



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

hh Информационная безопасность Вакансии Найти Расширенный поиск Работа в России

[Ищу работу](#) [Ищу сотрудников](#) [Помощь](#) [Компании](#) [Проекты](#) [Войти](#)

2 411 вакансий «Информационная безопасность»

по соответствию за месяц На карте Изменить запрос

Регион	
Россия	2221
Москва	1033
Санкт-Петербург	228
Еще 100	

Зарплата	
Указана	901
от 40 000 руб.	666
от 80 000 руб.	322
от 115 000 руб.	180
от 155 000 руб.	93
от 190 000 руб.	58

Специалист по информационной безопасности

IBA Group ✓ ☆
Минск

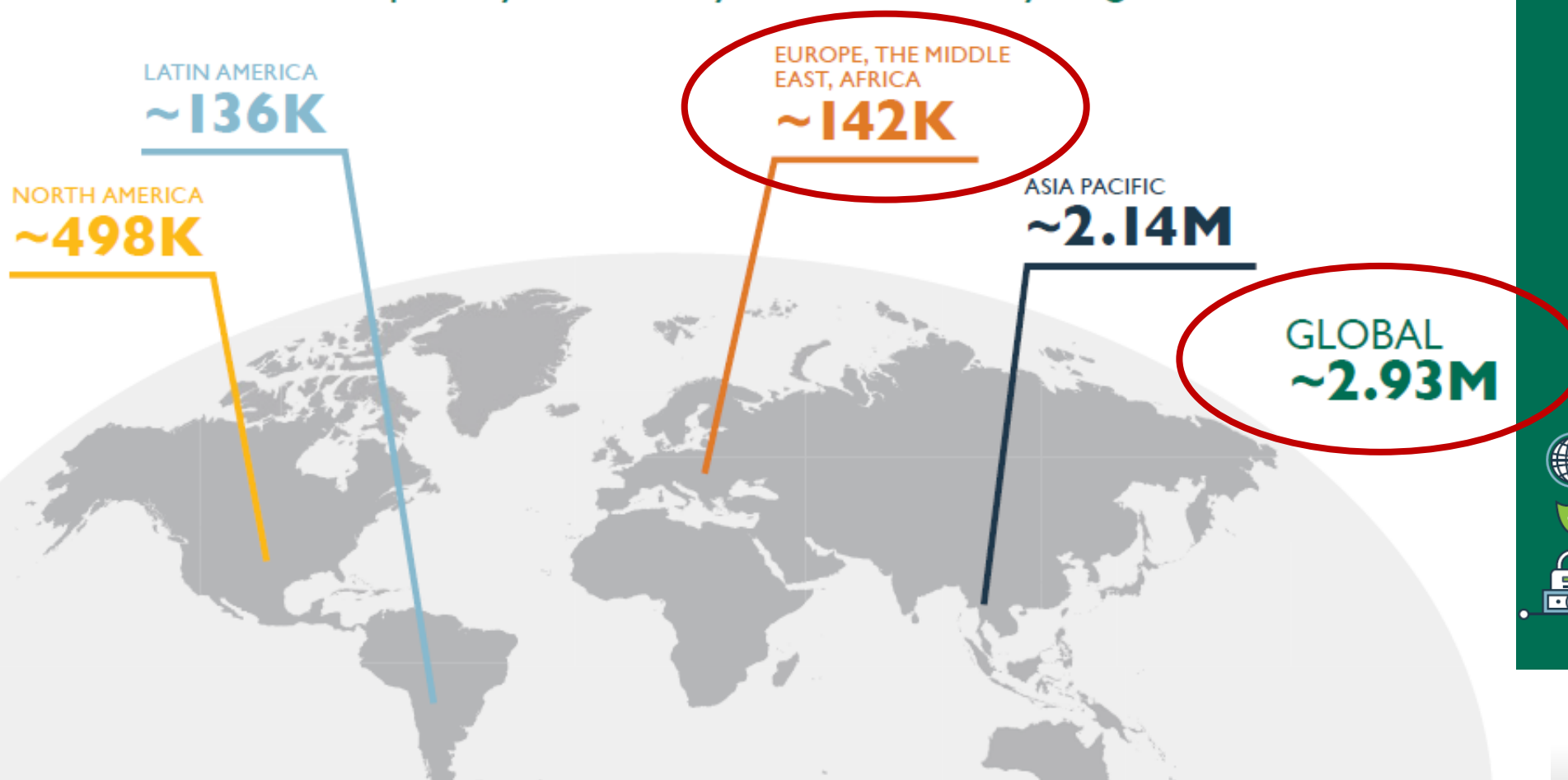
Проектирование и внедрение технических решений по ИБ. Разработка технической документации по проектируемым решениям. Сопровождение и поддержка внедряемых решений и систем...
Образованием в сфере IT. Опыт работы с различными системами **информационной безопасности** (FW/NGFW,WAF, IDS/IPS, Anti-virus, IDM, SIEM...

[Откликнуться](#)

1 ноября

Хорошие новости: Глобальный дефицит безопасников

Gap in Cybersecurity Professionals by Region



(ISC)²

Cybersecurity Professionals
Focus on Developing
New Skills as Workforce
Gap Widens

(ISC)² CYBERSECURITY WORKFORCE STUDY, 2018



Оборотная сторона медали

Плохие новости: Много соискателей работы

The screenshot shows the hh.ru job search interface. At the top, there is a search bar with the text 'Информационная безопасность', a dropdown menu for 'Резюме', and a blue 'Найти' button. To the right of the search bar are links for 'Расширенный поиск' and 'Работа в России' with a Russian flag icon. Below the search bar is a navigation bar with links: 'Ищу работу', 'Ищу сотрудников', 'Помощь', 'Компании', 'Проекты', and 'Войти'. A red oval highlights the search results summary: 'Найдено 141 458 соискателей с 158 159 резюме'. Below this, there are filters for 'Регион' and 'Профобласть'. The 'Регион' filter shows: Россия (140710), Москва (45621), Санкт-Петербург (17615), and 'Еще 385'. The 'Профобласть' filter shows: IT, телеком (65482), Безопасность (52355), Начало карьеры (12507), and 'Еще 25'. The main content area shows a job listing for 'Руководитель подразделения по информационной безопасности' with 36 years of age. It includes a profile picture of a man in a suit, 'Опыт работы 13 лет и 6 месяцев', and 'Последнее место работы: Начальник службы информационной безопасности, iQ-Solutions, Июль 2016 — Декабрь 2017'. The listing was updated on 6 ноября, 06:32. There is a link 'Изменить запрос' in the top right of the listing area.

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

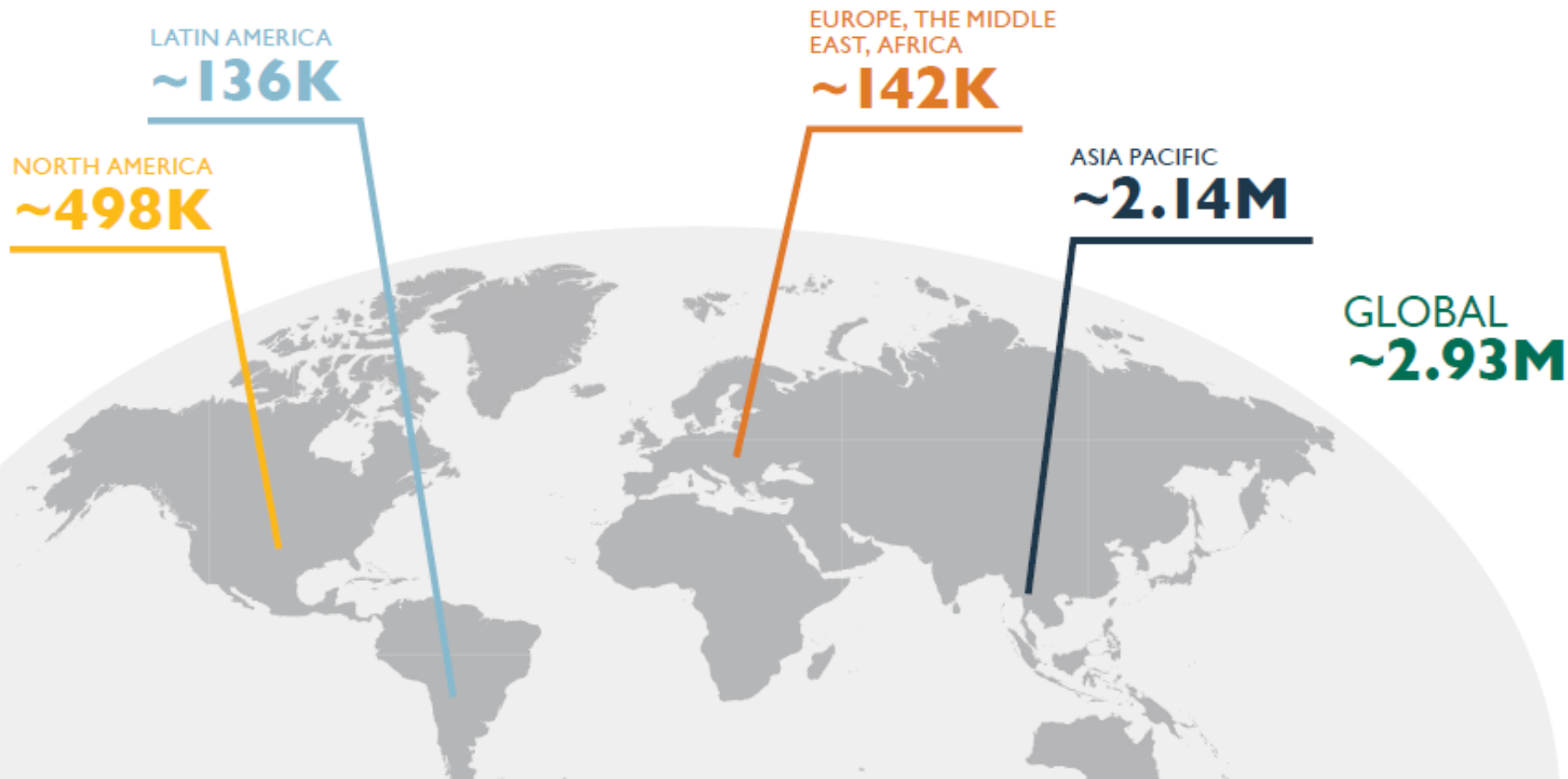
Опыт работы
13 лет и 6 месяцев

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

Обновлено 6 ноября, 06:32

Плохие новости: Ложка дегтя – нужны профессионалы ☹️

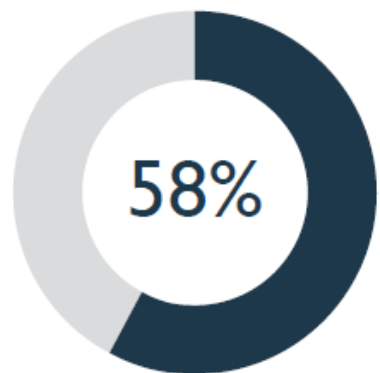
Gap in Cybersecurity Professionals by Region



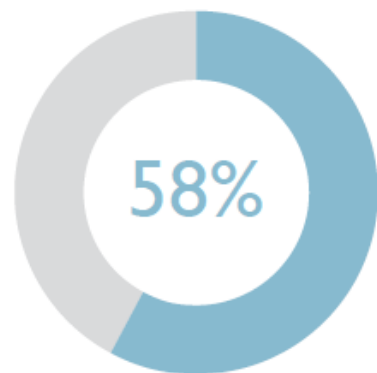
(ISC)²
Cybersecurity Professionals
Focus on Developing
New Skills as Workforce
Gap Widens
(ISC)² CYBERSECURITY WORKFORCE STUDY, 2018

The cover features a green background with white and yellow icons representing cybersecurity concepts like shields, padlocks, and data charts.

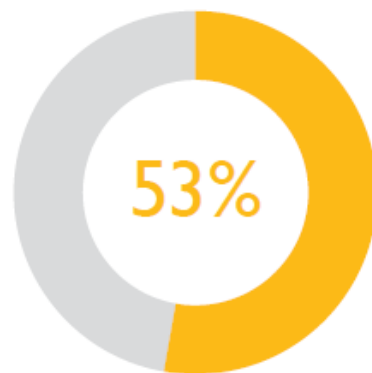
Какие знания должны быть у профессионала?



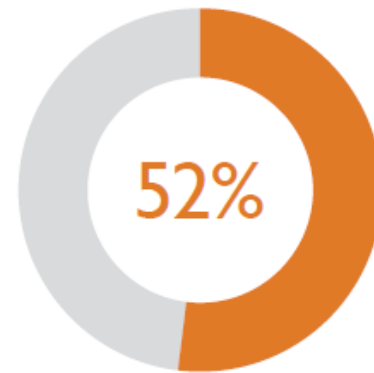
Security awareness



Risk assessment, analysis & management



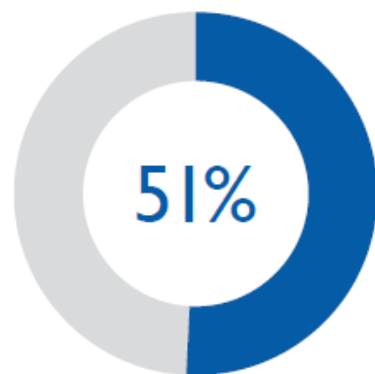
Security administration



Network monitoring



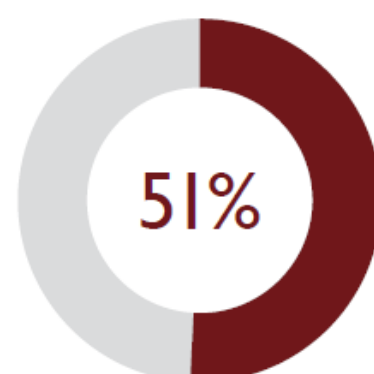
Incident investigation and response



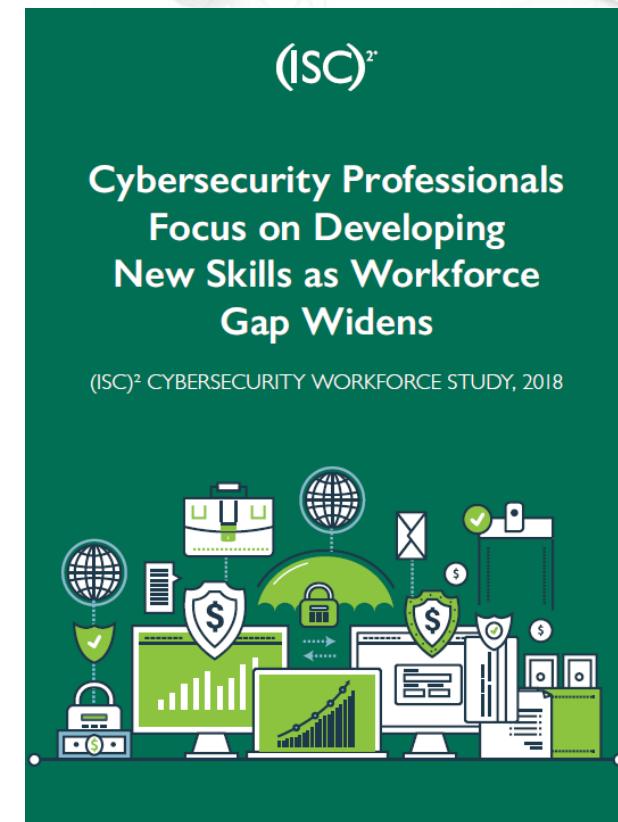
Intrusion detection



Cloud computing security



Security engineering



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

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

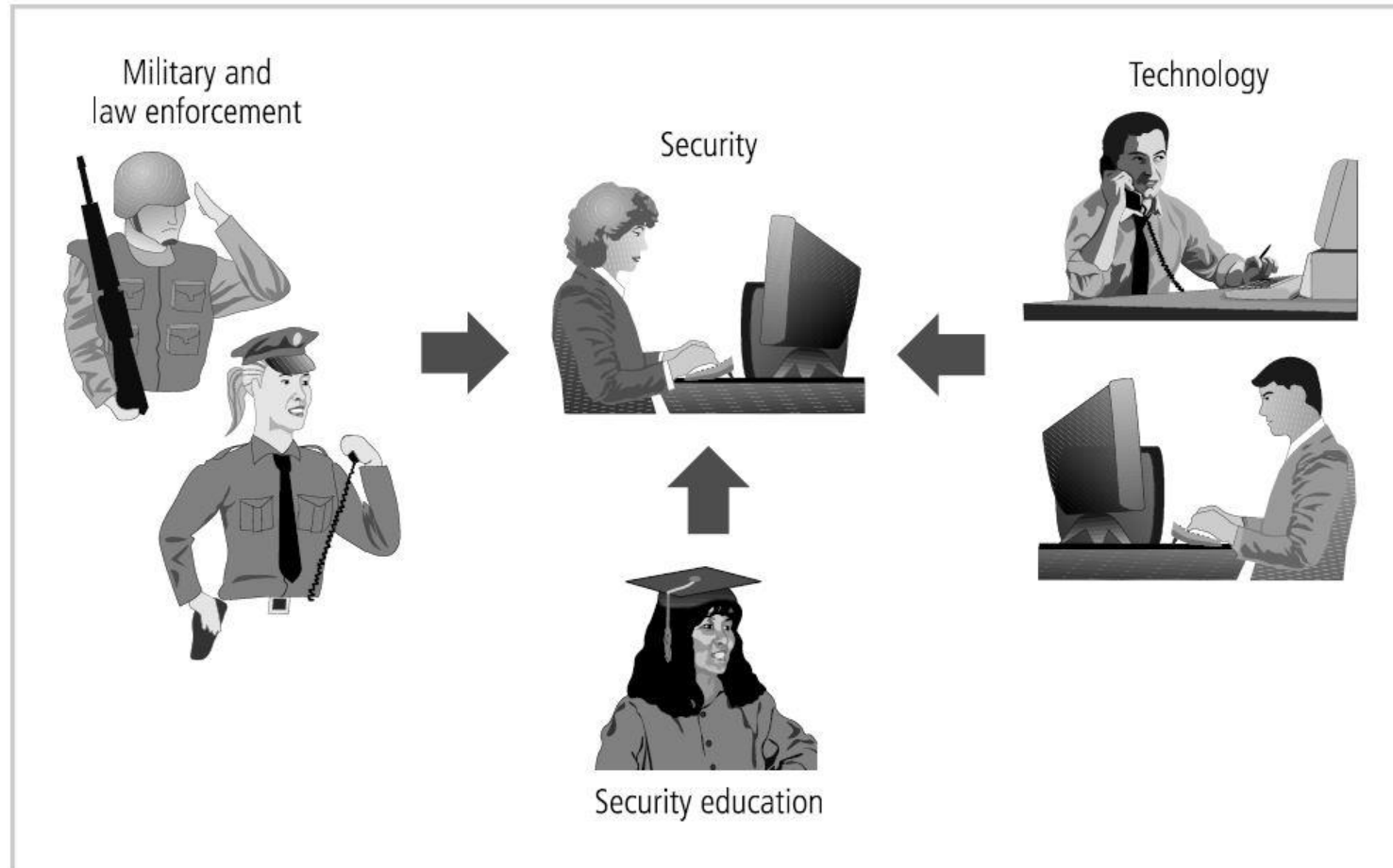
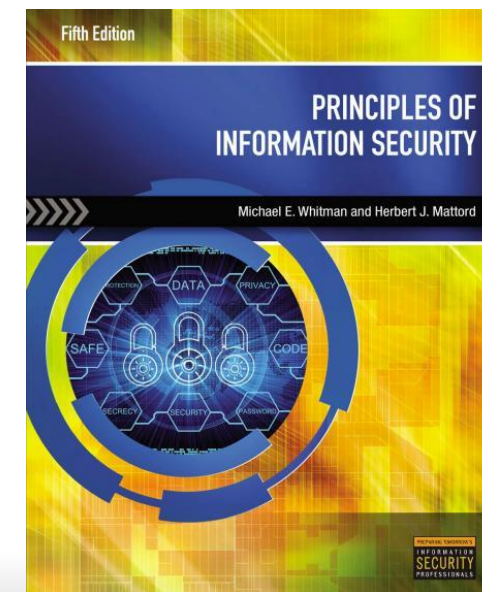


Figure 11-1 Career Paths to Information Security Positions

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



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

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

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)

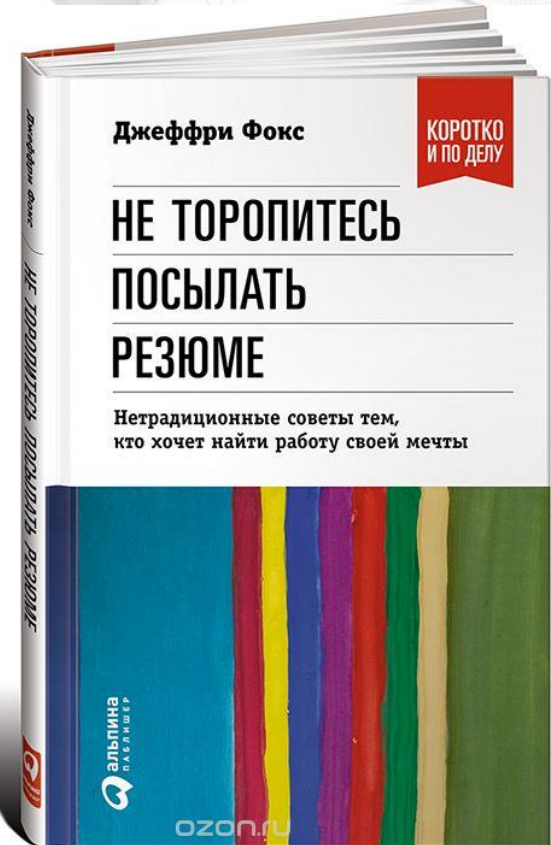
- Участие в реализации требований 382-П, комплекса стандартов СТО БР ИББС
- Разработка нормативных документов по информационной безопасности
- Проведение внутренних аудитов по ИБ
- Контроль соблюдения требований информационной безопасности
- Выявление и расследование инцидентов ИБ
- Проведение обучения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

Чего хотят работодатели (пример вакансии с hh.ru)

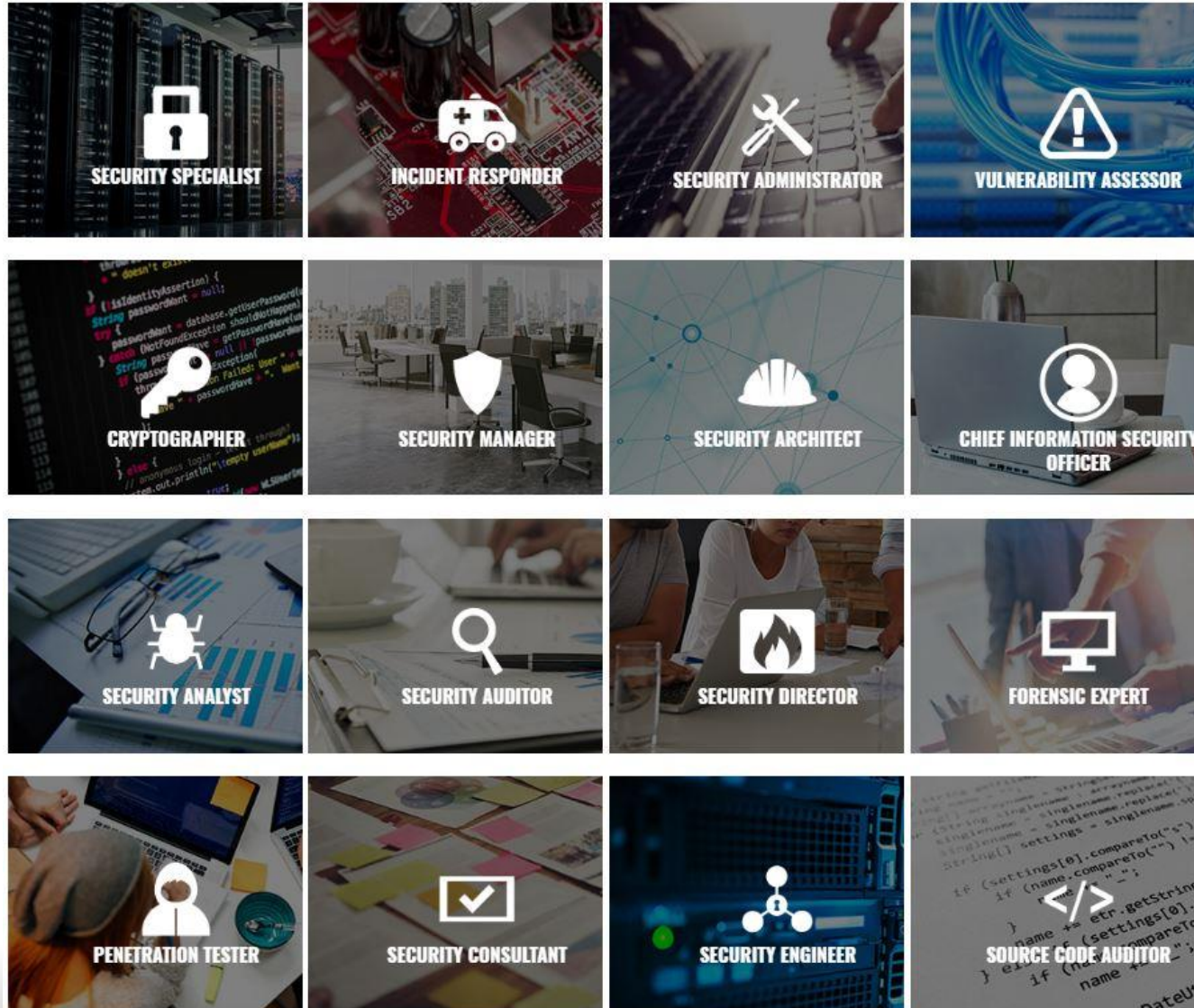
- Анализ информационных рисков компании
- Выявление возможных каналов утечки
- Разработка организационно-распорядительных документов
- Организация и координация работ, проводимых в рамках обеспечения ИБ
- Проведение аудита состояния ИБ
- Установка, настройка и сопровождение технических средств защиты
- 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 😊



Интересные зарубежные ресурсы



**CYBER SECURITY
EDUCATION**

www.cybersecurityeducation.org

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.



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.

Entry-Level

- System Administrator
- Security Administrator
- Network Administrator

Senior-Level

- IT Project Manger
- Security Manager
- Security Consultant
- Security Architect

Executive-Level

- Chief Information Security Officer
- Security Director



**CYBER SECURITY
EDUCATION**



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



Хороший ресурс для планирования карьеры www.cyberseek.org

CyberSeek™ About Interactive map Career pathway Who this tool is for Project partners

Cybersecurity Career Pathway

There are many opportunities for workers to start and advance their careers within cybersecurity. This interactive career pathway shows key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skillsets associated with each role.

[Share](#) [Embed](#)

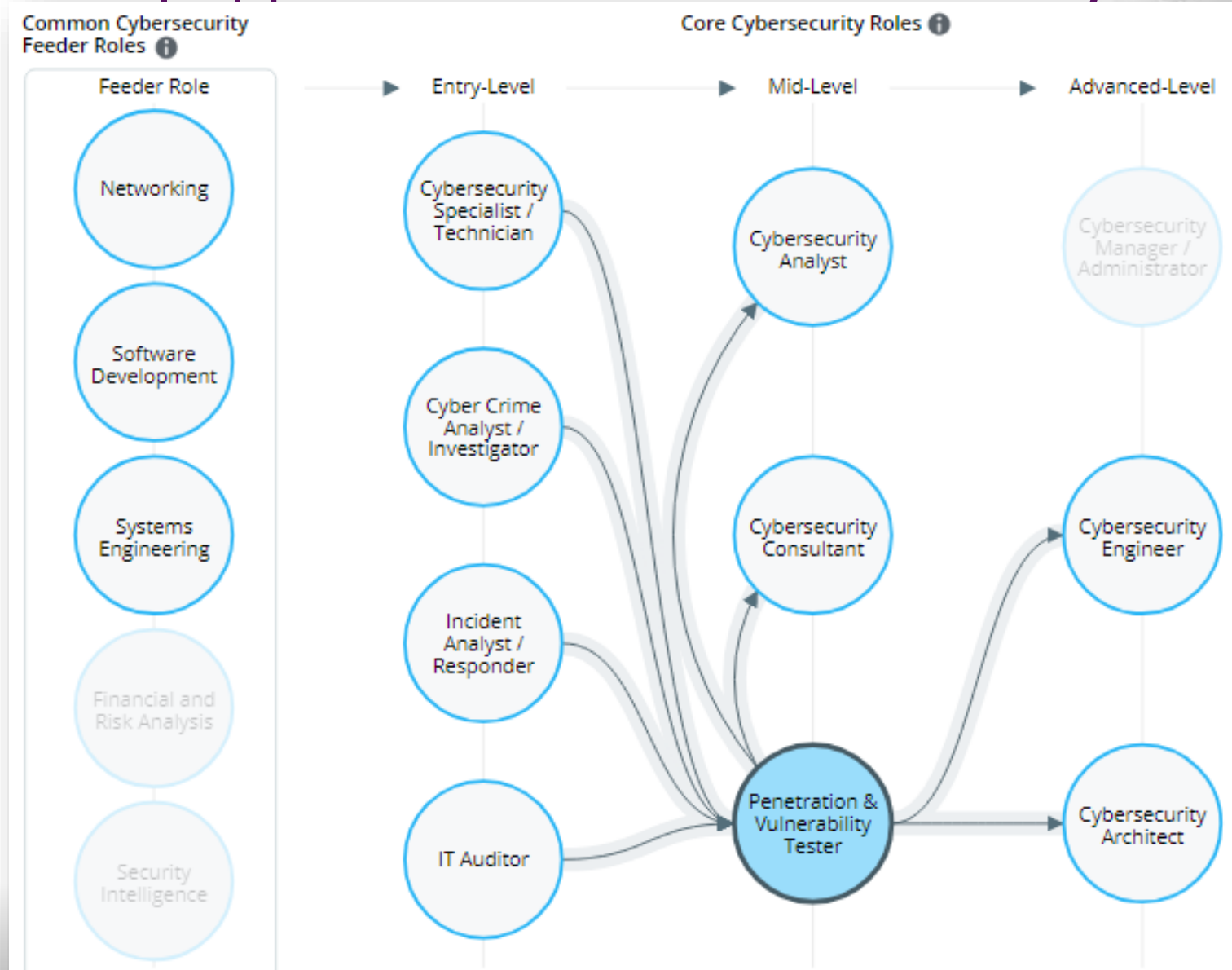
Common Cybersecurity Feeder Roles

- Networking
- Software Development
- Systems Engineering
- Financial and Risk Analysis
- Security Intelligence

Core Cybersecurity Roles

	Entry-Level	Mid-Level	Advanced-Level
	Cybersecurity Specialist / Technician	Cybersecurity Analyst	Cybersecurity Manager / Administrator
	Cyber Crime Analyst / Investigator	Cybersecurity Consultant	Cybersecurity Engineer
	Incident Analyst / Responder	Penetration & Vulnerability Tester	Cybersecurity Architect
	IT Auditor		

Наглядное представление возможных путей



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 ⓘ

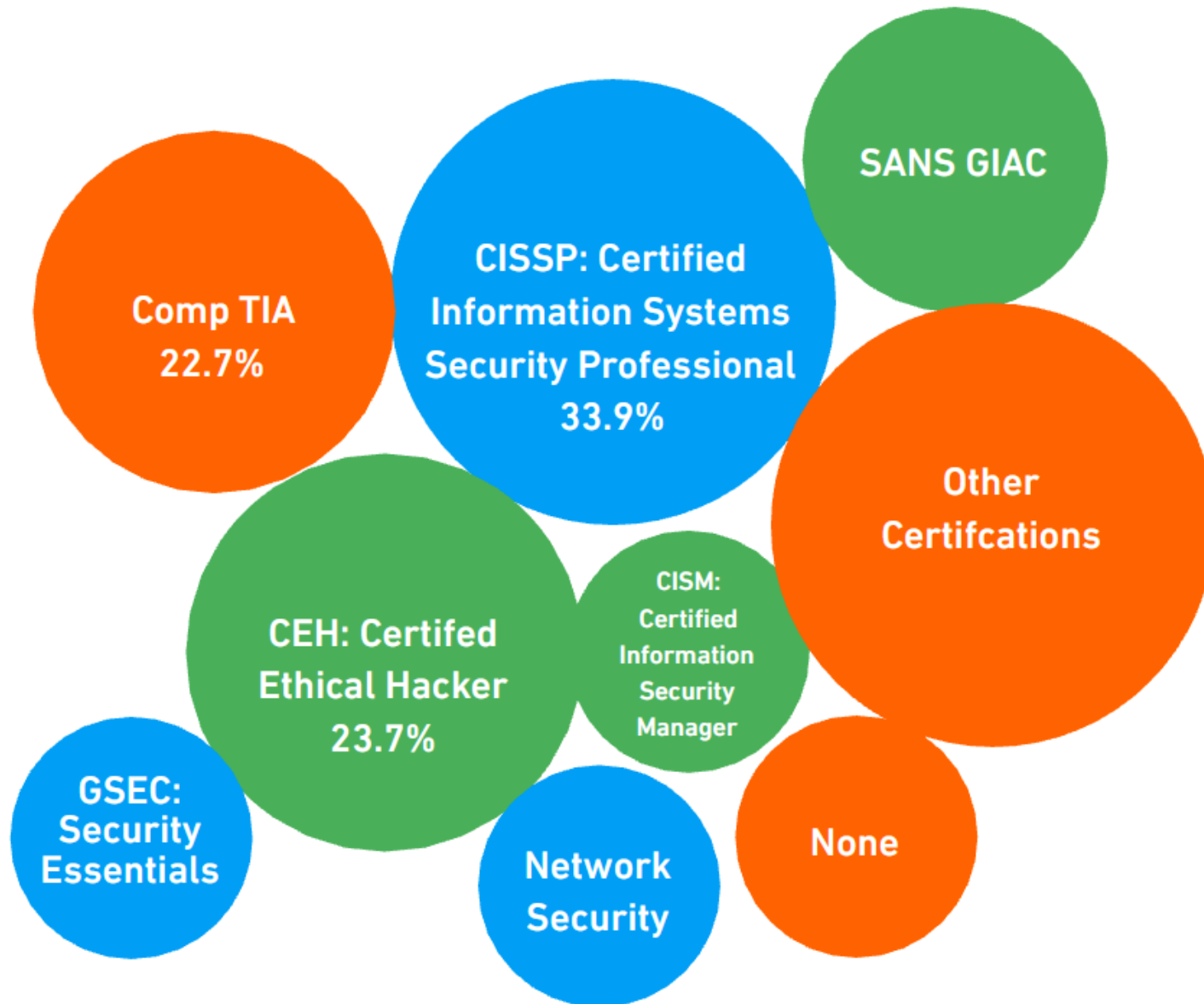
- Analyze
- Protect and Defend

TOP CERTIFICATIONS REQUESTED ⓘ

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



Что еще может быть полезно для карьеры



 **exabeam**

EXABEAM 2018 CYBER SECURITY PROFESSIONALS SALARY AND JOB REPORT:

COMPENSATION, JOB SATISFACTION, EDUCATION, AND TECHNOLOGY OUTLOOK

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

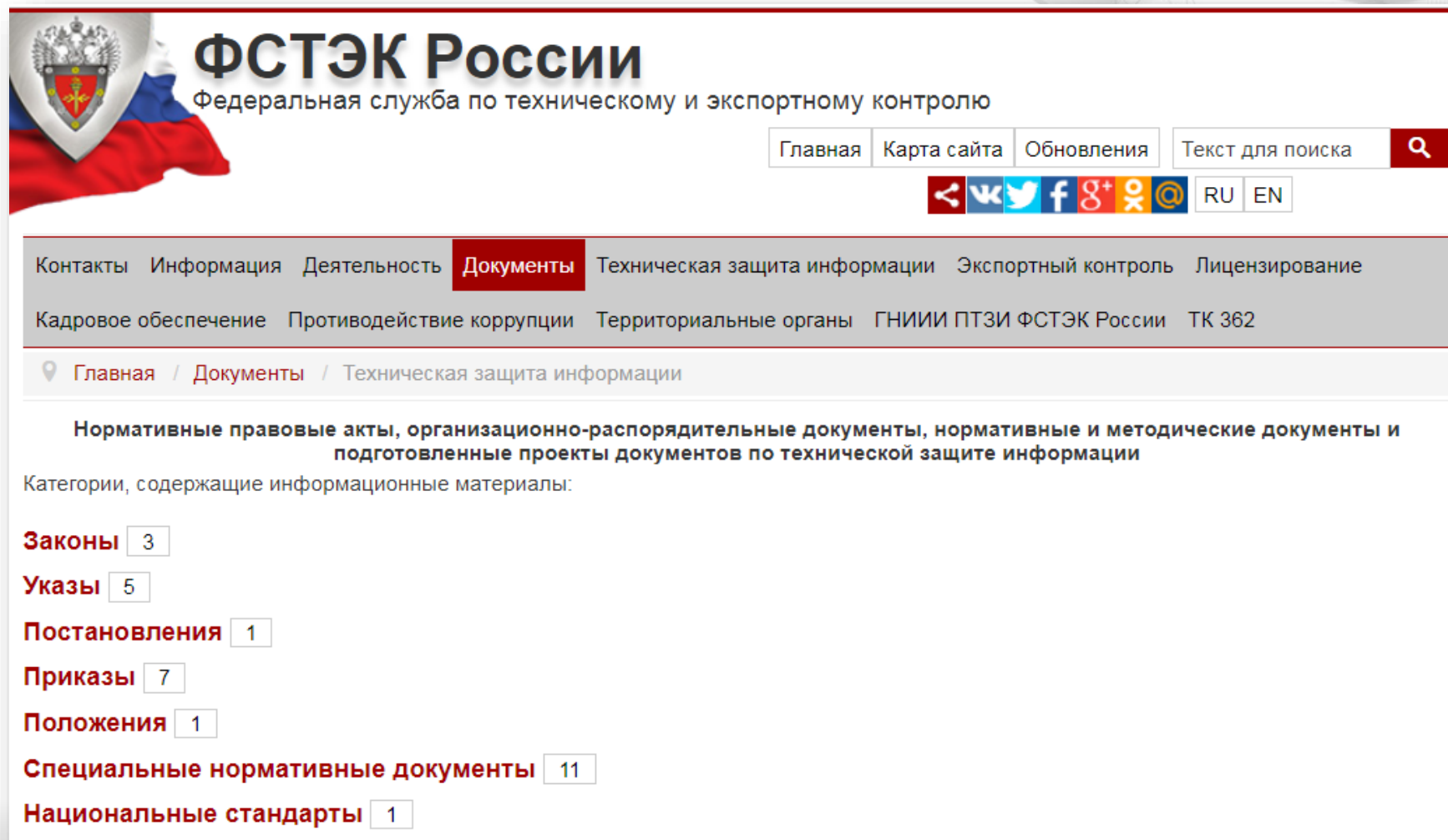
Группы мер обеспечения безопасности
(на примере Приказа ФСТЭК России от 25 декабря 2017 г. N 239 "Об утверждении
Требований по обеспечению безопасности значимых объектов критической
информационной инфраструктуры Российской Федерации")

	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) (COB)	*								*	*	*											*			*
VIII. Обеспечение целостности (ОЦЛ)																							*		*
IX. Обеспечение доступности (ОДТ)		*																							
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)																									
ЗИС.2,4,5 Защита периметра, сегментирование, 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/>



ФСТЭК России
Федеральная служба по техническому и экспортному контролю

Главная Карта сайта Обновления Текст для поиска 🔍

[RU](#) [EN](#)

Контакты Информация Деятельность **Документы** Техническая защита информации Экспортный контроль Лицензирование

Кадровое обеспечение Противодействие коррупции Территориальные органы ГНИИИ ПТЗИ ФСТЭК России ТК 362

📍 Главная / Документы / Техническая защита информации

Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации

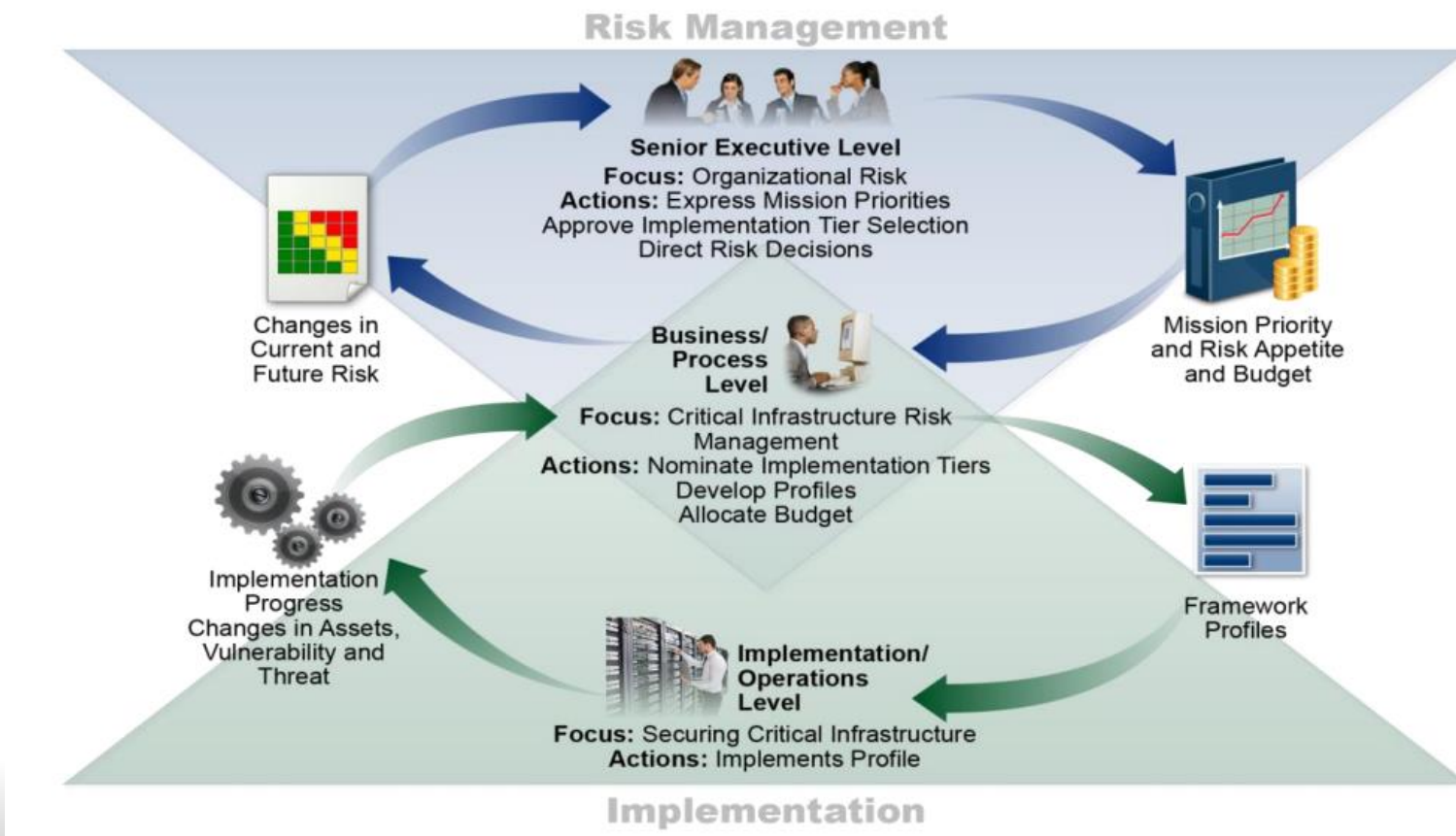
Категории, содержащие информационные материалы:

- Законы** 3
- Указы** 5
- Постановления** 1
- Приказы** 7
- Положения** 1
- Специальные нормативные документы** 11
- Национальные стандарты** 1

Изучайте международные документы

■ NIST Cybersecurity Framework

■ <https://www.nist.gov/cyberframework>



Используйте лучшие практики

■ CIS Critical Security Controls for Effective Cyber Defense

■ <https://www.sans.org/critical-security-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

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



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



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/>
- Емельяников 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



МЕЖДУНАРОДНАЯ
АКАДЕМИЯ
ЭКСПЕРТИЗЫ И ОЦЕНКИ

Профессиональная переподготовка по
программе «Информационная безопасность»

8 800 234 17 05

звонок по России бесплатный

Дистанционное обучение **специалистов** по **информационной безопасности** за 6 месяцев

На время осеннего периода предоставляем **15 льготных мест**
по цене ~~42 000 руб.~~ **30 000 руб.** (самая выгодная цена в России)

Осталось льготных мест: **0 3**

Зарезервируйте место по льготной цене:

В течение 1 минуты вам на почту придёт учебный план, документы для поступления и доп. информация

Введите Ваш e-mail



Введите Ваш телефон



ОСТАВЬТЕ ЗАЯВКУ

Нажимая на кнопку, вы даете согласие на
обработку своих персональных данных

Иностранным абитуриентам

Подарить обучение



В любом городе России.
Для занятий нужен только
компьютер и интернет



Подарок выпускникам:
квалификационный сертификат
соответствия профстандарту

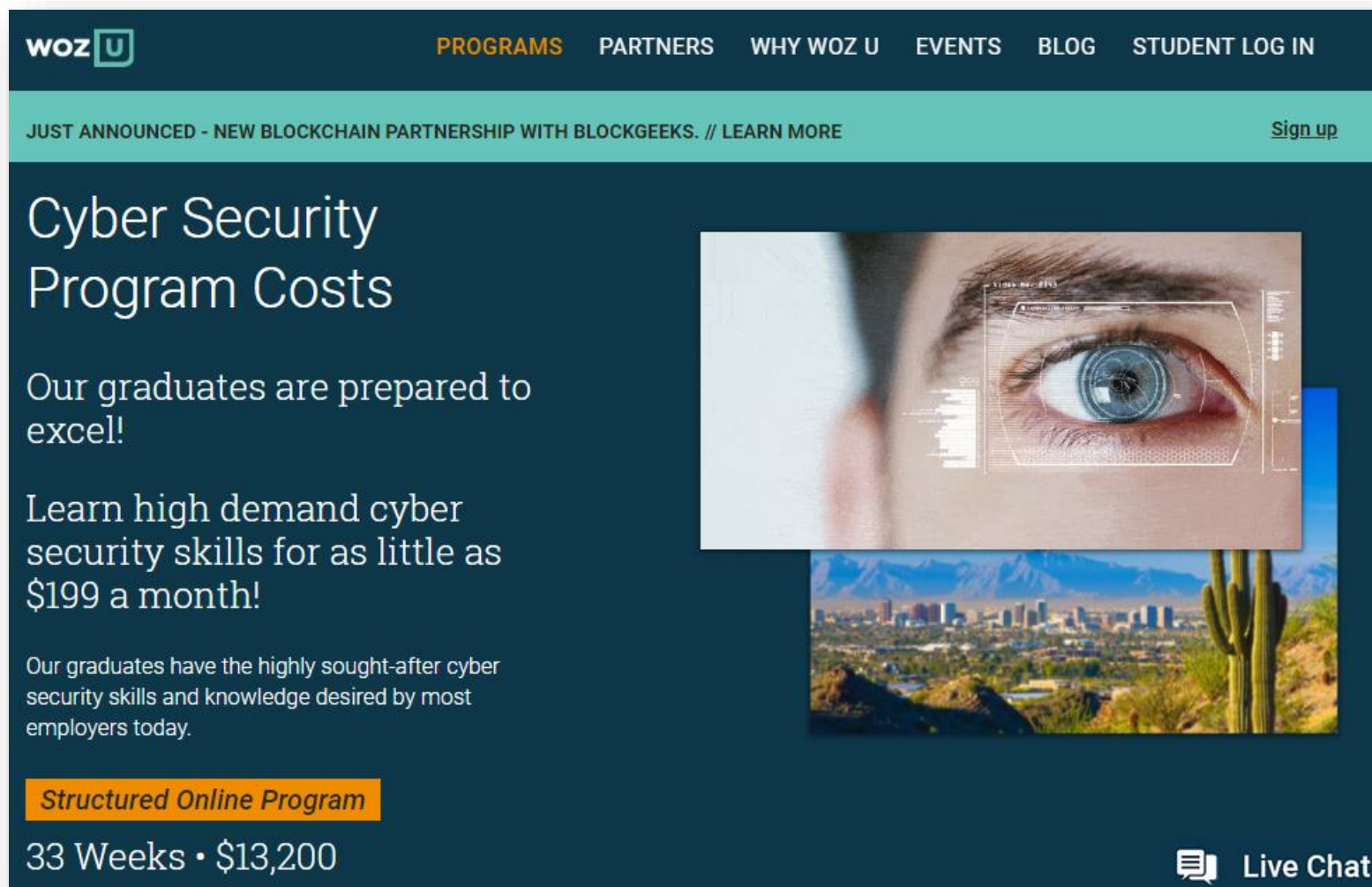


Старт ближайшей группы:
1 ноября 2018 года



Информзащита
Учебный центр

Про меркантильное



woz U PROGRAMS PARTNERS WHY WOZ U EVENTS BLOG STUDENT LOG IN

JUST ANNOUNCED - NEW BLOCKCHAIN PARTNERSHIP WITH BLOCKGEEKS. // [LEARN MORE](#) [Sign up](#)

Cyber Security Program Costs


Our graduates are prepared to excel!

Learn high demand cyber security skills for as little as \$199 a month!

Our graduates have the highly sought-after cyber security skills and knowledge desired by most employers today.

Structured Online Program

33 Weeks • \$13,200

 Live Chat



CYBER SECURITY

NETWORK FOUNDATIONS



SECURITY FOUNDATIONS



NETWORK DEFENSE



SYSTEM ADMINISTRATION



LOGGING AND MONITORING



CRYPTOGRAPHY AND ACCESS MANAGEMENT



WEB APPLICATION SECURITY



PROGRAMMING FOUNDATIONS



THREATS AND VULNERABILITIES



PROJECT MANAGEMENT



Ваш надежный помощник 😊



Информзашита
Учебный центр

+7 (495) 980-23-45 (*04)

edu@itsecurity.ru



Личный кабинет
Зарегистрироваться

Мы обучили

70715

специалистов

Курсы Расписание курсов **Обучение** Повышение осведомленности Контакты Учебный центр Поиск по сайту

Главная страница • Обучение

Концепция планирования компетентностного роста «Матрица»

Навигатор по обучению по ИБ и по ЭБ

Комплексные учебные программы по обучению по информационной, экономической и кадровой безопасности

Повышение квалификации по ИБ

Повышение квалификации по ЭБ

Переподготовка для лицензиатов ФСБ России более 500 часов

Переподготовка для лицензиатов ФСТЭК России более 360 часов

Обучение по защите гос. тайны

Очное обучение по ИБ и по ЭБ

Дистанционное обучение

Электронные курсы

Корпоративное обучение

Выездное обучение

Видекурсы для физ.лиц

Оплата обучения

Условия обучения

СВЕЖИЕ НОВОСТИ

"Матрица" - концепция планирования компетентностного роста

Чаще всего люди приходят учиться в двух случаях:

- когда перед ними встанут новые задачи, пути и способы решения которых они не в полной мере представляют,
- впрок, чтобы заложить некоторый базис для решения задач в будущем.

В первом случае Вы понимаете, чему Вы хотите научиться, и остается выбрать только уровень комплексной программы, с которого Вам необходимо начать обучение, чтобы не терять время на повторение уже известного вам материала.

Учиться "впрок" сложнее, так как перечень будущих задач не в полной мере определен. Учиться вообще всему - идеально, но долго и дорого. Профессионально занимаясь вопросами обеспечения информационной безопасности организаций, мы пришли к выводу, что вне зависимости от организационно-штатной структуры компаний в них можно выделить 5 четких ролей в процессе обеспечения безопасности (что четко следует из пятиуровневой модели системы управления информационной безопасностью организации):

- **руководитель** подразделения, непосредственно отвечающий за состояние безопасности ИТ и организацию работ по созданию КСЗИ в автоматизированной системе (АС);
- **аналитики**, отвечающие за анализ состояния безопасности ИТ, определение требований к защищенности различных подсистем АС (в том числе в разрабатываемых прикладных подсистемах) и путей обеспечения их защиты, а также за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации;
- **аудиторы**, контролирующие текущее состояние системы защиты на предмет соответствия ее заявленным целям;
- **администраторы** средств защиты, контроля защищенности и управления безопасностью, отвечающих за сопровождение и администрирование штатных и дополнительных средств защиты информации и средств анализа защищенности подсистем АС;
- **специалисты** по работе с конечными пользователями и обслуживающим персоналом АС, отвечающие за реализацию и контроль исполнения регламентов безопасной обработки информации в АС.



www.itsecurity.ru



Информзашита
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 РКИ (3 дня)

Специализация

- БТ31 Безопасность Windows 7/8.1/10/2012R2/2016 (5 дней)
- БТ12 Безопасность сетей на базе Linux (Unix) (5 дней)
- 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)



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 РКІ на основе ПАК «КриптоПро УЦ» 2.0 (3 дня)

Курсы вендоров

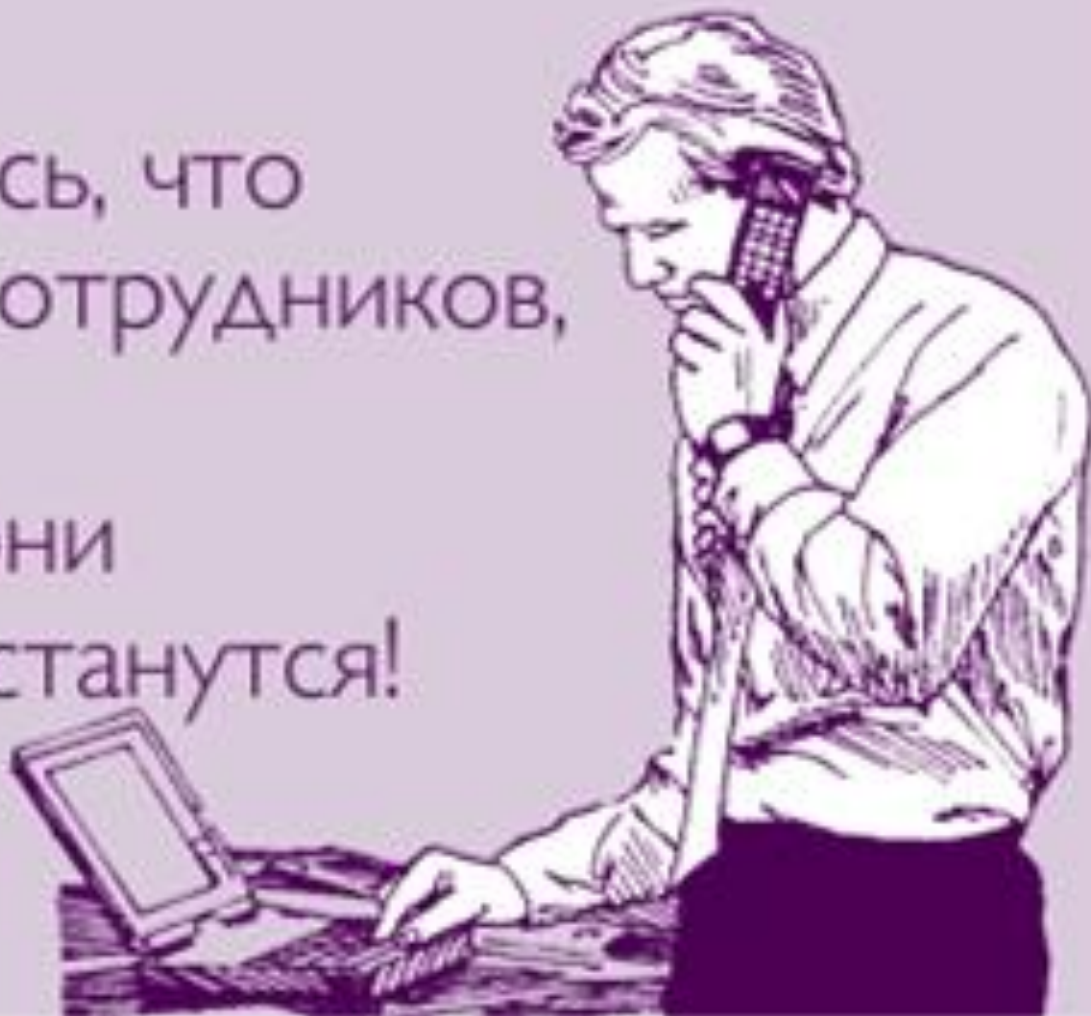
- Позитив Технолоджис
- Лаборатория Касперского
- Код Безопасности
- Крипто Про
- Аладдин Р.Д.
- HP ArcSight
- Microsoft
- CheckPoint
- Cisco

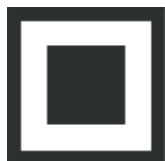


Вместо заключения

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

Atkritka.com





КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ



Информзащита
Учебный центр

Спасибо!

Андрей Степаненко

a.stepanenko@itsecurity.ru

(495) 980-2345 доб. 826

www.itsecurity.ru