Академия
Информационных
Систем

КОМПЕТЕНЦИИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ

Хайров Игорь
Заместитель директора Академии Информационных Систем,
канд.техн.наук
8(495)120-04-02, security@infosystem.ru
www.infosystems.ru
www.vipforum.ru

Москва, 2020

ГОСУДАРСТВЕННО РЕГУЛИРОВАНИЕ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Заседание Совета Безопасности РФ – поручения Президента Российской Федерации (**июль 2015, октябрь 2017 г**.)
- Заседание МВК по ИБ Совета Безопасности РФ

  (8 июня 2018 г., 9 октября 2018 г., 9 октября 2019 г.)
- Постановление Правительства РФ от **6 мая 2016 года № 399** «Об организации повышения квалификации специалистов по защите информации … в органах государственной власти и местного самоуправления».
- Концепция развития кадрового обеспечения в области информационной безопасности в РФ на долгосрочную перспективу и план ее реализации (утв. Заместителем Председателя Правительства РФ **30 мая 2017 г. № 365п-П4**).
- Федеральный проект «Информационная безопасность» национальной программы «Цифровая экономика РФ»

(Утв. Правительственной комиссией **27 декабря 2018 протокол № 6**)

ПРОФЕССИОНАЛЬНЫЕ СТАНДАРТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Код и наименование профессионального стандарта		Задачи специалиста
12.004	Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак	Разработка и эксплуатация систем обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы
12.005	Специалист по противодействию иностранным техническим разведкам	Противодействие иностранным техническим разведкам
06.030	Специалист по защите информации в телекоммуникационных системах и сетях	Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним
06.031	Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности	Автоматизация информационно-аналитической деятельности (АИАД) в государственных органах, обеспечивающих национальную безопасность
06.032	Специалист по безопасности компьютерных систем и сетей	Защита информации в компьютерных системах и сетях
06.033	Специалист по защите информации в автоматизированных системах	Обеспечение безопасности информации в автоматизированных системах
06.034	Специалист по технической защите информации	Техническая защита информации

Примеры должностей в профессиональных стандартах			
Администратор баз данных	Инженер по защите информации	Инженер-разработчик систем защиты информации	Специалист по защите информации в компьютерных системах и сетях
Администратор безопасности компьютерных систем и сетей	Инженер по телекоммуникациям	Консультант по специальным телекоммуникациям	Специалист по технической защите информации
Администратор по обеспечению безопасности информации	Инженер по технической защите информации	Научный консультант	Техник по безопасности компьютерных систем и сетей
Администратор сети	Инженер специальной связи	Научный консультант по защите информации	Техник по защите информации
Администратор телекоммуникационного оборудования	Инженер-программист	Научный сотрудник	Техник по обслуживанию телекоммуникационного оборудования
Дизайнер баз данных	Инженер-программист по технической защите информации	Руководитель проектов	Техник по технической защите информации
Инженер	Инженер-проектировщик	Системный аналитик	Эксперт по анализу защищенности компьютерных систем и сетей
Инженер - системный программист	Инженер-разработчик	Специалист по защите информации	

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

«Практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз»

Это означает связь и развитие профессиональной деятельности специалиста по информационной безопасности с разрабатываемыми информационными технологиями.

НАПРАВЛЕНИЯ РАЗВИТИЯ ИКТ В ЦИФРОВОМ МИРЕ

Направления развития ИКТ в среднесрочной перспективе (3-5 лет)*

ИКТ будет дополнена следующими **объектами профессиональной деятельности**:

- квантовые технологии и квантовая криптография;
- системы, реализующие облачные, туманные технологии;
- системы дополненной реальности, а также системы, реализующие функционал искусственного интеллекта,
- объекты критической информационной инфраструктуры;
- социальные сети;
- интернет вещей (IoT)

Направления, тенденции, возможности развития технологий, появление инноваций в ИКТ

- Повсеместный переход на мобильные устройства;
- Заказная разработка и поддержка программных продуктов;
- Производство тиражного программного обеспечения (для "облачных" технологий; для систем автоматизации бизнеса; для технологий обработки больших массивов данных; для приложений мобильных устройств);
- Массовое оборудование датчиками и исполнительными устройствами материальных объектов и их подключение к сетевой инфраструктуре;
- Интеллектуальные устройства и интернет-сервисы;
- Вывод служб, занимающихся информационными технологиями на предприятиях и в организациях, на аутсорсинг;
- Дальнейшее внедрение информационных технологий в управление бизнесом, автоматизацию государственного сектора, глобализацию рынка информационных технологий;
- Интернет-программирование и разработка интернет-сервисов;
- Совершенствование инструментов электронной коммерции

ПРОФИЛИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

США *по данным сайта*
https://www.cybersecurityeducation.org/

1. Security specialist (Специалист по безопасности)
2. Incident responder (Специалист по реагированию на инциденты)
3. Security administrator (Администратор безопасности)
4. Vulnerability assessor (Специалист по оценке уязвимостей)
5. Cryptographer (Специалист по шифрованию)
6. Security manager (Менеджер безопасности)
7. Security architect (Архитектор безопасности)
8. Chief information security officer (Главный сотрудник по информационной безопасности)
9. Security analist (Аналитик по безопасности)
10. Security auditor (Аудитор безопасности)
11. Security director (Директор по безопасности)
12. Forensic expert (Судебный эксперт)
13. Penetration tester (Специалист по тестированию на проникновение)
14. Security consultant (Консультант по безопасности)
15. Security engineer (Инженер по безопасности)
16. Source code auditor (Аудитор исходного кода)

Россия

Среднее профессиональное образование		
10.02.01	Организация и технология защиты информации	Техник по ЗИ (с 2019 г. набора НЕТ)
10.02.02	Инф. безопасность телекоммуникационных систем	Техник по ЗИ (с 2019 г. набора НЕТ)
10.02.03	Инф. безопасность автоматизированных систем	Техник по ЗИ (с 2019 г. набора НЕТ)
10.02.04	Обеспечение ИБ телекоммуникационных систем	Техник по ЗИ
10.02.05	Обеспечение ИБ автоматизированных систем	Техник по ЗИ
Высшее образование		
10.03.01	Информационная безопасность	Бакалавр
10.04.01	Информационная безопасность	Магистр
10.05.01	Компьютерная безопасность	Специалист по ЗИ
10.05.02	Инф. безопасность тел-коммун. систем	Специалист по ЗИ
10.05.03	Инф. безопасность автоматизированных систем	Специалист по ЗИ
	Информационно-аналитические системы	
10.05.05	Безопасность инф. технологий в правоохранит. сфере	Специалист по ЗИ
10.05.06	Криптография	Специалист по ЗИ
10.05.07	Противодействие техническим разведкам	Специалист по ЗИ
Подготовка кадров высшей квалификации		
10.06.01	Информационная безопасность	Исследователь.
10.07.01	(аспирантура, адъюнктура)	Преподаватель-исследователь

СПЕЦИАЛЬНОСТИ, ВОСТРЕБОВАННЫЕ ПРАКТИКОЙ

Специалисты в области информационной безопасности остаются остро востребованными. По оценкам ряда экспертов потребность государства в таких специалистах удовлетворяется примерно на 50 %.

Квалификации и компетенции специалистов в области информационной безопасности отражены в соответствующих профессиональных стандартах.

Эксперты также отмечают необходимость следующих специалистов:

Эксперт по кибербезопасности;

Эксперт по анализу данных для выявления мошенничества;

Аналитик по выявлению атак повышенной сложности;

Аналитик по киберразведке;

Аналитик по защищенности систем;

Аналитик данных;

Эксперт по blockchain;

Эксперт по искусственному интеллекту;

Инженер по робототехнике;

Аналитик по киберфизическим устройствам;

Инженер для «Интернет вещей»;

Специалист по дополненной реальности.

Намечается тенденция развития аналитической и экспертной деятельности.

Необходимо уточение формулировок (например, «Аналитик по киберфизическим устройствам» и «Инженер для «Интернет вещей» могут быть объединены в один профстандарт «Специалист-аналитик по киберфизическим устройствам»)

НОВЫЕ КОМПЕТЕНЦИИ И ОЖИДАНИЯ ОТ СОТРУДНИКОВ

В группе Soft skills:

- Инновационность и digital-навыки;
- Системное мышление и решение проблем;
- Развитие команд и сотрудничество;
- Управление результатом и ответственность;
- Управление собой;
- Клиентоориентированность.

В группе Hard skills:

- Развитие новых профессиональных компетенций и знаний;
- Технический бэкграунд;
- Владение языком бизнеса и бизнес-процессов организации;
- Уникальный опыт;
- Менеджмент (проекты, процессы и операции);
- Программирование и промышленная разработка ПО;
- Английский язык, грамотная речь, умение презентовать работу.

Компетенции будущего:

White team. Тестируют и пытаются найти слабости во всех новых цифровых приложениях и продуктах Банка перед их запуском в продукт

Red team. Атакуют промышленные приложения, пытаясь найти уязвимости, а также занимаются провокациями в отношении сотрудников, в том числе с использованием инструментов социальной инженерии

Hunters. Пытаются обнаружить в ИТ-системах банка скрытые внедренные вирусы, в том числе «спящие», подозрительный трафик и т.д.

Data scientists. Аналитики, моделисты. Математика «больших данных» и наука машинного обучения, разработка гипотез, аналитических моделей кибербезопасности и проверка их на практике.

ПОТРЕБНОСТЬ В СПЕЦИАЛИСТАХ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Качественные изменения в спросе на специалистов в среднесрочной перспективе (в течение 3-5 лет)

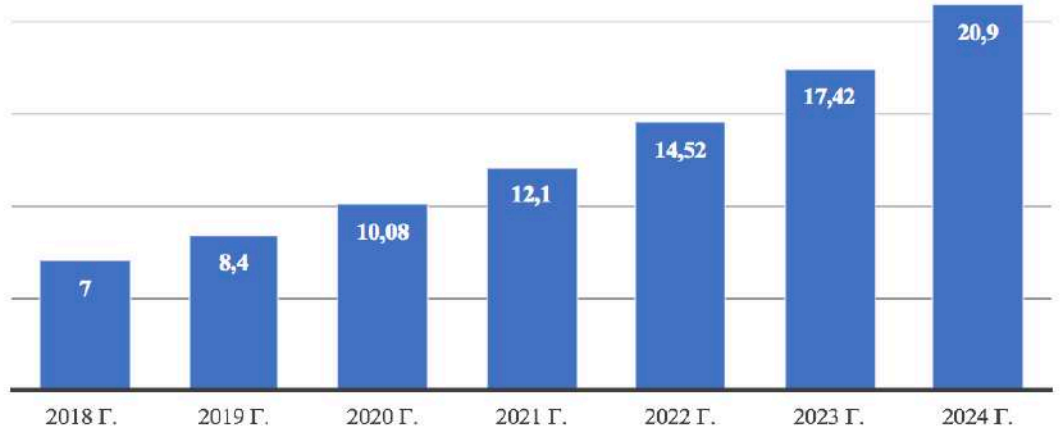
Экспертное мнение

В среднесрочной перспективе качественные изменения в спросе на специалистов будут связаны с востребованностью следующих специалистов:

- специалисты по квантовой криптографии;
- специалисты по обеспечению информационной безопасности объектов критической информационной инфраструктуры;
- специалисты по обеспечению информационной безопасности социотехнических систем;
- специалисты по обеспечению информационной безопасности интернет вещей (IoT).
- эксперт по кибербезопасности;
- эксперт по анализу данных для выявления мошенничества;
- аналитик по выявлению атак повышенной сложности;
- аналитик по киберразведке;
- аналитик по защищенности систем;
- аналитик данных;
- эксперт по blockchain;
- эксперт по искусственному интеллекту;
- инженер по робототехнике;
- аналитик по киберфизическим устройствам;
- инженер для «Интернет вещей»;
- специалист по дополненной реальности.

Ожидаемая потребность в подготовке специалистов по информационной безопасности в 2020-2024 г., тыс. чел.

Федеральный проект «Информационная безопасность»

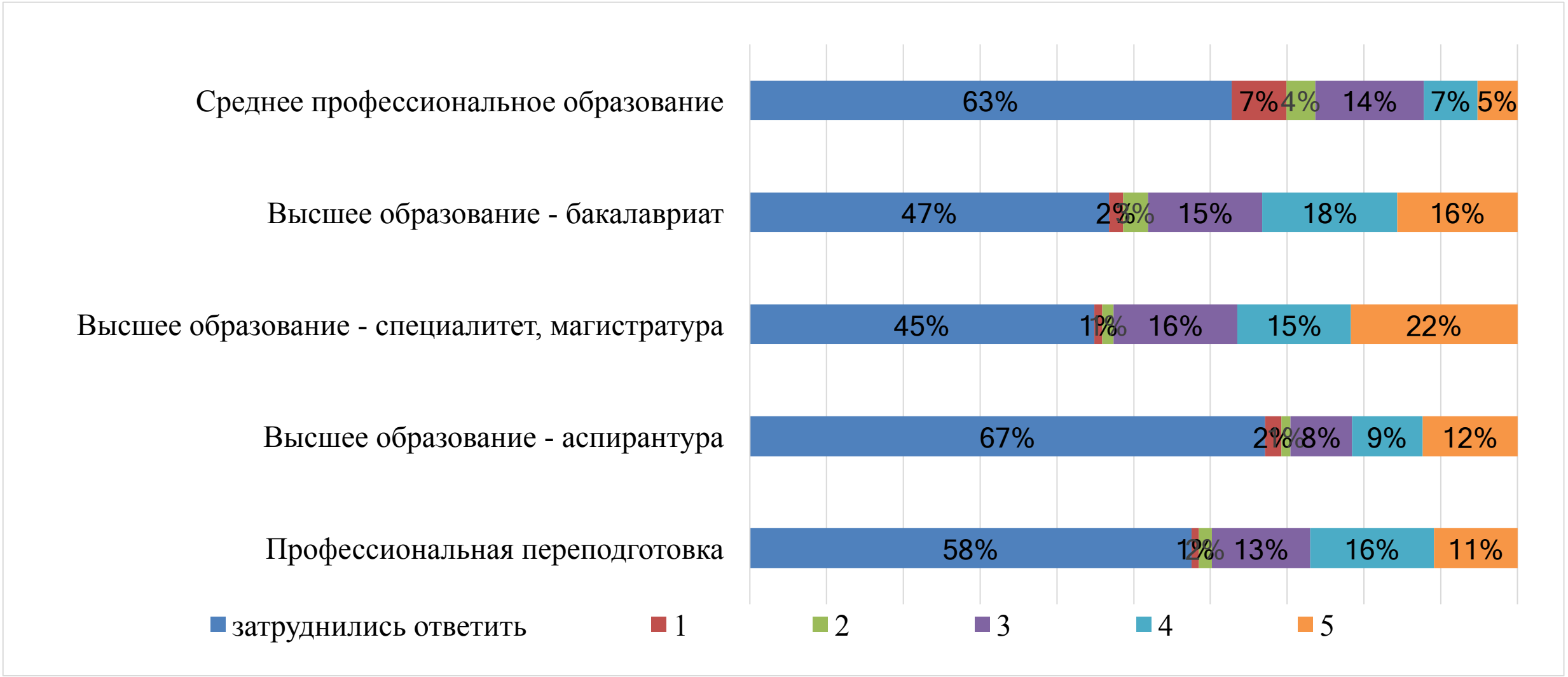


Подготовка по УГСНП 10.00.00 «Информационная безопасность»

Контрольные цифры приема граждан на 2017 - 2020 г.

Уровни образования	2017	2018	2019	2020
Бакалавриат	2287	2379	2673	2918
Магистратура	953	999	606	808
Специалитет	3158	3264	3812	3743
Итого	**6398**	**6642**	**7091**	**7469**

УДОВЛЕТВОРЕННОСТЬ ПОДГОТОВКОЙ ВЫПУСКНИКОВ В ОБЛАСТИ ИБ



МЕРОПРИЯТИЯ ПО РАЗВИТИЮ ПЕРСОНАЛА В ОБЛАСТИ ИБ

ОСНОВНЫЕ ВЫВОДЫ

1. Существует неразрывная связь между развитием профессиональной деятельности специалиста по информационной безопасности с разрабатываемыми информационными технологиями и перспективами развития ИКТ.
2. Сформулированы новые компетенции специалистов и ожидания от специалистов в цифровом мире.
3. Представители опрошенных организаций в целом не в полном объеме удовлетворены уровнем подготовки выпускников образовательных организаций. Наиболее высоко оценивается уровень подготовки выпускников с высшим образованием и прошедших профессиональную переподготовку, это более 60%. Удовлетворенность подготовкой выпускников СПО не многим превышает 40%.
4. Среди мероприятий по развитию персонала преобладают такие, как программы повышения квалификации, обмен опытом, краткосрочные тренинги и семинары. К сожалению, организация стажировок для студентов и работников, а также целевое обучение студентов распространены очень мало, что не дает возможности студентам во время обучения получать начальный практический опыт.

Академия
Информационных
Систем

СПАСИБО ЗА ВНИМАНИЕ

Хайров Игорь, АИС
8(495)120-04-02
security@infosystem.ru

www.infosystems.ru
www.vipforum.ru