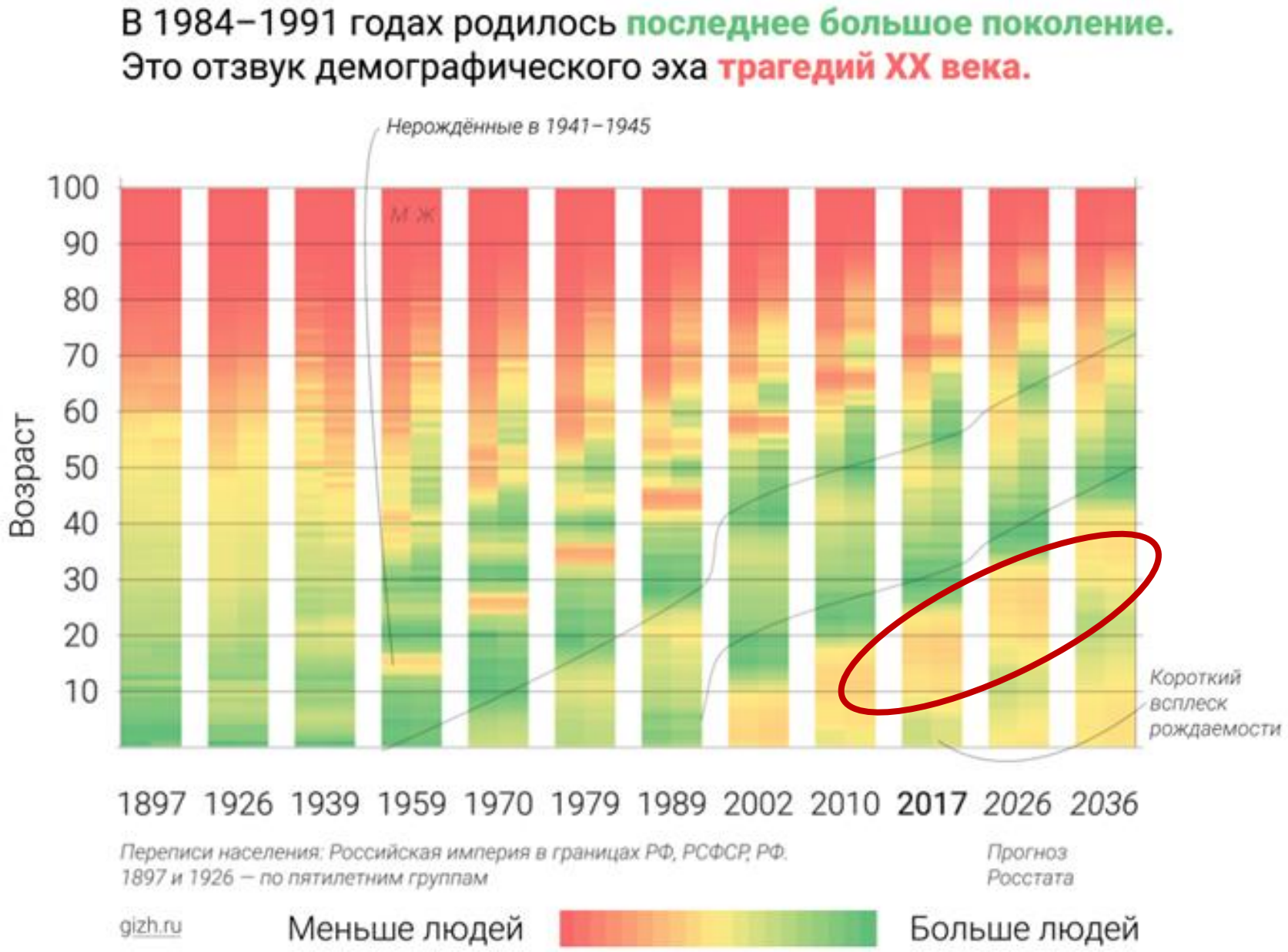
Для размышления – с кем мы работаем

Название поколения	Годы рожде-ния	Психологическая характеристика
Бэби-бумеры 17 млн. чел. (до 65 лет)	1945-1964	Оптимизм, командный дух, заинтересованность в личностном росте и вознаграждении, культ молодости.
Поколение X 31 млн. чел.	1965-1984	Прагматизм, индивидуализм, техническая грамотность, стремление учиться в течение всей жизни, готовность к изменениям.
Поколение Y 28 млн. чел.	1985-2003	Скептицизм, неумение подчиняться, ориентация на немедленное вознаграждение.
Поколение Z 19 млн. чел.	2004-2023	Безответственность, массовое соответствие моде, ветреность.



Информзащита
Учебный центр

Дополнительный минус – демографическая яма

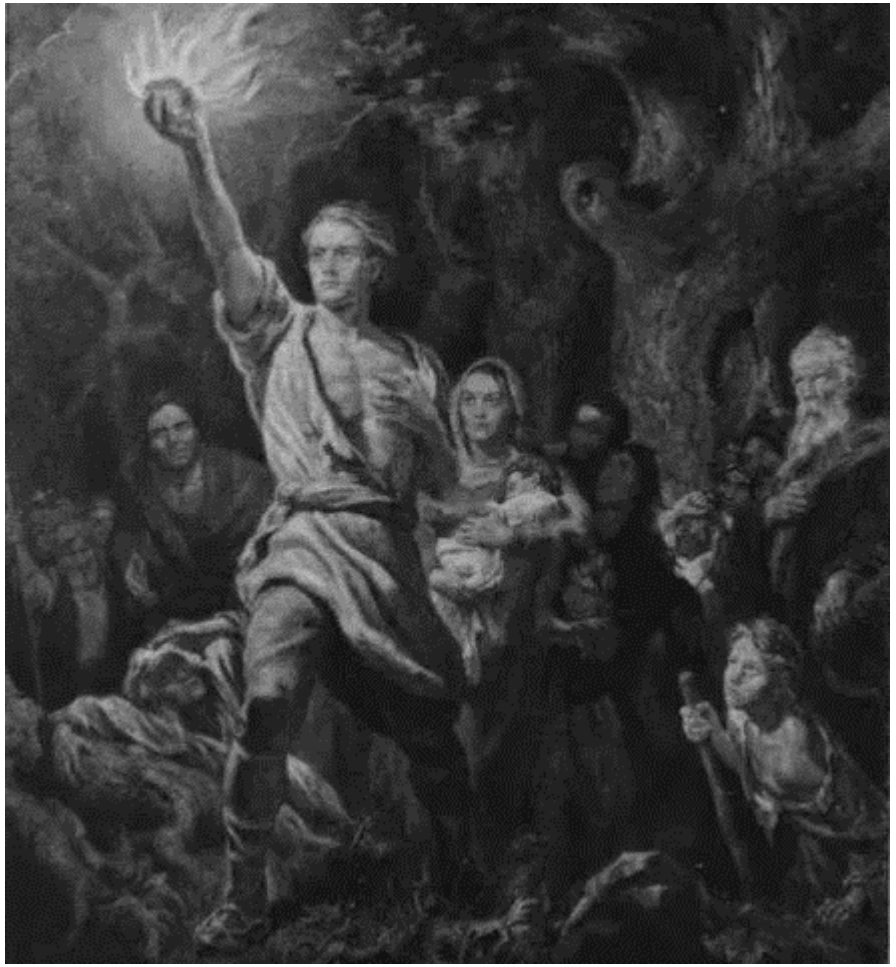


Информзащита
Учебный центр

Рекомендуемый подход к поиску

Приоритеты безопасника:

- Лояльность
- Обучаемость
- Профессионализм



Информзащита
Учебный центр

Быстрый способ оценки лояльности

Тест Сонди (метод портретных выборов)

Информзащита
Учебный центр

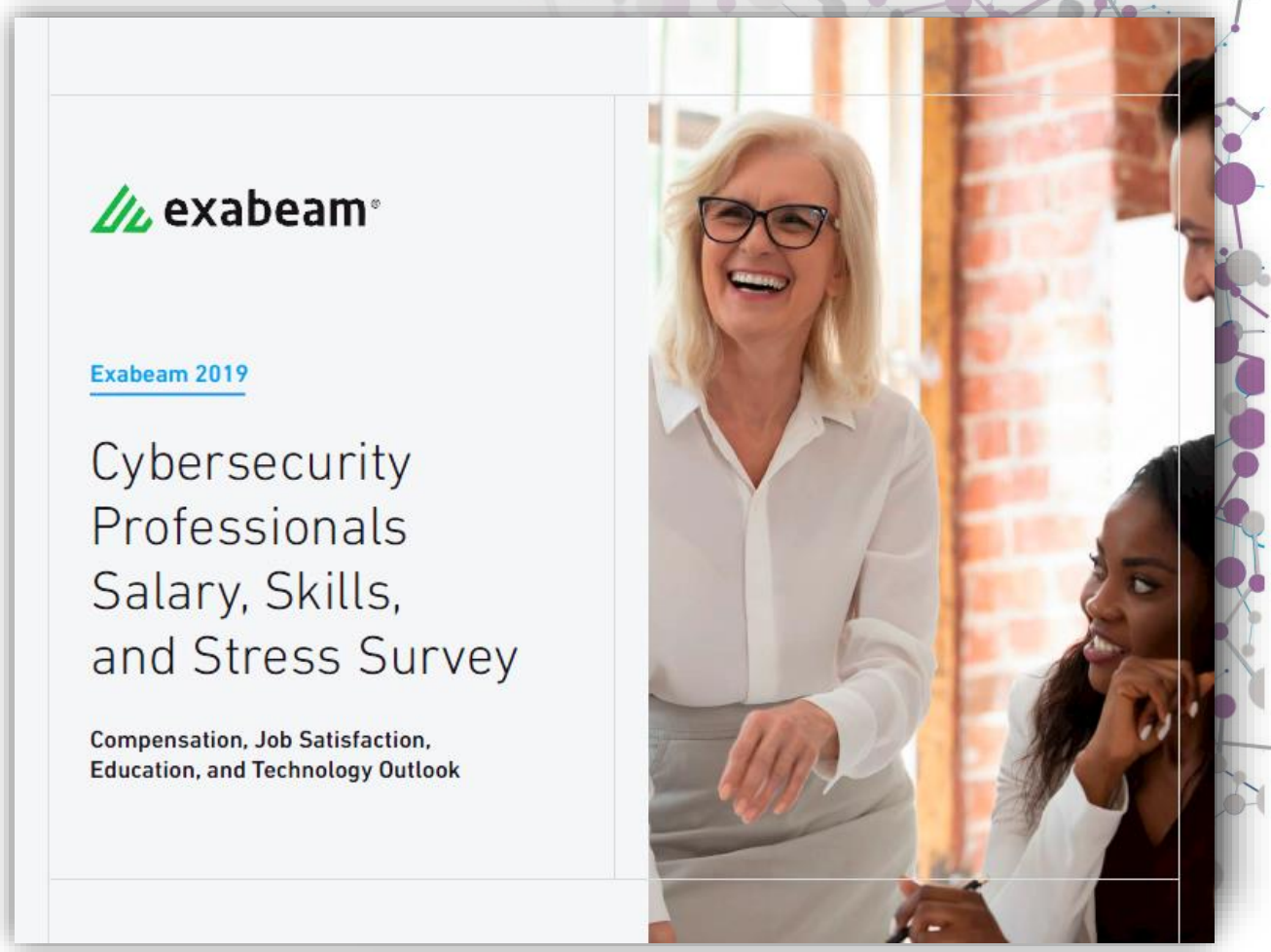
Что дальше

- Минимизируем раздражители
- Следим за наличием пряников

Информзащита
Учебный центр

Что раздражает в работе

- Вмешательство в работу (28%)
- Частые авралы (23%)
- Скука (12%)



Информзащита
Учебный центр

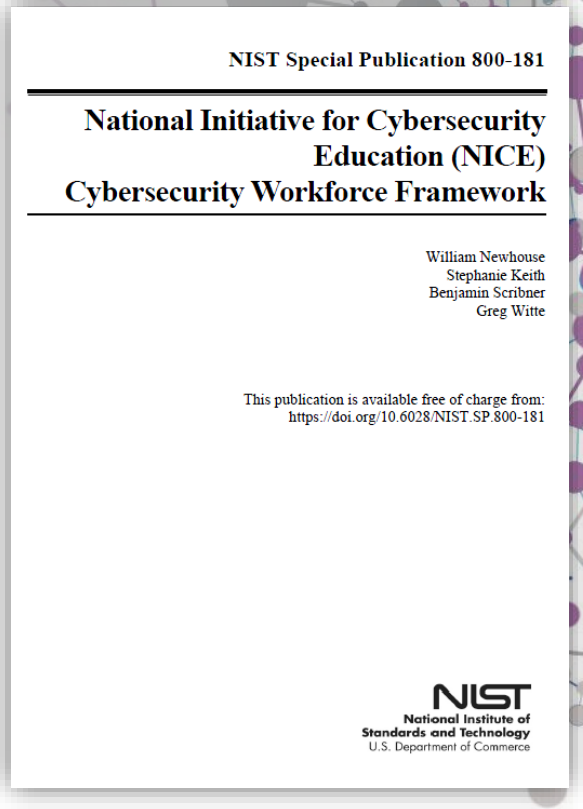
Что ценят в работе (кроме денег ☺)

- Возможности для обучения и развития (57%)
- Хороший коллектив (46%)
- Работа с новыми технологиями (35%)

Планирование саморазвития и обучения

NIST SP 800-181 «NICE Cybersecurity Workforce Framework»

- 7 групп общих функций безопасников
- 33 специализации
- 52 роли в терминах
  - выполняемые задачи (Task)
    - 1007 типовых задач
  - требуемые знания/умения/способности (KSA)
    - 630 областей знаний (Knowledge)
    - 374 практических умений (Skill)
    - 176 навыков/способностей (Ability)


NIST Special Publication 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

William Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181

NIST National Institute of Standards and Technology U.S. Department of Commerce

Информзащита
Учебный центр

Очень полезный источник знаний

Серия стандартов BSI 200 IT-Grundschutz
https://www.bsi.bund.de/EN/

- 200-1 Information Security Management Systems
- 200-2: IT-Grundschutz Methodology
- 200-3: Risk Analysis based on IT-Grundschutz
- 100-4: Business Continuity Management
- IT-Grundschutz Catalogues

Federal Office
for Information Security

Информзащита
Учебный центр

IT-Grundschutz Catalogues

Content

Настольная книга для расстановки приоритетов

Top 20 Security Controls for Effective Cyber Defense
https://www.cisecurity.org/controls/

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

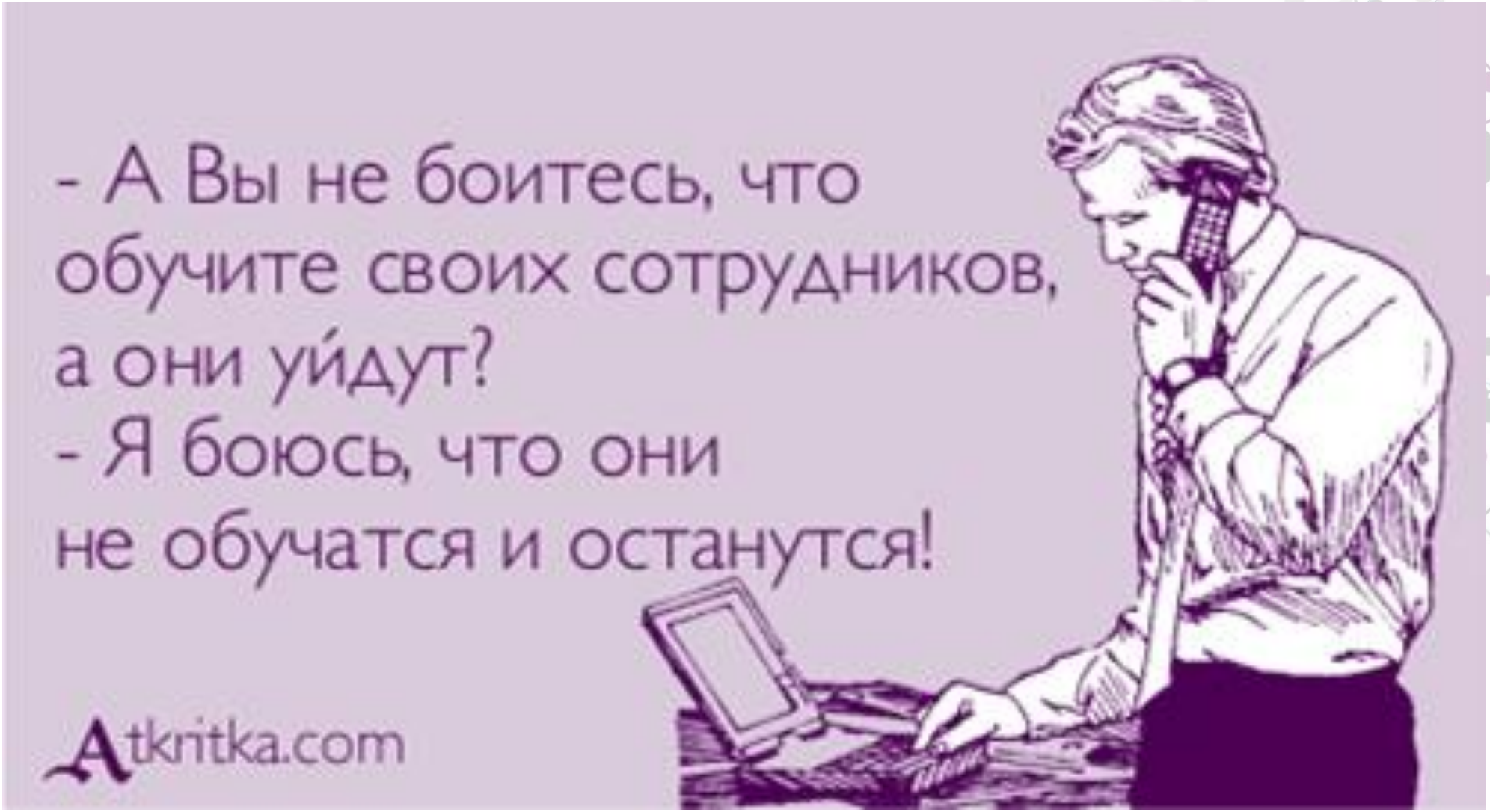
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Информзащита
Учебный центр

Чему еще учить

- Коммуникационные навыки
- Презентационные навыки
- Навыки работы в команде
- Управление проектами и тайм-менеджмент
- Английский язык
- Русский язык ☺

Вместо заключения



Информзащита
Учебный центр

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ИТОГИ

Спасибо!

Андрей Степаненко
a.stepanenko@itsecurity.ru
+7 (495) 980 2345 доб.04

Информзащита
Учебный центр