



Московский институт электроники и
математики им. А.Н. Тихонова НИУ ВШЭ

Профессиональные кадры как основа киберустойчивости России: проблемы профессиональной подготовки в области информационной безопасности

Сергеев А.В.

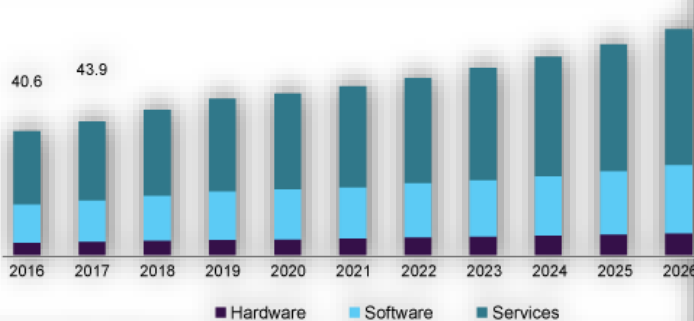
*Советник, директор Центра программных
разработок и цифровых сервисов*

2024, май

Проблема нехватки кадров ИБ

- **МинТруд РФ:** нехватка более **18 000 специалистов по ИБ**
 - **МитТруд США:** **500%** рост вакансий по кибербезопасности в США и в мире 2013 to 2023¹
 - **+3.5 миллионов нехватка специалистов** по кибербезопасности в мире ^{1,2, 4}
- **Недостаток квалификации специалистов:** 1 из 4-х человек имеет необходимые проф. навыки
 - Приток кадров из смежных отраслей: ИТ, МВД/МО/ФСТЭК, гос. органы и т.п.
 - Указ 250 и возрастающие требования к квалификации
- **Россия — проблема до СВО:** нет механизмов оценки уровня подготовки специалистов
 - Нет актуальных национальных стандартов оценки квалификации для негосударственного сектора ИБ
 - Ориентация на западные сертификационные центры
- **Россия — проблема с началом СВО:** ориентация на пассивную защиту
 - Система подготовки заточена на «защиту информации», а не «активное мультимодальное противостояние»

U.S. cyber security market size, by component, 2016 - 2027 (USD Billion)



The cybersecurity unemployment rate is at zero percent in 2019, where it's been for the past 8 years.



663,434

cybersecurity
job openings

1,129,659

employed in the
cybersecurity workforce

Source: CyberSeek June 2023

Системные барьеры подготовки кадров ИБ не преодолены

- **Нет общепринятых национальных стандартов оценки квалификации в области ИБ**
 - Аналогичных CISA, OSCP, OSCP
 - Наличие корпоративных программ не решает проблемы
- **ФГОС определяет квалификацию выпускника только «на бумаге»**
 - Выпускники двух разных ВУЗов по одному ФГОС могут иметь абсолютно разный набор навыков и умений
- **Передачи образовательной экспертизы между ВУЗами почти не происходит**
 - Отдельные исключения («Академическое партнёрство» НИУ ВШЭ) не меняет системы
- **ФУМО занимает крайне пассивную позицию**
 - Актуализация ФГОС носит номинальный характер, не разрабатываются оценочные средства, объективный контроль качества образования не проводится
- **Принятие новых профессиональных стандартов: крайне медленная работа Совета по профессиональным квалификациям в области ИТ (СПК ИТ)**
 - 4 профстандарта за 10 лет, профстандарт «Специалист по ИБ в КФС» принимался 3 года
- **Нет ответственного.** В России нет государственной структуры, отвечающей за координацию кадровой политики в гражданском кибербезопасности, аналогичного CISA или NIST NICE (со статусом Федерального агентства).

2023 – Указ о кибербезопасности и защите сетей правительственных структур от хакерских атак (Дж. Байден)

2020 – Утверждены единые национальные требования к специалистам по информационной безопасности (NIST 800-181)

2018 – Создание Агентства по кибербезопасности и защите инфраструктуры США (CISA)

2014 - Закон о повышении кибербезопасности (Д. Трамп), новые соревнования по кибербезопасности международного уровня

2010 – Создание Киберкомандования США (DOD)

2008 -  создание [Комплексной национальной инициативы по кибербезопасности](#)

РАЗВИТИЕ ИБ В США ЗА 15 ЛЕТ

- **Единый стандарт требований к трудовым ролям в области информационной безопасности**
 - Постоянная актуализация общенациональной системы трудовых стандартов
 - Понятные карьерные треки с вариантами найма правительственными структурами, бизнесом, образовательными организациями штатов и т.п.
- **Новые и пересобранные старые профессиональные сообщества**
 - K12 — сообщество преподавателей в области кибербезопасности
 - Federal Information Security Educators (FISSEA) community -- сообщество внештатных специалистов, сотрудничающих с федеральными агентствами
 - WorldSkills Cybersecurity Skill Area
- **Десятки международных сертификационных программ:** CISA, CISSP, OSCP, OSWE, OSEP, OSED, OSDA, OSWA, OSWE, OSWP, EXP301, EXP312, WEB300, CEH, CKLP, CCNA
 - Повышение квалификации
 - Воронка вовлечения лучших специалистов орбиту влияния
- **Новые федеральные и ведомственные структуры, направленные на управление кадрами и координацию**
 - Киберкомандование, CISA, NIST NICE и т.п.
- **Кибер-ЧВК на основе профессиональных сообществ**
 - Разведка, вербовка, нападение
- **Производство средств кибернападения**
 - OffSec (Kali, ExploitDB и т.п.), KeySight/IXIA (BreakingPoint) и т.п
 - Программы спецслужб типа Weeping Angel и т.п..
- **Инициативы по развитию кадрового потенциала и развитию талантов**
 - Десятки соревнований для молодых специалистов (BH, Social Engineering Competitions, National Cyber League, US Cyber Games, Cyber Skills Curricula, Q-Mission), конференций, выставок



Устаревшие квалификационные справочники

- Квалификационные требования к специалистам ИБ, представленные в «Единых квалификационных справочниках» устарели
- Справочниками вынуждены пользоваться все органы гос. власти, госкорпорации, субъекты КИИ и т.п

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ И СОЦИАЛЬНОГО РАЗВИТИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Приказ

от 22 апреля 2009 года N 205

Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел "Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации"

В соответствии с пунктом 5.2.52 Положения о Министерстве здравоохранения и социального развития Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 30 июня 2004 года N 321¹ (Собрание законодательства Российской Федерации, 2004, N 28, ст.2898; 2005, N 2, ст.162; 2006, N 19, ст.2080; 2008, N 11 (ч.1, ст.1036; N 15, ст.1555; N 23, ст.2713; N 42, ст.4825; N 46, ст.5337; N 48, ст.5618; 2009, N 2, ст.244; N 3, ст.378; N 6, ст.738; N 12, ст.1427),

¹ Бюллетень трудового и социального законодательства РФ, 2004, N 7, с.66-75.

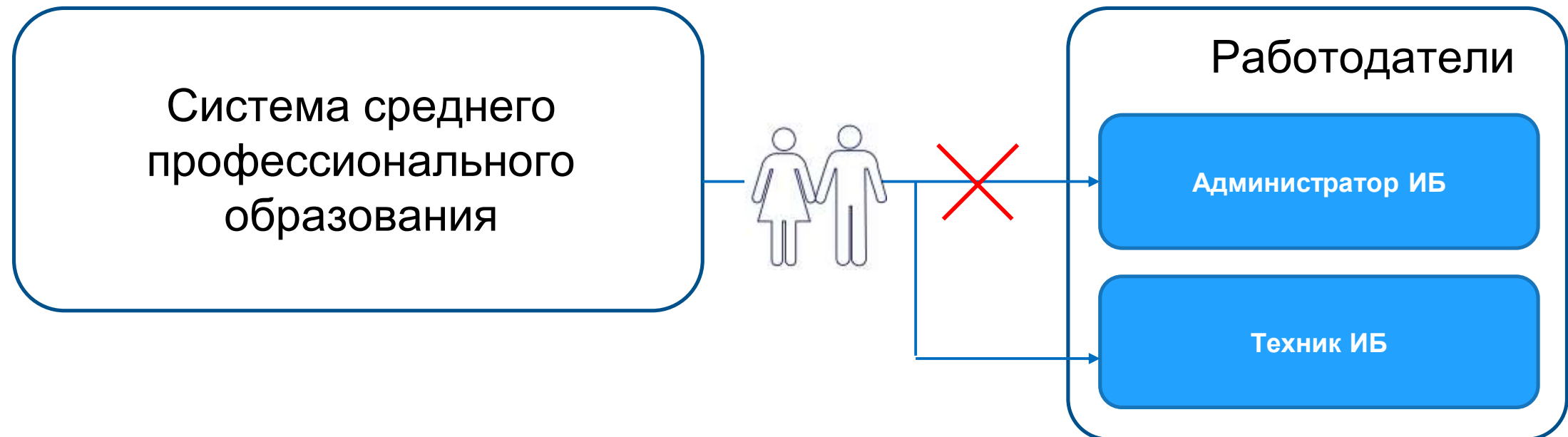
приказываю:

Утвердить Единый квалификационный справочник должностей руководителей, специалистов и служащих, раздел "Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации" согласно приложению.

Министр
здравоохранения и
социального развития
Т.Голикова

Устаревшие квалификационные справочники

1. Текущие квалификационные характеристики* (2009) в области ИБ катастрофически устарели
2. Обязательны к использованию в ФОИВ, РОИВ, компаниях с гос. участием и т.п.
3. Не отвечают современным требованиям компетенциям / профессиям ИБ
4. Выпускники организаций СПО могут претендовать только на позицию уровня «техник»
5. Ресурс системы СПО не используется для наполнения рынка труда квалифицированными специалистами



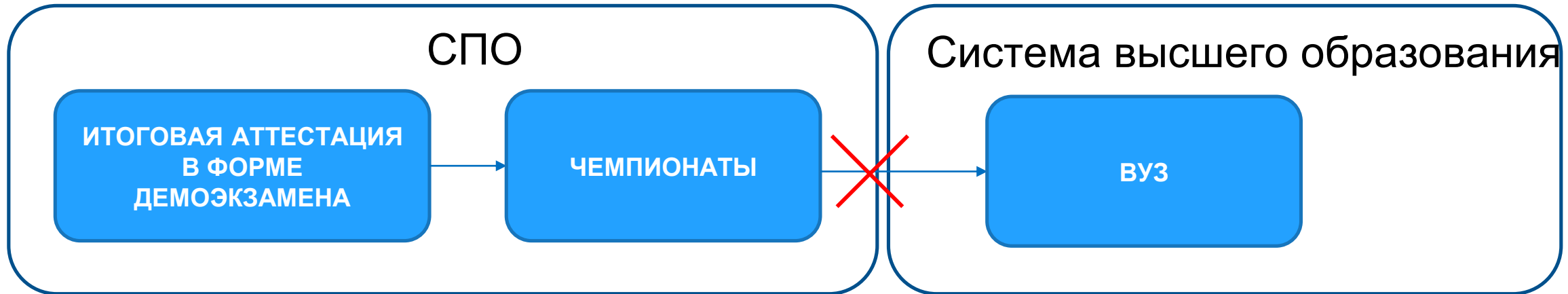
* Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры

Устаревшие квалификационные справочники

- **Минимальные требования к квалификации на позицию «Специалист по защите информации»:**
 - «Высшее профессиональное образование по специальности <...> без предъявления требования к стажу работы».
- **Рост числа компетенций и профессий в ИБ не отражен в квалификационных справочниках**
- **Выпускники системы СПО не могут заместить основные, самые востребованные позиции в ИБ**
 - Проблема ещё более усугубилась после принятия «Указа №250»
 - Искусственное завышение приёма в ВУЗы по направлению УГС 10.00.00 «Информационная безопасность»
- **Предложение:** Провести анализ и актуализировать «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации» с учетом современных трендов в области защиты информации и уровня подготовки кадров национальной системы образования.

Сегментированность системы образования

- Нет связки между СПО и ВУЗами
- Результаты чемпионатов и практических экзаменов студентов-выпускников колледжей, ориентированные на практический трек подготовки, никак не учитываются при поступлении в ВУЗы
- У студентов-практиков нет возможности параллельно вести интенсивную подготовку практического трека и подготовку к ЕГЭ



Чему учат? Оборонительная парадигма

- Ориентация на защиту, а не нападение
- Новые государственные инициативы, например «Национальный технологический центр цифровой криптографии» направлены на укоренное внедрение российских ИТ-технологий и интеграцию с криптографическими решениями – т.е. снова на защиту информации, а не активное противодействие враждебным странам и организациям.
- В национальном проекте «Экономика данных», анонсированном в 2022 году, блок безопасности посвящен, традиционно, технологиям защиты – квантовых коммуникаций и квантового шифрования.
- Отдельной проблемой является прямой запрет в российском законодательстве (ст. 273-274 УК РФ) на изготовление и применение даже в исследовательских целях программного обеспечения, направленного на моделирование угроз информационной безопасности, проверку киберустойчивости систем и организаций

— Безопасность данных. Необходимо продолжить работу над технологиями квантовых коммуникаций и квантового шифрования. Они помогают отражать любые кибератаки, как классические, так и с применением квантовых компьютеров. Благодаря таким технологиям системы безопасности страны будут неуязвимы для взлома.

— Стандарты и протоколы работы с данными. Они нужны для обеспечения безопасности, для надёжной обработки и хранения данных. Особенно в части хранения персональных данных граждан. В том числе — с применением технологий квантовой криптографии.

”

15,8. млрд. рублей – потери россиян от хищения денежных средств в 2023 году*

50 раз – рост количества киберпреступлений за 2014-2022 гг.

*Данные Банка России

Есть ли положительные примеры?

- **Совместные образовательные программы:**
 - НИУ ВШЭ и Банк России, ТУСУР и ИнфоТеКС и т.п.
- **Профильные компетенции МинПросвещения (созданные на базе инициатив WorldSkills Russia)**
 - Компетенция «Корпоративная защита от внутренних угроз ИБ», «Информационная безопасность»
 - Единые оценочные средства для системы среднего профессионального образования
 - Система чемпионатов профессионального мастерства
- **Интеграция СТФ-движения в систему образования**
 - Новая Всероссийская олимпиада школьников «Технологии» профиль «Информационная безопасность»
- **Корпоративные университеты**
 - Новые форматы: Передовые инженерно-математические школы



ПИМШ НИУ ВШЭ



ВСОШ по ИБ



Канал компетенции «Корпоративная защита»



Компетенция «Корпоративная защита от внутренних угроз информационной безопасности»

500+ экспертов из 47 регионов РФ,
9000+ участников мероприятий за 3 года



Ориентация на технологический суверенитет: 100% национальные СЗИ

Корпоративный и вузовский треки: ГК Росатом, ГК Роскосмос, ГпН, ГК Ростех, Сибур

Профильные программы СПО / ВПО / ДПО





НЕИМЕ
НННЕ
AND BIG DATA
F5

КОРПОРАТИВНА ЗАЩИТА ОТ
ВНУТРЕННИ УГРОЗИ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ENTERPRISE INFORMATION SYSTEMS SECURITY
F7

R22

13:17:10

КОРПОРАТИВНА ЗАЩИТА ОТ
ВНУТРЕННИ УГРОЗИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ENTERPRISE INFORMATION
SYSTEMS SECURITY
F

infotecs

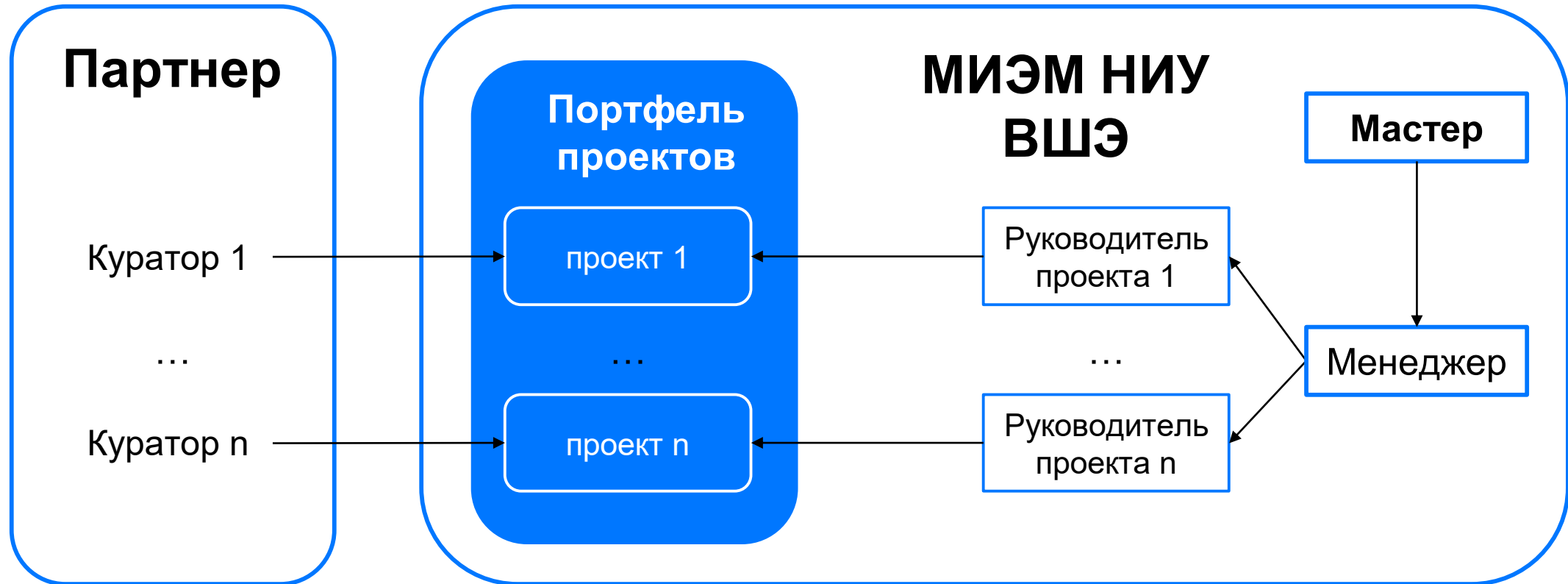
future skills
F

КОРПОРАТИВНА ЗАЩИТА ОТ
ВНУТРЕННИ УГРОЗИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ENTERPRISE INFORMATION
SYSTEMS SECURITY
F

F

«Корпоративная защита от внутренних угроз информационной безопасности»,
финал в Казани

Новый формат взаимодействия ВУЗа и Партнёров: Мастерские в Передовых инженерных школах



Что делать? Решения для бизнеса

- **Корпоративные университеты**
 - По примеру Сбера ,Тинкофф, Банка России
- **Собственные или партнёрские программы с лидерами Системы образования**
 - По примеру VK, Инфовотч, ИнфоТеКС
- **Национальные компетенции и система чемпионатов профессионального мастерства**
 - Вход в систему СПО и корпоративных чемпионатов
 - Корпоративные чемпионаты для сотрудников, перенос экспертизы от других организаций
- **Ранний отбор талантов**
 - Участие в СТФ, интеграция в образовательные программы, ВСОШ, другие олимпиады
- **Собственные стандарты**
 - «Безопасность начинается с тебя»



HIGHER SCHOOL OF ECONOMICS
NATIONAL RESEARCH UNIVERSITY

**Московский институт электроники и
математики им. А.Н. Тихонова НИУ ВШЭ**

Антон Сергеев

avsergeev@hse.ru

Варианты сотрудничества

Форма сотрудничества	Приоритетное направление сотрудничества	Формирование штата	Участие специалистов партнёра в образовательном процессе	Реализация проектов по заказу партнёра	Участие студентов в работе структуры	Схема Финансирования
Мастерская	Образовательное + R&D	Сотрудники МИЭМ (совмещение) + сотрудники партнёра (ГПХ)	Да, средний объём нагрузки Привлечение для преподавания в т.ч. специалистов партнёра	Обязательна В зависимости от типа проектов	Конкурсный отбор со всех образовательных программ Стипендиальная поддержка со стороны партнера	Договор пожертвования
Партнёр образовательной программы	Образовательное	Только сотрудники МИЭМ	Возможна	Возможна. Только студенческие	Студенты на практике, проектах, стажировках в организации-партнёре	Договор пожертвования

Совместная магистратура Банка России и НИУ ВШЭ «Информационная безопасность в кредитно-финансовой сфере»



Банк России



МИЭМ

Московский институт электроники
и математики НИУ ВШЭ

Московский институт электроники и математики им. А.Н. Тихонова НИУ ВШЭ и Банк России открывают новую магистерскую программу

«Информационная безопасность в кредитно-финансовой сфере».

Набор на Программу уже стартовал – с 1 сентября 2024 года начнется обучение специалистов по информационной безопасности для банков и других организаций финансового сектора.



Совместная магистратура Банка России и НИУ ВШЭ

«Информационная безопасность в кредитно-финансовой сфере»

- **Объединение экспертизы лидеров.** Программа разработана и реализуется совместно Департаментом информационной безопасности Банка России и Московским институтом электроники и математики им. А.Н. Тихонова НИУ ВШЭ, при организационном участии Университета Банка России.
- **Прямой доступ к топ-экспертам** по информационной безопасности Банка России и всей отрасли
- **Подготовка управленческих кадров** для блока ИБ организаций кредитно-финансовой сферы
- **Эталонная магистерская программа** на базе нового профессионального стандарта 06.053 «Специалист по информационной безопасности в кредитно-финансовой сфере»
- **Привлечение практиков из отрасли.** Актуальная информация об особенностях регулирования ИБ, последних нормативных трендах, лучших практиках защиты информации.
- **Российский и международный комплаенс**

МИЭМ НИУ ВШЭ

**Московский институт электроники и математики им. А.Н. Тихонова
Национального исследовательского университета «Высшая школа экономики»**



Москва, ул. Таллинская 34, Кампус «Строгино»

МИЭМ НИУ ВШЭ: ПОДРАЗДЕЛЕНИЯ ИНФОБЕЗОПАСНОСТИ

Образование и исследования

Кафедра Компьютерной безопасности

Специалитет

С 1997 года

Работает в тесном контакте с регулятором

Криптография, нормативная база, КИИ, обнаружение компьютерных атак

Кафедра Информационной безопасности киберфизических систем

Бакалавриат и 3 магистерских программы

С 2018 года

Ориентация на современные тренды в области кибербезопасности

Защищенная разработка, оценка защищенности, построение безопасной инфраструктуры, защищенные системы связи

Базовая Кафедра ГК Инфовотч

Поддержка обучения по DLP-технологиям

С 2018 года

Современные технологии противодействия внутренним угрозам и защиты АСУ-ТП

Исследования и разработка

Центр программных разработок и цифровых сервисов

Проведение исследований и разработка систем: C/C++, Python (Flask/Jango), PHP, BI, инфраструктурные сервисы, работа с СЗИ



Банк России



СИСТЕМА
АКЦИОНЕРНАЯ ФИНАНСОВАЯ КОРПОРАЦИЯ

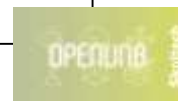


INFOWATCH®



ТК
194

Кибер-физические
системы



HUAWEI

WEBINAR.RU

ZECURION



Тинькофф Банк

kaspersky



Ростех

Совместная магистратура Банка России и НИУ ВШЭ

«Информационная безопасность в кредитно-финансовой сфере»

- Бюджетные (15 в 2024 году) и коммерческие места для обучения.
- Программа рассчитана на тех, кто планирует связать свою карьеру с защитой кредитно-финансовых организаций от внутренних и внешних угроз информационной безопасности:
 - сотрудников и руководителей служб ИТ и ИБ банков (имеющих профильный опыт работы)
 - выпускников бакалавриата и специалитета НИУ ВШЭ и других вузов, окончивших обучение по профильным направлениям, таким как информационная безопасность, финансы и кредит, информационные технологии и др.
- Прием на программу - по результатам конкурса портфолио и собеседований, в оценке которых примут участие преподаватели МИЭМ НИУ ВШЭ и эксперты Банка России и КФС.
- Выпускники магистерской программы будут востребованы в Банке России и организациях финансового сектора – банках, страховых компаниях, биржах, а также в других компаниях, предоставляющих финансовые и инвестиционные услуги, и т.д.

БАРЬЕРЫ В РАЗВИТИИ ОТРАСЛИ

ЗАДАЧИ подготовки кадров, оценки квалификации,
разработки стандартов «размыты»:
ФСТЭК ФСБ, МинОбр, МинПрос, МинТрудом, ФУМО, БР



ЦРУ и другие разведывательные структуры активно специалистов в свои ряды

Browse CIA Jobs —

Cyber Security Researcher

Cyber Security Researchers focus in the cyber arena and specialist in the design, development, integration, and deployment of cutting-edge tools, techniques, and systems to support cyber operations.

Full time

Starting salary: \$69,287 - \$122,459

Bachelor's degree

Opportunities for domestic travel are poss

EXPRESS INTEREST

<https://www.cia.gov/careers/jobs/cyber-security-researcher/>

БАРЬЕРЫ В РАЗВИТИИ ОТРАСЛИ

ЗАДАЧИ подготовки кадров, оценки квалификации,
разработки стандартов «размыты» между
ФСТЭК ФСБ, Минобр, МинПрос, МинТрудом, ФУМО, БР

В России нет государственной структуры, отвечающей за координацию гражданского кибербеза, аналогичного CISA или NIST NICE (со статусом Федерального агентства)

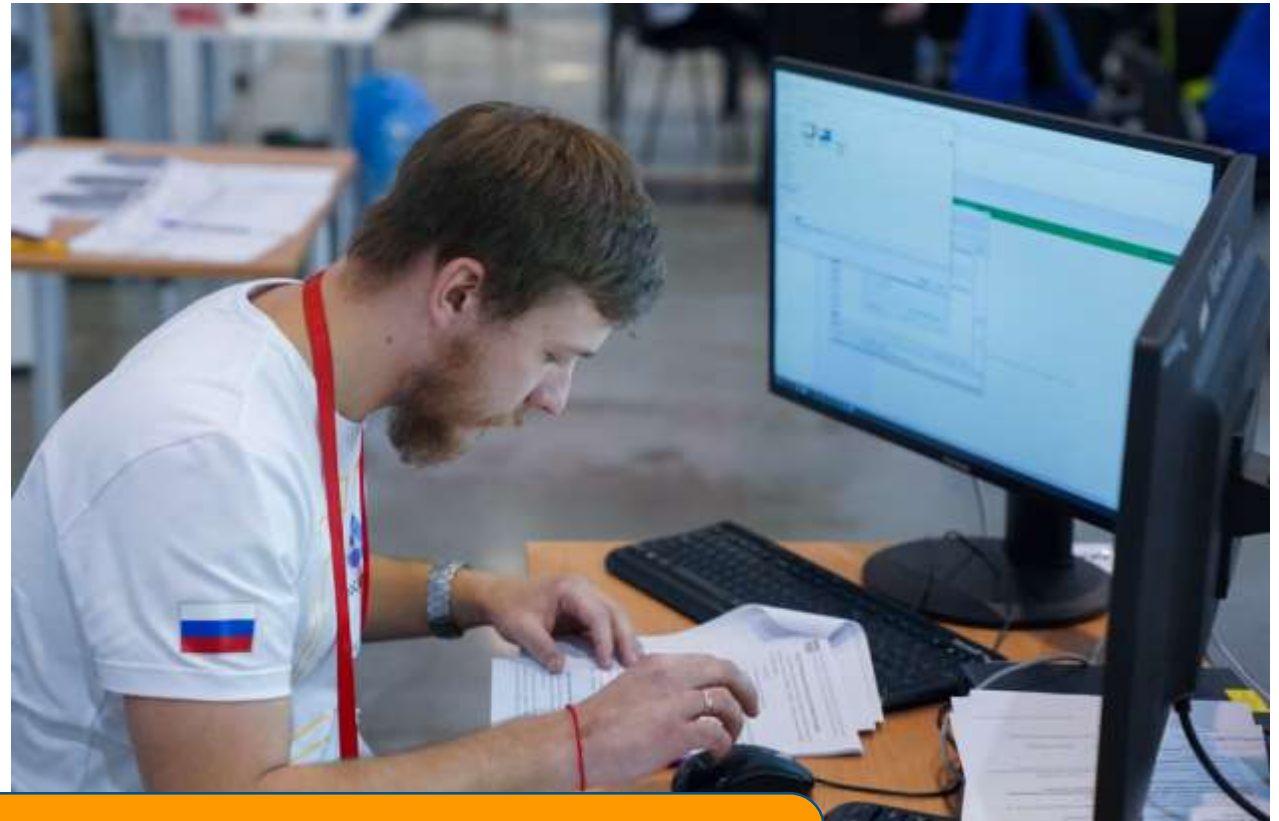
КТО ОТВЕЧАЕТ ЗА ГОТОВНОСТЬ СТРАНЫ ПРОТИВОСТОЯТЬ КИБЕРУГРОЗАМ?

Отдельные независимые инициативы в области ИБ в России не решают проблемы.

- **СТФ-движение (соревнования по практической безопасности)** ориентированы на учебные крайне упрощенные примеры. Они отличаются высоким уровнем либерализма и открытости, что не позволяет на его базе проводить серьезные задачи.
- **Федеральное учебно-методическое объединение занимает крайне пассивную позицию:** за 10 лет создано только 3 профстандарта, нет современной базы оценочных средств, реальное развитие заменяется подготовкой отчетности
- **Профильные компетенции МинПросвещения (созданные на базе инициатив WorldSkills Russia),** такие как «Корпоративная защита», ориентированы на реальные корпоративные сценарии, однако, оставаясь в российском правовом поле, вынуждены смещать фокус на защиту информации, практику применения СЗИ, а не активные атакующие действия.
- Новые государственные инициативы, например **«Национальный технологический центр цифровой криптографии»** направлены на укоренное внедрение российских ИТ-технологий и интеграцию с криптографическими решениями – т.е. снова на защиту информации, а не активное противодействие враждебным странам и организациям.
- В национальном проекте «Экономика данных», анонсированном в 2022 году, блок безопасности посвящен, традиционно, технологиям защиты — квантовых коммуникаций и квантового шифрования.
- Отдельной проблемой является прямой запрет в российском законодательстве (ст. 273-274 УК РФ) на изготовление и применение даже в исследовательских целях программного обеспечения, направленного на моделирование угроз информационной безопасности, проверку киберустойчивости систем и организаций

Положительный опыт. Демонстрационные экзамены по «Корпоративной защите» — один из немногих положительных примеров

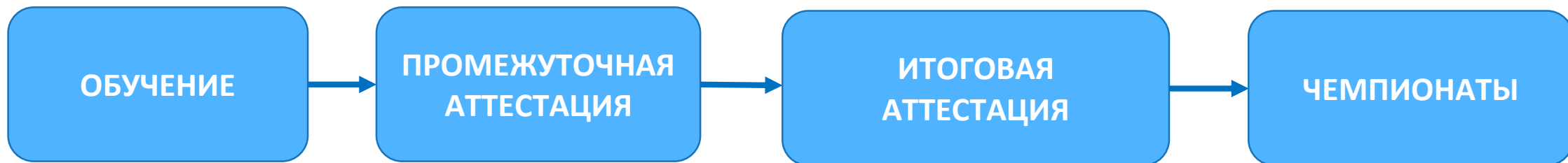
Реальное влияние на уровень подготовки специалистов ИБ в стране



**Компетенция №1 в стране в области
информационной безопасности**

РОССИЯ: ЕДИНЫЙ ТРЕК ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИБ: ДЕМОЭКЗАМЕНЫ → ЧЕМПИОНАТЫ

ЕДИНЫЙ СТАНДАРТ СПЕЦИФИКАЦИИ КОМПЕТЕНЦИИ



В ФОРМЕ ДЕМОЭКЗАМЕНА

В ФОРМЕ ДЕМОЭКЗАМЕНА

AtomSkills, Роскосмос
ОС, ФНЧ, HiTech, DS

На УМК и лабораторных комплексах, гармонизированных с Техническим описанием Компетенции

Упрощенные комплекты оценочной документации (КОДы)

Комплекты оценочной документации (КОДы / ОМ)

Комплексное чемпионатное задание, отбор лучших

Обучение по отдельным группам навыков

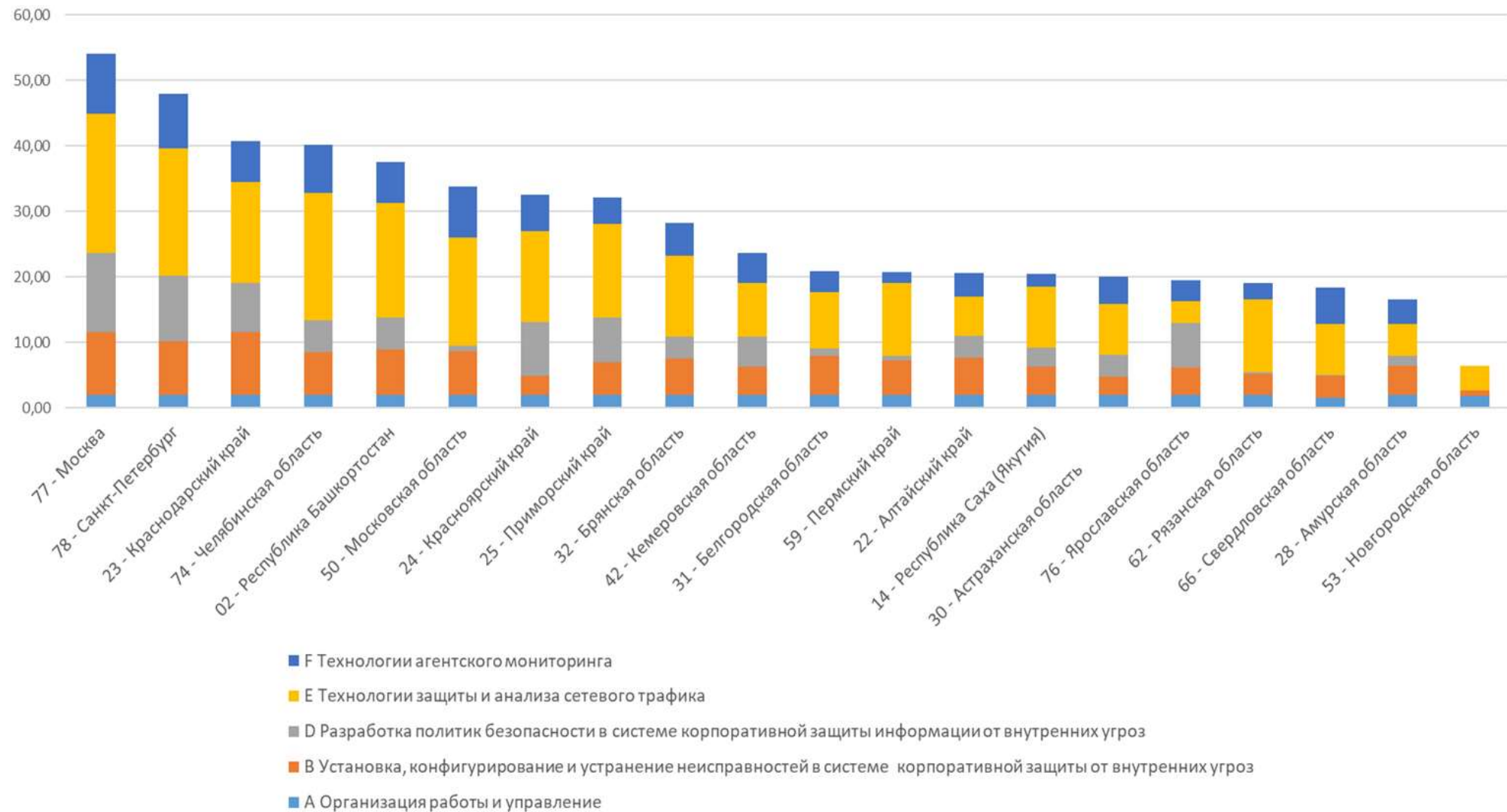
6000
человек в год

4000
человек в год

400
человек в год

СУЩЕСТВЕННЫЙ РОСТ УРОВНЯ ПОДГОТОВКИ

Объективные показатели контроля + вовлеченность сообщества в оценивание + актуальное задание



БАРЬЕРЫ В РАЗВИТИИ ОБЛАСТИ

ЗАДАЧИ подготовки кадров, оценки квалификации,
разработки стандартов «размыты» между
ФСТЭК ФСБ, Минобр, МинПрос, МинТрудом, ФУМО, БР

В России нет государственной структуры, отвечающей за координацию гражданского кибербеза, аналогичного CISA или NIST NICE (со статусом Федерального агентства)

Квалификационные требования к специалистам ИБ
значительно устарели