



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

ИТОГИ

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

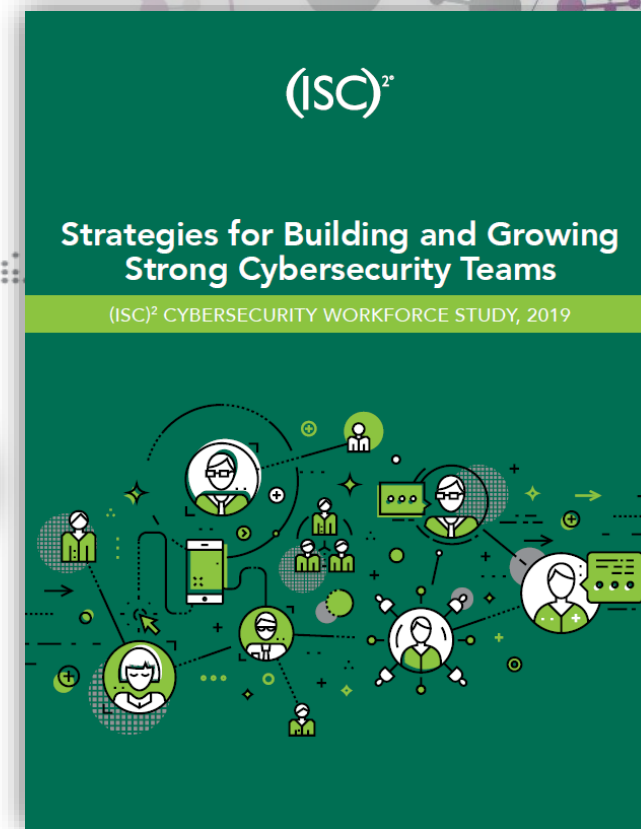
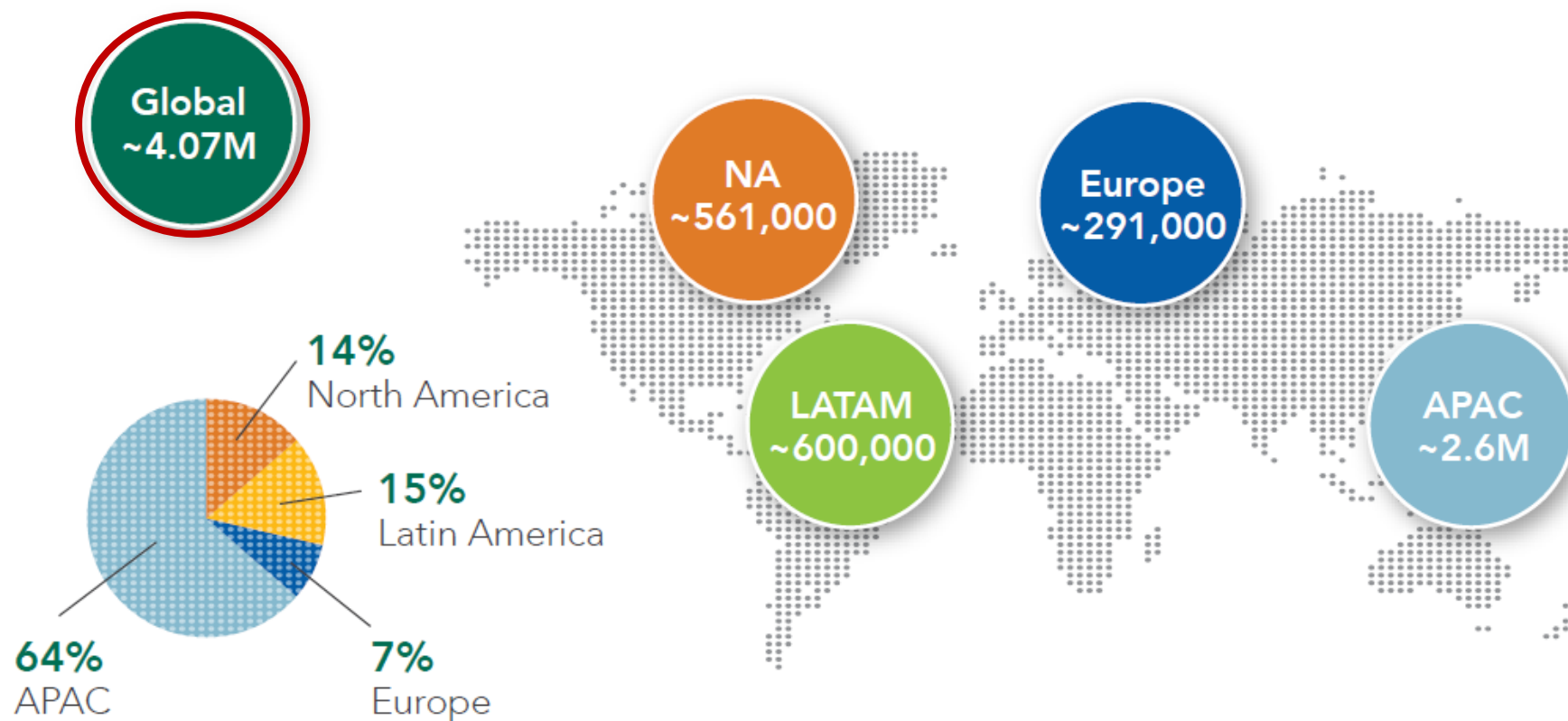
Андрей Степаненко, директор



Информзащита
Учебный центр

Глобальный дефицит безопасников

The Cybersecurity Workforce Gap by Region



Российские реалии

The screenshot shows the hh.ru website interface. At the top left is the 'hh' logo, followed by links for 'Прайс-лист' and 'Помощь'. A search bar contains the text 'Информационная безопасность'. To the right of the search bar are a dropdown menu set to 'Резюме' and a blue 'Найти' button. Below the search bar, a large red oval highlights the text: 'Найдено 16 256 резюме у 13 923 соискателей'. Underneath, there is a filter section with 'Информационная безопасность' and 'Все слова - везде'. A grey box contains the text: 'После регистрации вам будет доступно 55 001 резюме и открыты фотографии', with '55 001' circled in red. Below this is a green 'Зарегистрироваться' button. At the bottom left, there is a 'Регион' dropdown menu with a list: 'Россия' (selected), 'Москва' (5869), 'Санкт-Петербург' (2139), and 'Московская область' (1099). To the right of the region menu are two dropdown menus: 'за месяц' and 'по соответствию'. At the bottom right, there is a blue link: 'Руководитель направления по информационной безопасности' with '39 лет' below it.

hh Прайс-лист [Помощь](#)

Информационная безопасность Резюме ▾ [Найти](#)

Найдено 16 256 резюме у 13 923 соискателей

Информационная безопасность

Все слова ▾ везде ▾

После регистрации вам будет доступно 55 001 резюме и открыты фотографии

[Зарегистрироваться](#)

[Как сделать поиск более эффективным?](#)

Регион

Россия	×
Москва	5869
Санкт-Петербург	2139
Московская область	1099

за месяц ▾ по соответствию ▾

[Руководитель направления по информационной безопасности](#)
39 лет



Как ищем (если мы не Сбербанк и т.п.)

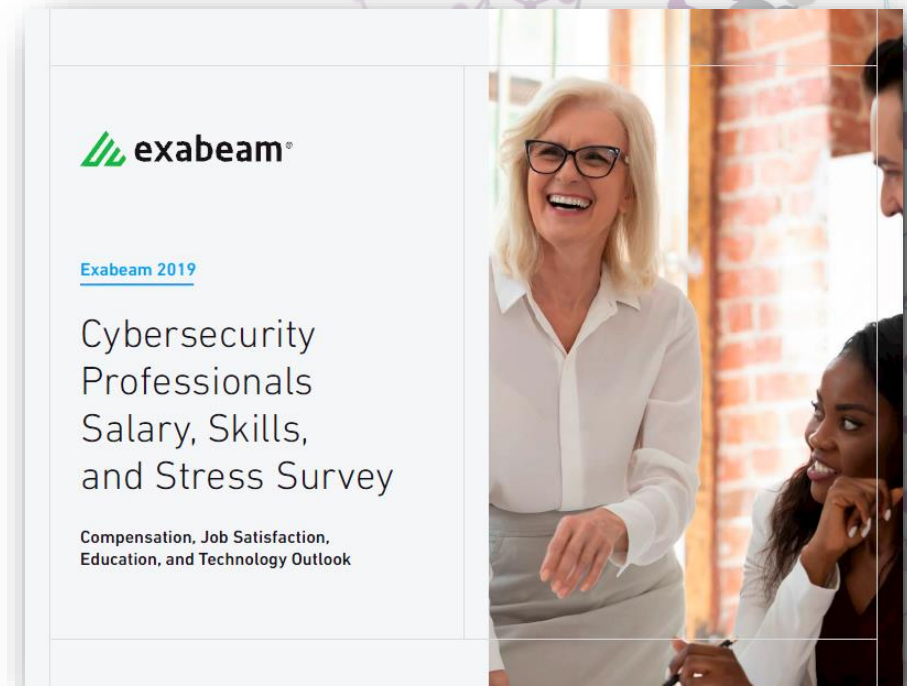
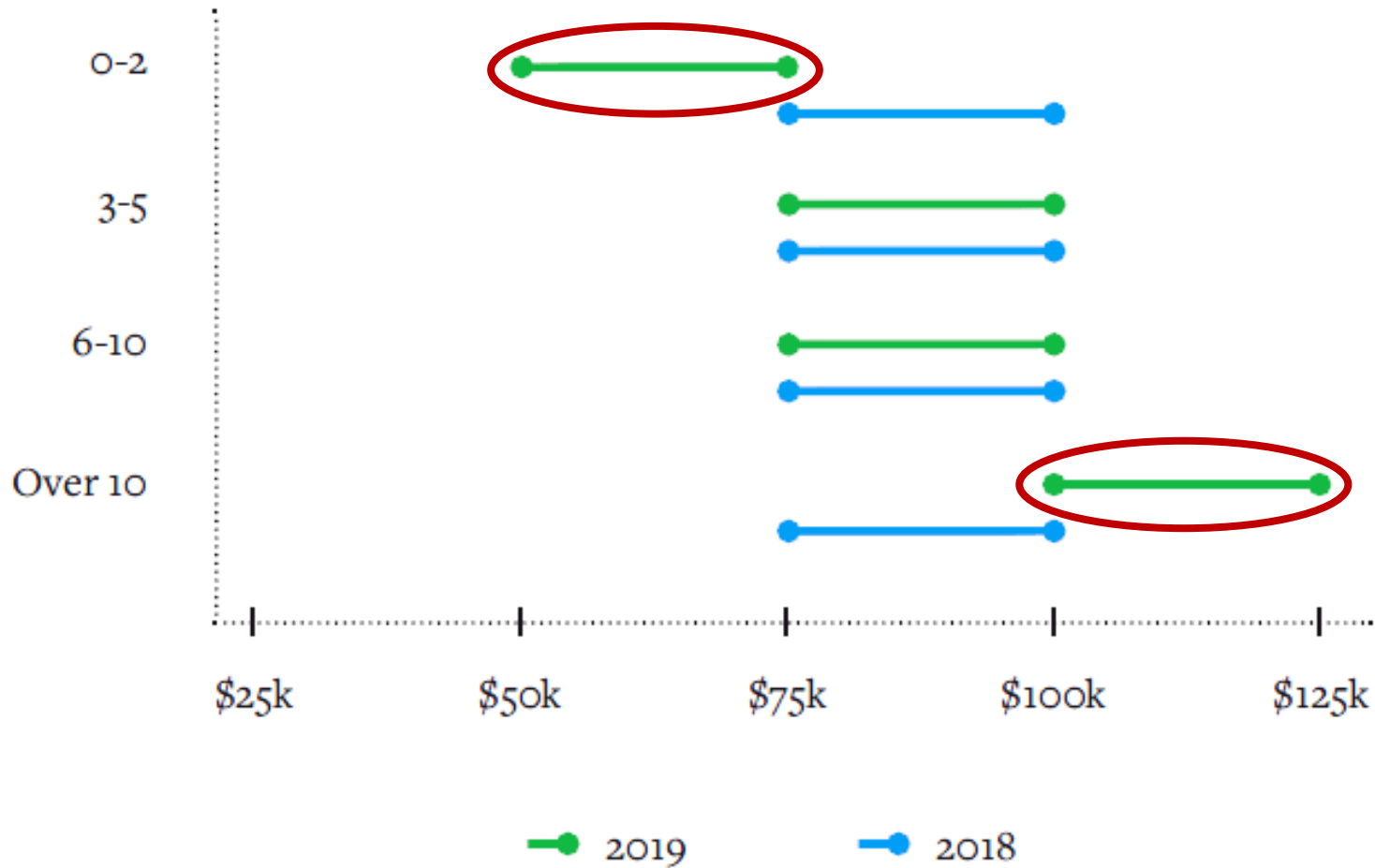
Приоритеты кадровика:

- Профессионализм
- Желание работать за маленькую зарплату



Наметившаяся тенденция

MEDIAN SALARY BY TIME WITH EMPLOYER



Откуда берутся безопасники

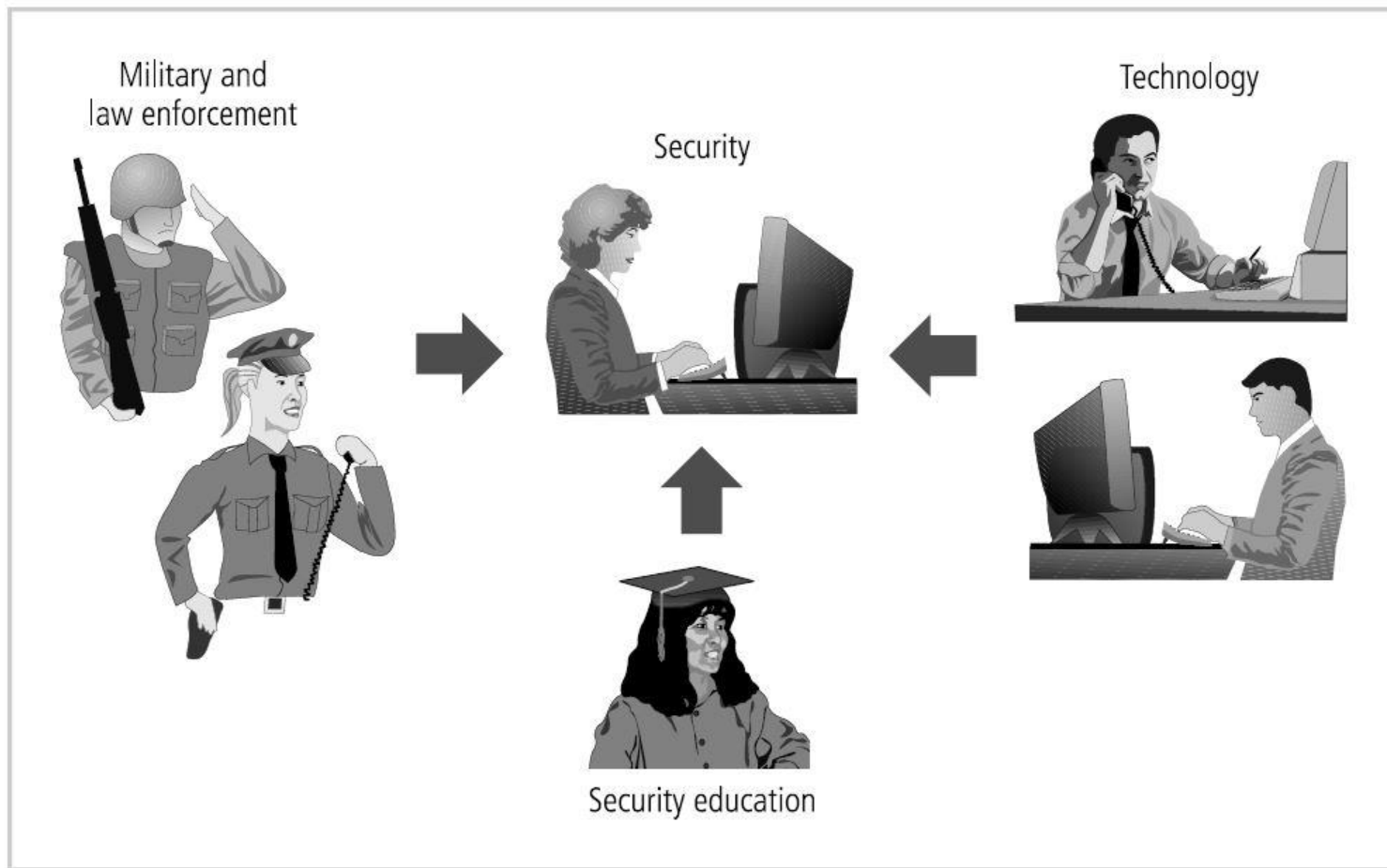
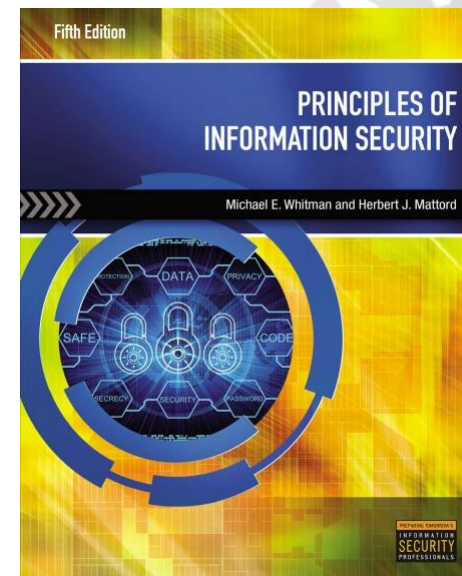


Figure 11-1 Career Paths to Information Security Positions

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



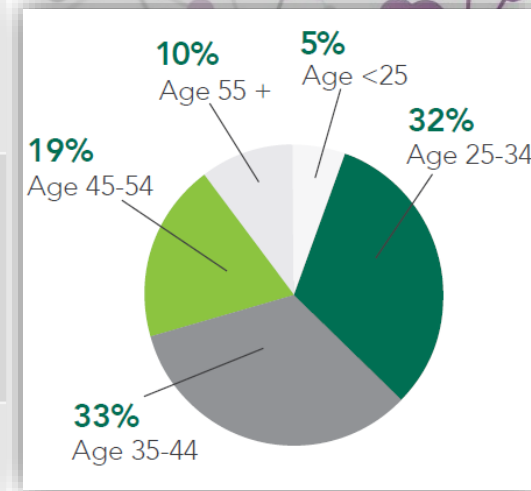
Перспективы

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

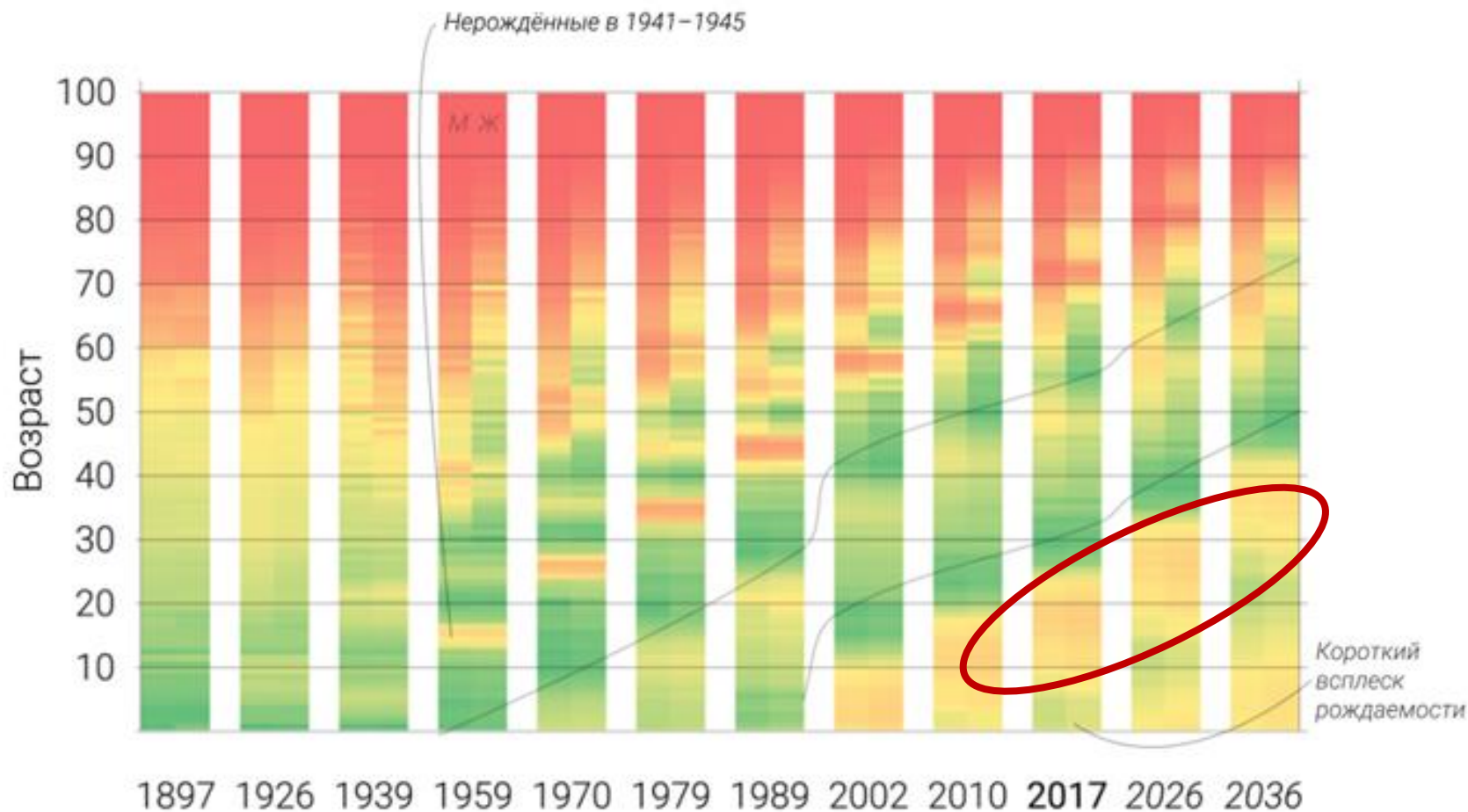
Для размышления – с кем мы работаем

Название поколения	Годы рождения	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.



Дополнительный минус – демографическая яма

В 1984–1991 годах родилось **последнее большое поколение**.
Это отзвук демографического эха **трагедий XX века**.



Переписи населения: Российская империя в границах РФ, РСФСР, РФ.
1897 и 1926 – по пятилетним группам

Прогноз
Росстата



Рекомендуемый подход к поиску

Приоритеты безопасника:

- Лояльность
- Обучаемость
- Профессионализм



Быстрый способ оценки лояльности

Тест Сонди (метод портретных выборов)



Что дальше

- Минимизируем раздражители
- Следим за наличием пряников



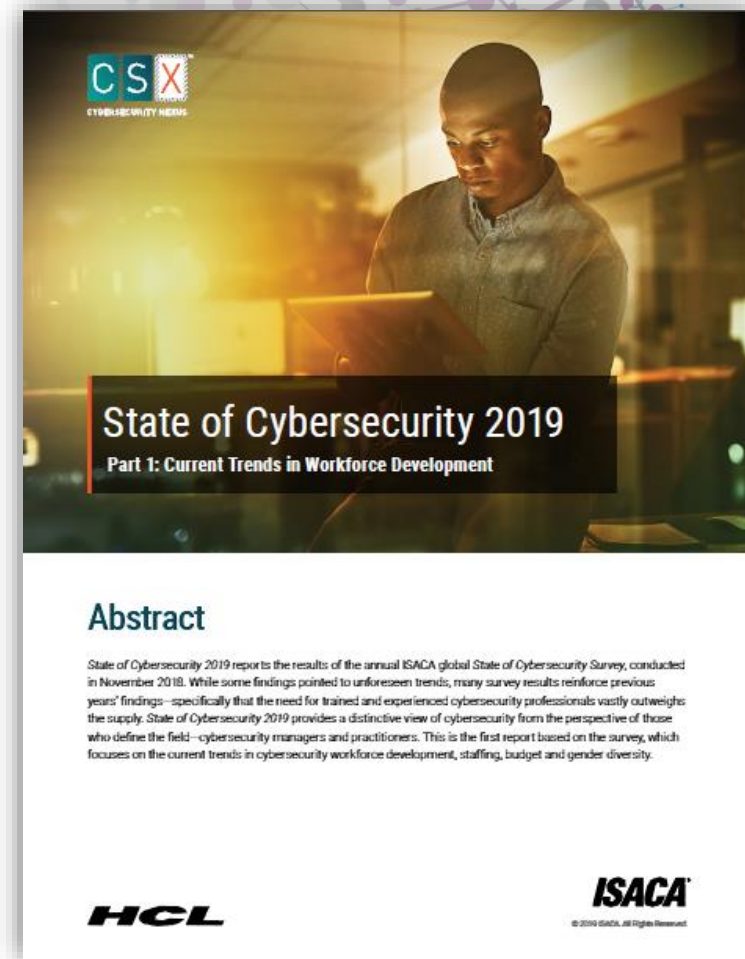
Что раздражает в работе

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



Что ценят в работе (кроме денег 😊)

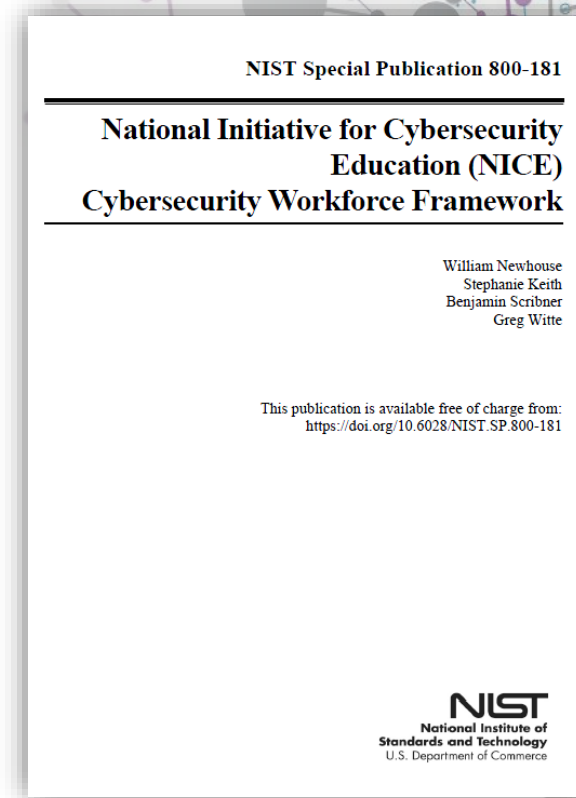
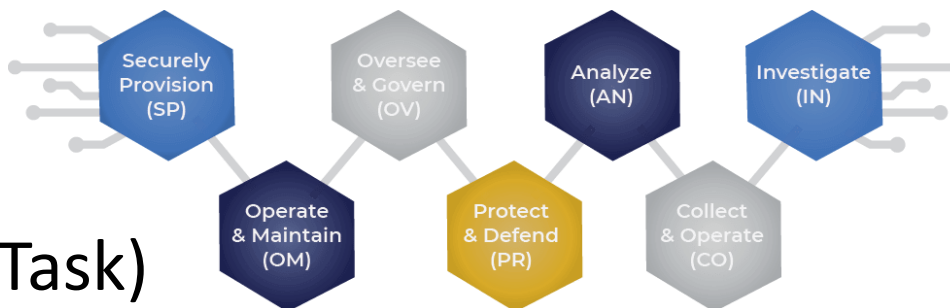
- Возможности для обучения и развития (57%)
- Хороший коллектив (46%)
- Работа с новыми технологиями (35%)



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)



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

IT-Grundschutz Catalogues

Content

Foreword.....	2
Acknowledgements	5
New functions in the 13th version of the IT-Grundschutz Catalogues.....	8
1 IT-Grundschutz - The basis for information security.....	11
2 Layer model and modelling.....	27
3 Roles.....	38
M 1 Common aspects.....	43
M 2 Infrastructure.....	113
M 3 IT-Systems.....	155
M 4 Networks.....	288
M 5 Applications.....	324
T 0 Threat catalogue Basic threats.....	418
T 1 Threat catalogue Force Majeure.....	466
T 2 Threat catalogue Organisational Shortcomings.....	486
T 3 Threat catalogue Human Error.....	695
T 4 Threat catalogue Technical Failure.....	833
T 5 Threat catalogue Deliberate Acts.....	944
S 1 Safeguard catalogues Infrastructure	1142
S 2 Safeguard catalogues Organisation	1269
S 3 Safeguard catalogues Personnel.....	2411
S 4 Safeguard catalogues Hardware and software.....	2625
S 5 Safeguard catalogues Communication.....	3565
S 6 Safeguard catalogues Contingency planning.....	3939

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

4 Controlled Use of Administrative Privileges

2 Inventory and Control of Software Assets

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

3 Continuous Vulnerability Management

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

12 Boundary Defense

8 Malware Defenses

13 Data Protection

9 Limitation and Control of Network Ports, Protocols and Services

14 Controlled Access Based on the Need to Know

10 Data Recovery Capabilities

15 Wireless Access Control

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

16 Account Monitoring and Control

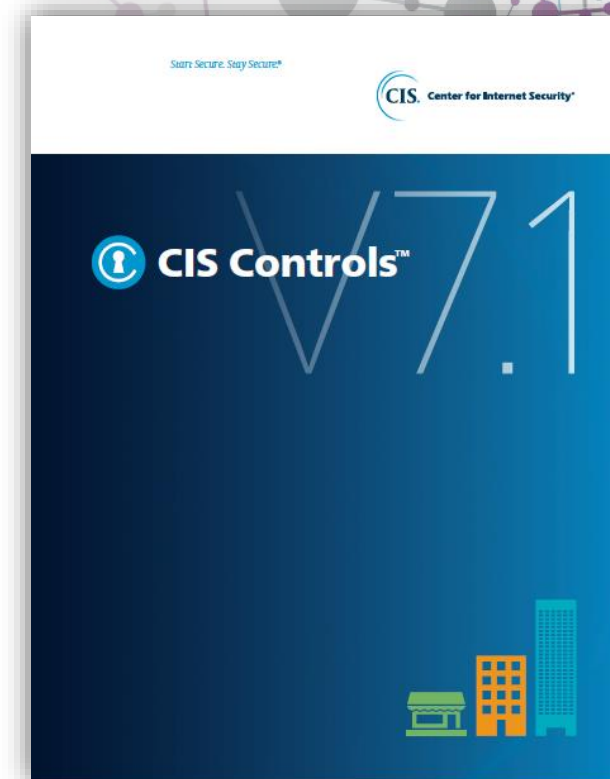
Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises



Чему еще учить

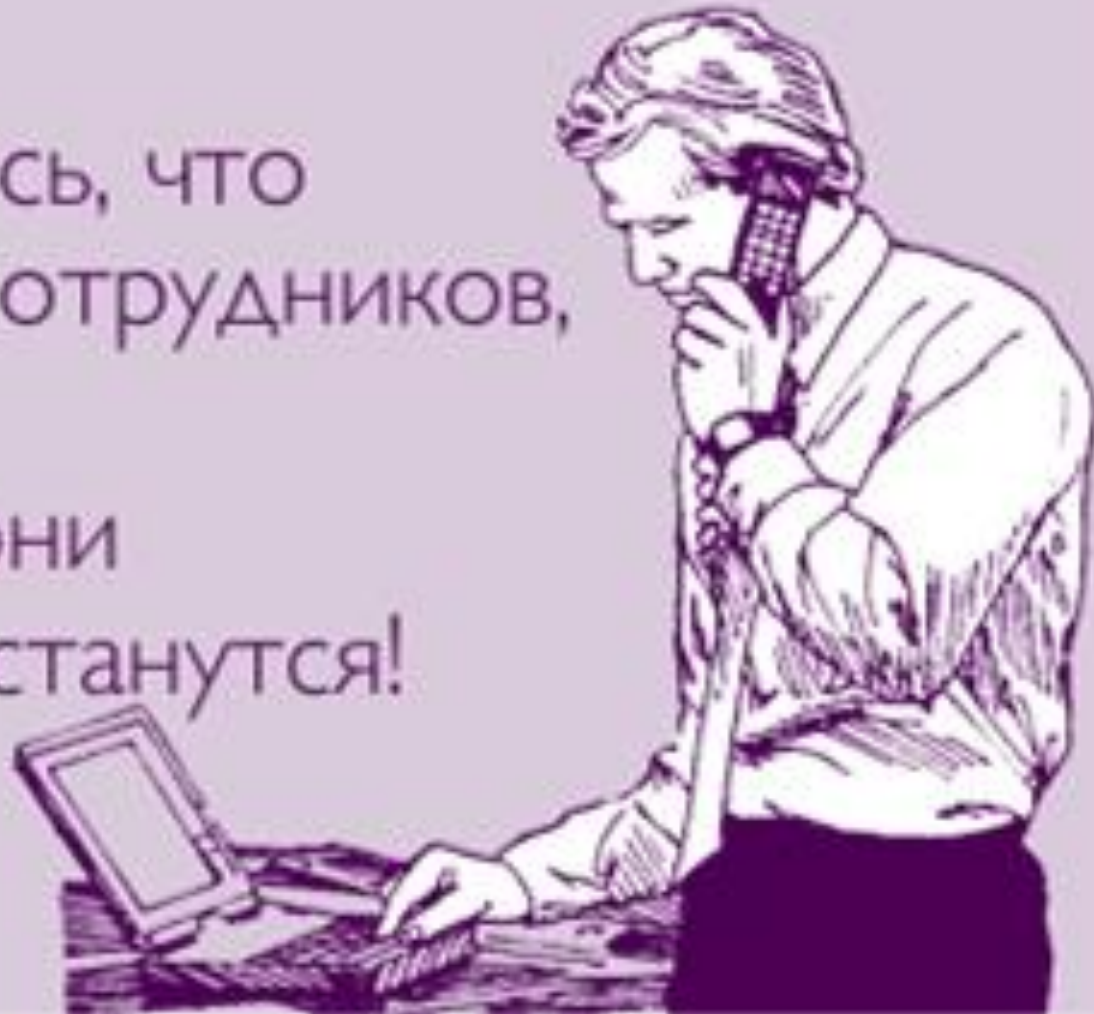
- Коммуникационные навыки
- Презентационные навыки
- Навыки работы в команде
- Управление проектами и тайм-менеджмент
- Английский язык
- Русский язык 😊



Вместо заключения

- А Вы не боитесь, что обучите своих сотрудников, а они уйдут?
- Я боюсь, что они не обучатся и останутся!

 Atkritka.com





КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

ИТОГИ

Спасибо!

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



Информзащита
Учебный центр