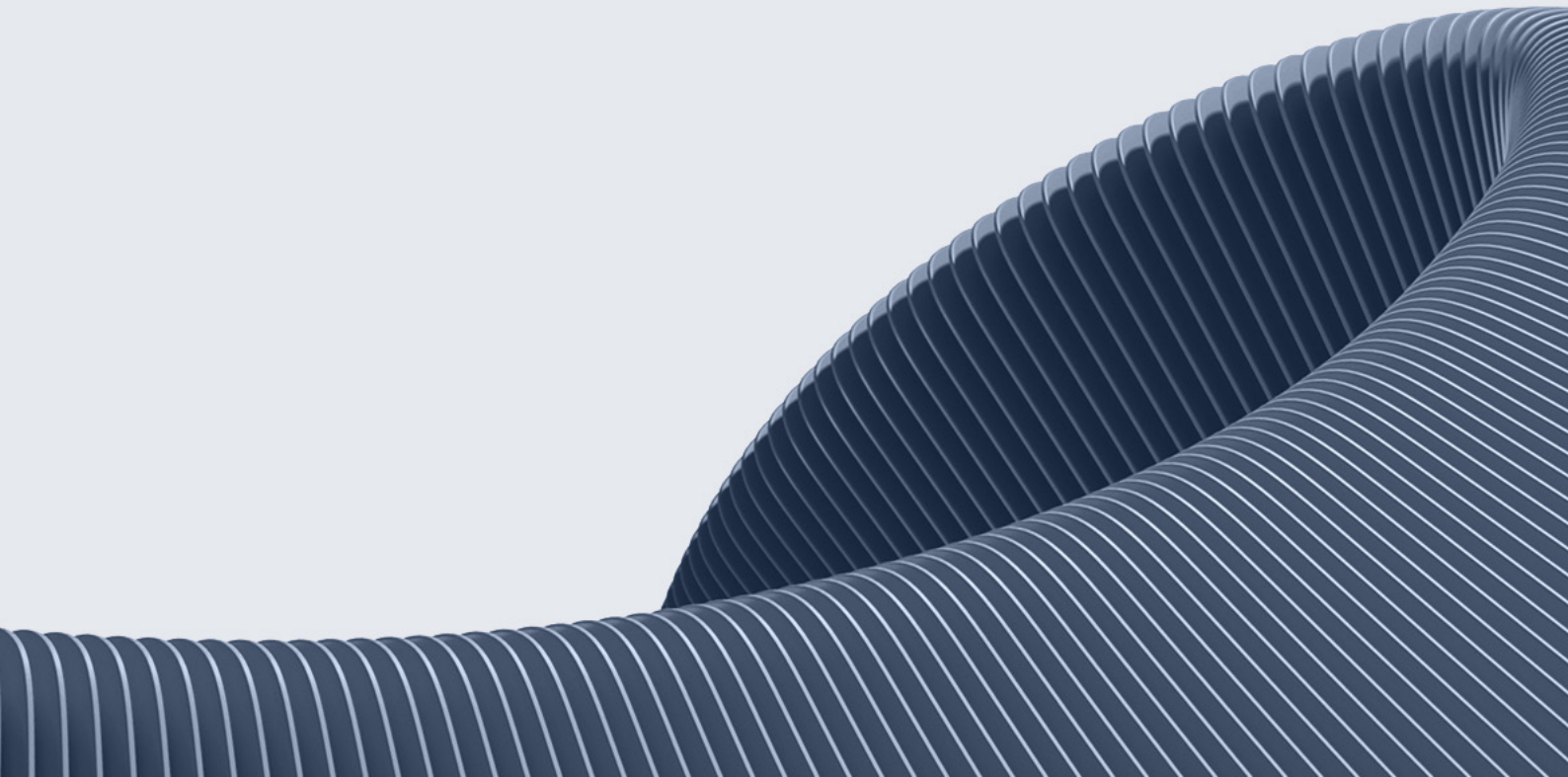
РЫНОК ТРУДА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ В 2024–2027 ГГ.:

прогнозы, проблемы и перспективы

Экспертно-аналитический доклад
Май 2024 г.

ВВЕДЕНИЕ

На российском рынке труда в информационной безопасности в 2022–2024 гг. сформировался острый дефицит специалистов, в том числе под давлением вопросов технологического суверенитета и национальной безопасности. Растет уровень внедрения технологий, меняющих архитектуру и принципы, на которых строится информационная безопасность (ИБ), а вместе с ними и правила организации рынка труда. В этих условиях отраслевой рынок труда ИБ ожидает ряд кардинальных изменений.



Масштабный рост занятости

С текущих 110 тысяч к 2027 году число занятых в ИБ может вырасти до 181–196 тыс. человек, число вакансий вырастет в 1,5–1,6 раза. Тем не менее ожидается, что дефицит в кадрах сократится до 29–33% от количества занятых с текущих 45%, но вырастет в абсолютном значении — с текущих 50 тыс. до 52–65 тыс. человек в 2027 году. Таким образом, ситуация «рынка предложения» сохранится в горизонте до 2027 года.

В период же до 2030 года рынок труда в сфере ИБ может выйти на плато, что может быть связано как с исчерпанием трудовых ресурсов, так и с достижением потолка расходов на безопасность потребителей ИБ-продуктов и услуг. В связи с этим возникают потенциальные угрозы, выраженные неконтролируемым ростом заработной платы ИБ-специалистов и неспособностью отрасли решать возникающие технологические вызовы.

Основная причина роста — углубление разделения труда в секторе

Усилится разделение труда и произойдет переход к четкой ролевой структуре, где большинство специалистов будет обладать достаточно узкими функциональными ролями, подразумевающими четкий набор выполняемых задач и требований к знаниям и навыкам. Ожидается переход от рынка труда многофункциональных специалистов в сфере ИБ к структуре, которая потребует большей численности узких ИБ-специалистов — архитекторов и инженеров, аналитиков, ИБ-консультантов и аудиторов, чем сегодня.

Рост количества и сложности киберугроз, переход на отечественное ПО, построение цифрового суверенитета, а также появление новых цифровых технологий, требующих защиты, будут способствовать росту востребованности ИБ-специалистов.

Перелом на рынке труда в горизонте 3–5 лет маловероятен, но возможен

при условии больших инвестиций в ИИ и автоматизацию (до 27 тыс. рабочих мест, то есть около 10% от общей потребности в ИБ-специалистах к 2027 году, может быть оптимизировано за 2024–2027 гг.). При этом в таком случае изменится и структура занятости — автоматизация станет причиной роста востребованности высококвалифицированных кадров, способных осуществлять сложные типы работ.

Снижению дефицита будет способствовать и вовлечение новых когорт потенциальных сотрудников (ожидается увеличение доли женщин и сотрудников старше 50 лет в сфере ИБ, что станет основой для привлечения порядка 33 тыс. дополнительного персонала за 2024–2027 гг.).

В условиях ограниченности традиционных образовательных программ импульс к развитию получат новые форматы

Система профессиональной подготовки кадров, включающая среднее профессиональное и высшее образование, даст дополнительно до 54 тыс. выпускников за 2024–2027 гг. Однако данного количества недостаточно для покрытия дефицита кадров в условиях растущего спроса на ИБ-специалистов. Более того, не все из них пойдут работать в сектор ИБ. Увеличение же объемов выпуска в рамках системы профподготовки, обычно подразумевающей длительный срок обучения, ограничено.

В связи с этим развитие получат программы дополнительного образования, позволяющие более оперативно и гибко реагировать на вызовы рынка. Ожидается увеличение числа таких программ, а также рост уровня взаимодействия между участниками рынка при реализации программ ДПО. Кроме того, развитие могут получить и иные форматы обучения — геймифицированные системы, стажировки и другие.

Новые профессии

Благодаря развитию ИИ уже в ближайшие 3–4 года оформится устойчивый спрос на специалистов MLSecOps, а также на ряд других профессий. При этом, несмотря на перспективность данного направления и его потенциальную востребованность, система профессионального образования может отреагировать на изменение с лагом, что может спровоцировать дефицит высококвалифицированных специалистов с требуемыми компетенциями в сфере ИИ.

Важно и то, что помимо появления новых профессий внутри ИБ изменения будут происходить и в смежных отраслях, и прежде всего в других сегментах сектора безопасности в стране. Переквалификация сотрудников сектора безопасности и в целом его еще больший разворот в сторону цифровых технологий, возможно, станет триггером для существенного роста рынка труда ИБ.

Доклад ЦСР «Северо-Запад» и Positive Technologies — это попытка определить возможный ландшафт рынка труда в информационной безопасности в 2027 году, а также предложить некоторую систему рекомендаций для участников рынка ИБ.

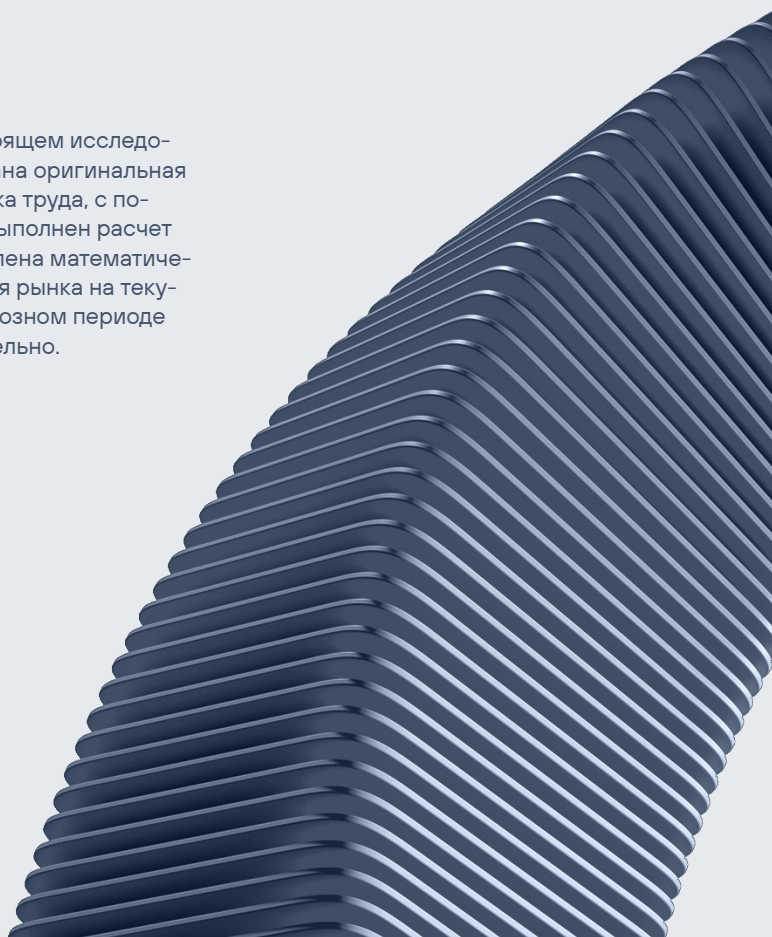
Целевой аудиторией данного доклада является широкое экспертное сообщество рынка труда, в том числе руководители ИБ-компаний, включая руководителей их HR-подразделений; руководители ИБ-подразделений компаний — заказчиков ИБ-услуг; представители организаций, осуществляющих образовательную деятельность по подготовке потенциальных ИБ-специалистов, а также представители органов государственной власти, определяющих и реализующих политику в сфере образования и науки, в том числе на региональном уровне.

ОСОБЕННОСТИ МЕТОДОЛОГИИ ИССЛЕДОВАНИЯ

Особенностью рынка труда в сфере информационной безопасности является сервисный характер ИБ по отношению к отраслям экономики. Это означает, что специалисты ИБ трудоустроены в основном не в специализированных организациях, а в компаниях-клиентах, действующих в различных отраслях экономики, а также в ИТ-компаниях, часто совмещающих разработку продуктов и оказание услуг в ИБ с другими направлениями в сфере ИТ*.

Для рынка труда ИБ характерно отсутствие качественной статистики. В частности, в отрасли отсутствует систематический мониторинг даже общей численности занятых. Имеются проблемы отслеживания и других показателей развития этого рынка труда.

В связи с этим в настоящем исследовании была разработана оригинальная методика оценки рынка труда, с помощью которой был выполнен расчет показателей и составлена математическая модель состояния рынка на текущий момент и в прогнозном периоде до 2027 года включительно.



* Анализ топ-200 нанимателей в ИБ в России демонстрирует, что на специализированные ИБ-компании приходится лишь 21% от общего числа вакансий. При этом доля вакансий банков составляет 26%, промышленных и энергетических компаний — 17%, ИТ-компаний — 12%. Доля госсектора составляет 6%. В топ-100 компаний по числу размещенных за последний год вакансий более 50% организаций являются именно клиентами — на них проходится 53% вакансий. Более подробно распределение отражено в Приложении В.

Количество занятых в ИБ в России

Показатель «количество занятых в ИБ в России» представляет собой совокупность лиц, занятых в задачах по обеспечению информационной безопасности организаций. В соответствии с методологией ОЭСР, к занятым в ИБ относится широкий спектр различных ролей и должностей, отвечающих за защиту данных, систем, инфраструктуры и других киберресурсов от сбоев, опасностей и киберугроз. При этом к специалистам в сфере ИБ не относятся разработчики ПО, программисты, сетевые инженеры и роли, которые могут быть прямо или косвенно быть связаны с информационной безопасностью. Более подробно список ролей, включенных в понятие «ИБ-специалист», описан в приложении Б, а также в отчете Building a Skilled Cyber Security Workforce in Five Countries[1].

Объективные первичные статистические данные о фактической величине этого показателя в России отсутствуют. Показатель рассчитан на основе бенчмарка, по аналогии с методом, применяемым в расчетах числа занятых в ИБ, проводимых международной организацией ISC2 для тех стран, где отсутствует объективная статистика занятости в ИБ. За основу взяты оценки рынков и объемов занятости на 2023 год в США, Великобритании, Франции, Германии, Японии и Южной Корее как стран, близких к России в рейтинге ВВП по ППС, по которым доступны соответствующие данные. Путем сопоставления объемов рынков стран и количества занятых сначала вычислено удельное число занятых на условный 1 млрд долл. выручки рынка. Далее перевод полученного значения через пропорцию на размеры российского рынка ИБ позволил установить, что количество занятых в ИБ на российском рынке труда составляет 110 тыс. человек.

Представленный результат расчета показателя косвенно подтверждается сопоставлением с другим непрямым методом оценки — с помощью анализа предполагаемой динамики ретроспективных данных, составленной исходя из последней доступной официальной оценки занятости в ИБ, и динамикой развития рынка за прошедший период. Последняя опубликованная оценка занятых в ИБ в России была выполнена Минтруда России в 2016 году, когда показатель составил около 35 тыс. человек. Учитывая ограничения в расчетах Минтруда, не учитывающих менеджеров, аудиторов, консультантов, которые могли составлять еще до 20 тыс. человек в 2016 г., а также среднегодовой темп роста занятости в ИКТ в 2016–2023 гг. в 11%, пересчет данных на 2023 год составил бы 111 тыс. чел., что практически полностью соответствует первоначальной оценке в 110 тыс. чел., выполненной по методике ISC2, которую и принимаем в настоящем исследовании за исходную.

Дефицит рабочей силы и потребность рынка труда

Объективные статистические данные о потребности и дефиците рабочей силы в сфере ИБ в России также отсутствуют. В связи с этим для аналитики и расчетов используется консенсусный показатель, рассчитанный на основе 7 экспертных оценок (оценки экспертов Positive Technologies, Сбера, Минцифры, HeadHunter и SearchInform), которые получены из публикаций СМИ и экспертных интервью, проведенных в рамках подготовки доклада. Потребность рынка труда в специалистах ИБ была рассчитана как сумма числа занятых и дефицита кадров в ИБ.

Количество вакансий и структура рынка труда

Фактическое количество и параметры вакансий в данном экспертно-аналитическом докладе оцениваются по данным платформы «РосНавык», агрегирующей вакансии с ресурсов HeadHunter, Superjob, «Работа России», «Работа.ру». Платформа использует нейросетевой анализ для классификации навыков, указываемых в вакансиях, затем на основе этих навыков производится классификация по специальностям. Вакансии, проанализированные в данном исследовании, представлены специальностью «Специалист по информационной безопасности».

Распределение работников на рынке ИБ по функциональным группам осуществляется на основе данных вакансий, опубликованных с марта 2023-го по март 2024 года. Более подробно методология распределения по функциональным группам описана в Приложении Б.

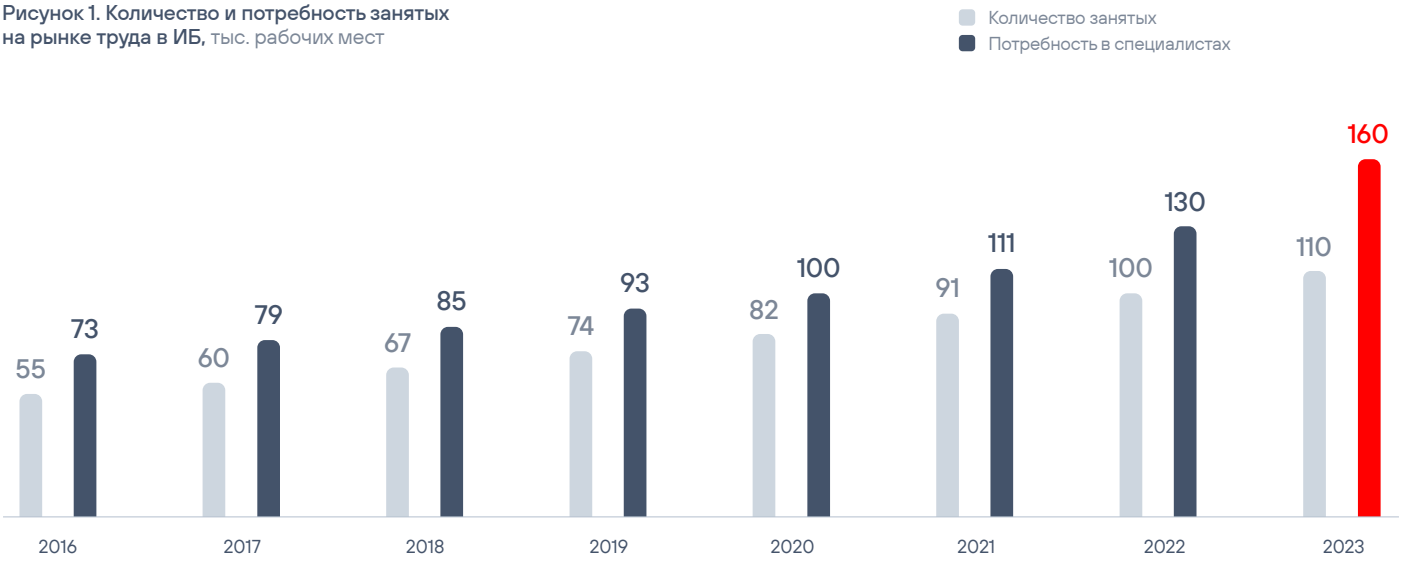
ОГЛАВЛЕНИЕ

01

ТЕКУЩЕЕ СОСТОЯНИЕ И ПРОБЛЕМЫ РЫНКА ТРУДА В ИБ

В текущий момент наблюдается активный рост рынка информационной безопасности. Число занятых за период с 2016 по 2023 годы удвоилось и достигло 110 тыс. человек. Существенно вырос и дефицит кадров: если в конце 2010-х годов дефицит составлял порядка 25–30%[2] от численности занятых в отрасли, то к 2023 году — уже 45%, или порядка 50 тыс. специалистов сферы ИБ.

Рисунок 1. Количество и потребность занятых на рынке труда в ИБ, тыс. рабочих мест

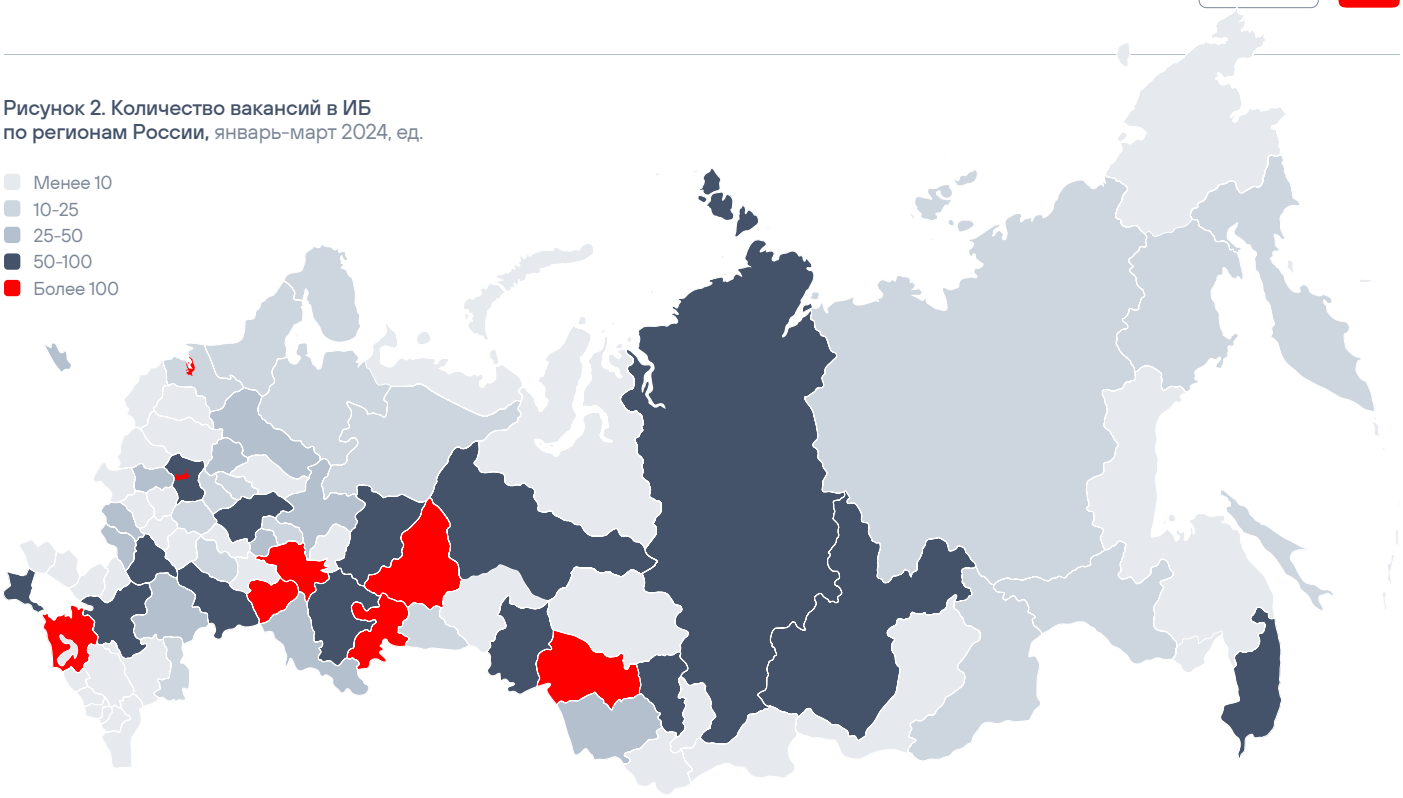


Источник: ЦСР «Северо-Запад»

Количество вакансий в ИБ за первые 3 месяца 2024 года составило 6109 шт. Этот спрос распределен по регионам России неравномерно. Очевидными лидерами по спросу являются Москва и Санкт-Петербург (50% от общего количества вакансий). Также можно выделить группу регионов с количеством вакансий 100–500. Эти регионы представляют собой крупные агломерации, где формируются новые центры занятости в ИБ, в том числе и благодаря удаленной занятости, за счет открытия новых площадок федеральных ИБ-компаний — например, компания Axenix (бывшая Accenture) открыла офис в Краснодаре, куда нанимает аналитиков SOC и инженеров по ИБ[3].

В большинстве российских регионов спрос за 3 месяца составил от 10 до 100 человек, при этом внутри этой группы можно выделить 14 промышленно развитых и сырьевых регионов, которые сформировали спрос в размере более 50 человек, — к таким относятся Красноярский край, Кемеровская область, Пермский край и Ханты-Мансийский автономный округ. Кроме того, выделяются регионы, в которых количество вакансий составило менее 10, что говорит о единичном спросе на специалистов в ИБ. К таким регионам можно отнести Северный Кавказ, Новороссию, некоторые регионы на северо-западе России, в Южной Сибири и на Дальнем Востоке (рисунок 2).

Рисунок 2. Количество вакансий в ИБ по регионам России, январь-март 2024, ед.



Источник: ЦСР «Северо-Запад» по данным Роснавык

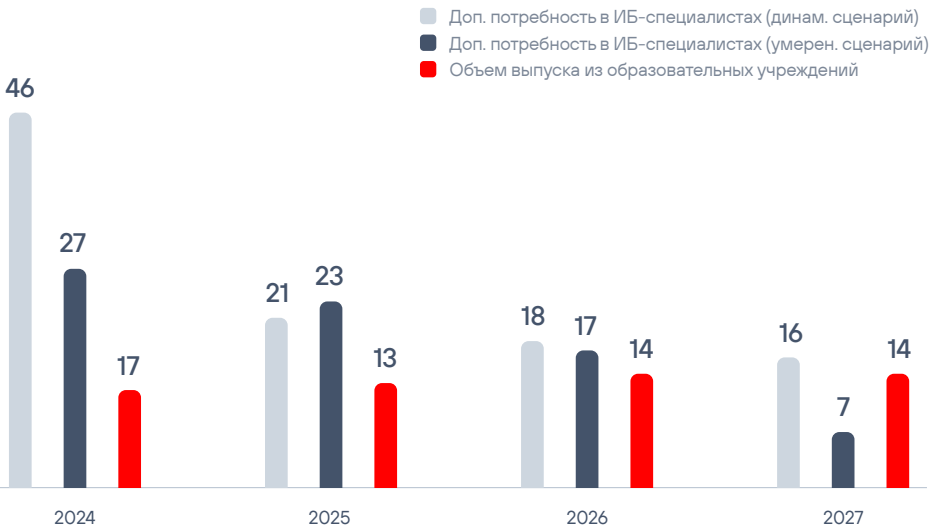
1.1

Демографические барьеры рынка труда

Рост спроса на квалифицированных ИБ-специалистов наблюдается в условиях общей нехватки рабочей силы, негативных демографических тенденций, выраженных в старении населения, а также ограниченных возможностей образовательной системы по наращиванию выпуска профильных специалистов.

Система высшего и среднего профессионального образования в текущий момент обеспечивает приток в ИБ порядка 8–10 тыс. кадров ежегодно, при этом потребность в кадрах превышает данные показатели в 2–3 раза. Но помимо недостаточного объема выпуска кадров проблемой также является длительный срок подготовки специалистов, который делает невозможным решение проблемы дефицита кадров в ИБ в рассматриваемый период (в ближайшие 3–4 года), даже если существенным образом будет увеличен набор на соответствующие образовательные программы (рисунок 3).

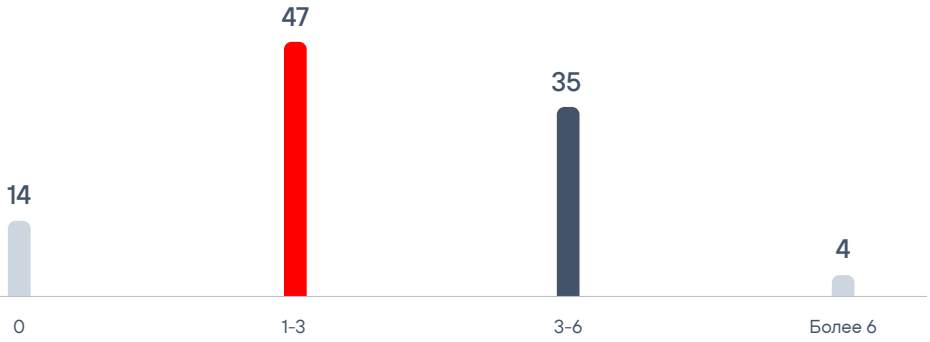
Рисунок 3. Разница между дополнительной потребностью в ИБ-специалистах и объемом подготовки образовательными учреждениями в рамках системы профессионального образования, тыс. чел., 2024—2027 гг.



Источник: ЦСР «Северо-Запад»

Кроме того, система образования выпускает на рынок труда специалистов без опыта или с минимальным опытом работы — так называемых junior-специалистов. Однако данные специалисты сталкиваются с умеренным спросом со стороны работодателей — на них приходится порядка 14% вакансий на рынке. Наибольшую востребованность же на рынке имеют middle-специалисты, имеющие опыт работы и портфолио проектов, не требующие существенного обучения. Так, на специалистов с опытом 1–3 года приходится 47% вакансий на рынке, с опытом от 3 до 6 лет — 35%* (рисунок 4).

Рисунок 4. Структура вакансий в области ИБ в России в зависимости от требуемого опыта работы (январь — апрель 2024 г.), %



Источник: ЦСР «Северо-Запад», по данным «РосНавыка»

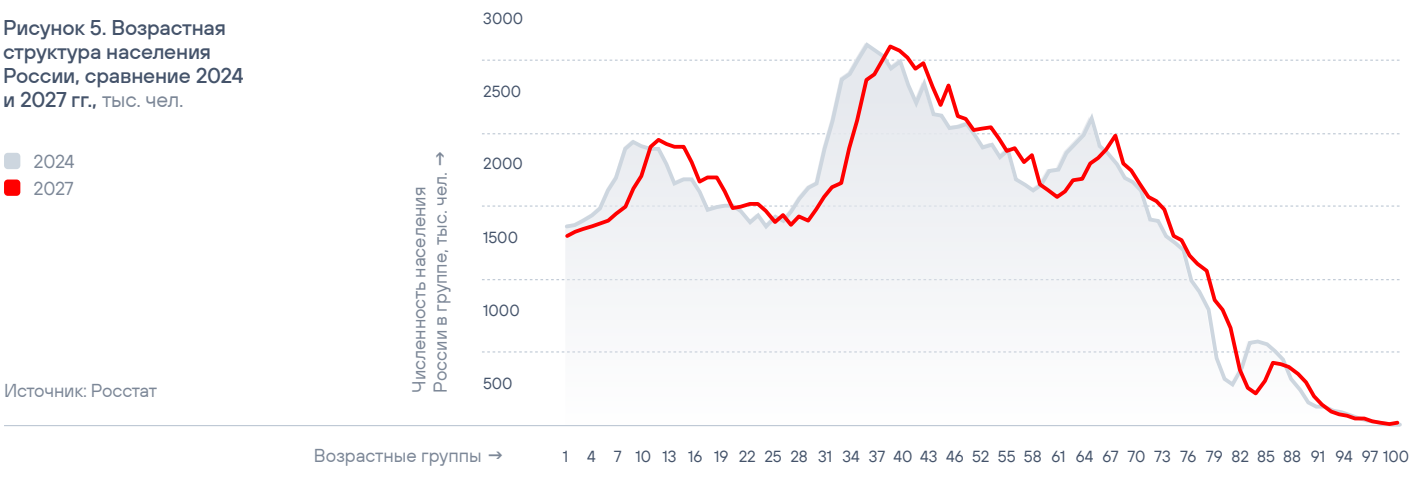
Другими словами, на рынке труда ИБ созрел запрос на новые формы и форматы подготовки, позволяющие ускоренно выпускать специалистов, максимально готовых к работе в отрасли.

Проводя аналогии с другими сегментами ИТ, можно увидеть, что постепенно такие форматы подготовки появляются (например, «Школа21» Сбера), и их аналоги могут быть реализованы и для рынка ИБ. Существует и потенциал развития программ дополнительного профессионального образования, позволяющего более гибко реагировать на вызовы, возникающие в отрасли. Активного развития потребует система стажировок, уже реализуемая такими компаниями, как Positive Technologies, «Солар», ИнфоТеКС и другими, и позволяющая осуществлять обучение молодых и заинтересованных специалистов на реальных задачах. Более подробно данная тема раскрыта в разделе 4.1 данного доклада.

Проблемой является и современная социально-демографическая ситуация. Наблюдается «демографическая яма» (рисунок 5). Каждый год на рынок труда выходит примерно на 100 тыс. молодых людей меньше, чем годом ранее[4]. Это будет негативно влиять и на источники кадров для рынка ИБ.

* Данные платформы «РосНавык» на начало апреля 2024 г. (выборка за период с 09.04.2023 г. по 09.04.2024 г., 24 171 вакансия)

Рисунок 5. Возрастная структура населения России, сравнение 2024 и 2027 гг., тыс. чел.



Источник: Росстат

Проблемой стал и отток ИБ-специалистов за рубеж в последние годы, а также сохранение риска оттока в обозримой перспективе. Хотя в начале 2024 г. массового оттока кадров не наблюдалось, а некоторыми экспертами даже отмечается обратный процесс — возврат в Россию некоторого числа квалифицированных специалистов, все же интерес российских специалистов к зарубежному рынку сохраняется на высоком уровне, а отдельные события и поводы могут влиять на возникновение новых волн оттока кадров в будущем[5].

В данных условиях ИБ-компании вынуждены более активно рассматривать нетрадиционные для сферы ИБ источники рабочей силы, включая представителей старшего поколения и женщин, доля которых в сфере ИБ пока мала. При этом данные категории, вероятно, потребуют обучения, что в условиях ускорения мобильности рынка труда и зарплатной гонки для многих работодателей может быть сочтено за высокорискованную инвестицию. Обучившись, работник может перейти в другую компанию на более высокую зарплату[6]. Тем не менее в условиях дефицита специалистов работодателям, скорее всего, придется идти на него — самостоятельно вовлекать и обучать данные когорты населения, о чем будет сказано далее.

В условиях дефицита кадров потребуется и привлечение иностранных специалистов. В текущий момент запускается проект по развитию экспорта российского ИТ-образования. Для его реализации Минцифры создало единого оператора российского ИТ-образования. Увеличивается и квота для иностранных граждан — за три года она выросла вдвое. В соответствии с данной квотой иностранные абитуриенты могут поступить в 39 университетов по программам информационной безопасности. Данные практики требуют масштабирования, а также специализации для информационной безопасности. Помимо привлечения студентов необходимо и стимулирование их трудоустройства в России — на данный момент лишь 7% обучившихся в России иностранцев остается в стране.

1.2

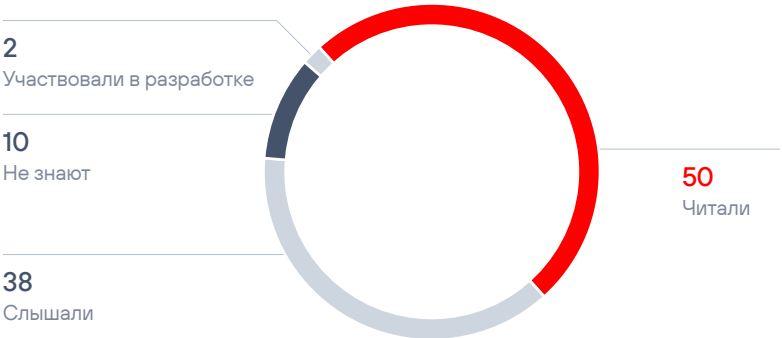
Общая рамка для сертификации специалистов в ИБ отсутствует: профессиональные и образовательные стандарты отрасли не соответствуют требованиям работодателей

Обучение специалистов построено на основе федеральных государственных образовательных стандартов и профстандартов, которые имеют ряд существенных недостатков, не позволяющих применять их как общеотраслевые документы, на основе которых осуществляется сертификация специалистов.

В настоящее время в России действует 6 профессиональных стандартов в сфере ИБ и обсуждается 2 проекта новых профессиональных стандартов.

Текущие стандарты были утверждены в 2016 году и обновлены в 2022 году. На их основе разработаны 13 федеральных государственных образовательных стандартов. При этом можно отметить низкое вовлечение компаний отрасли в принятие решений о разработке этих стандартов, что характерно для многих отраслевых рынков: например, только 2% опрошенных НТИ «Энерджинет» экспертов принимали участие в разработке образовательных стандартов, и 52% знакомы с их содержанием[7] (рисунок 6).

Рисунок 6. Степень осведомленности ИБ-специалистов об образовательных стандартах, %



Источник: НТИ «Энерджинет»

Хотя большинство (89%) участников рынка ИБ сходятся на том, что сфере ИБ необходимы профессиональные стандарты, описывающие отраслевую специфику, в настоящее время принят только один подобный стандарт — профстандарт «Специалист по ИБ в кредитно-финансовой сфере».

Практически отсутствует синхронизация профессиональных стандартов с требованиями, предъявляемыми к вакансиям на рынке труда. Это объясняется тем, что методика составления профстандартов не включает в себя необходимость анализа вакансий, публикуемых работодателями.

Динамика изменений профстандартов в значительной степени отстает от динамики изменений на рынке труда. Это связано с длительной системой утверждения и обновления стандартов, включающей в себя прохождение через Ассоциацию предприятий компьютерных и информационных технологий, Национальное агентство развития компетенций и Минтруд[8].

При этом зарубежная практика демонстрирует более динамичный и взаимосвязанный тип моделей компетенций. За счет более тесного взаимодействия представителей отрасли, образовательных учреждений и органов государственного управления достигается более высокая скорость обновления фреймворков, чем в России*.

Альтернативная же система сертификации ИБ-специалистов в России в сфере информационной безопасности проходит стадию трансформации. Если ранее профили ИБ-специалистов строились на основе международных сертификатов, выдаваемых вендорами или независимыми организациями, то в условиях ухода зарубежных вендоров и невозможности прохождения международной сертификации системе сертификации приходится адаптироваться. Крупнейшие российские вендоры начинают формировать собственные системы сертификации. Минцифры же сообщило о возможном запуске проекта по сертификации по аналогии с зарубежными ИБ-сертификатами типа CISSP, CompTIA Security+, CCNA Security и другими. Однако некоторые эксперты отмечают, что данные системы не смогут на данном этапе конкурировать с зарубежными аналогами — причиной тому является отсутствие доверия и развитого бренда[9].

1.3 На рынке происходит переток кадров в более привлекательные направления в ИТ-сфере

Участниками рынка отмечается высокий порог входа в сферу информационной безопасности. Это связано как с высокими требованиями работодателей к выпускникам в части знаний и навыков, так и с наличием практики найма по знакомству.

В таких условиях, когда для получения работы требуется обладать большим стэком компетенций, а также системой неформальных отношений, студенты и выпускники предпочитают иные направления ИТ-сектора.

Более того, требуя меньший набор компетенций от специалиста, данные направления могут предлагать большую оплату труда — медианная заработная плата в разработке на 42% больше в сравнении с информационной безопасностью, в аналитике — на 25%[10].

Можно выделить и проблему крайне низких размеров заработной платы, предлагаемой государственным сектором, который является важным работодателем в сфере информационной безопасности (рисунок 7). Лишь 24% ИБ-студентов готово работать за сумму от 20 до 40 тыс. руб. в первое время после трудоустройства[11]. В итоге подобные размеры заработной платы вовсе не стимулируют потенциальных ИБ-специалистов выбирать данное направление, особенно в регионах, где количество работодателей не столь высоко, как в Москве, Санкт-Петербурге и других крупных агломерациях.

Рисунок 7. Медианные заработные платы по секторам, 2022 г., тыс. руб.

Источник: ЦСР «Северо-Запад», по данным HeadHunter

Отмечается и психологический фактор: некоторые аспекты работы в сфере информационной безопасности могут казаться недостаточно интересными молодым специалистам. В качестве проблемы озвучиваются и особенности режима работы, когда обнаруженная атака может заставить действовать здесь и сейчас, даже в нерабочее время[12].

Можно отметить и то, что работа ИБ-специалиста часто не видна окружающим. Молодым же людям, жаждущим признания и интересных проектов, нередко деятельность в сфере ИБ кажется неинтересной. В связи с этим специалисты, имеющие требуемый набор навыков, предпочитают ИТ-сферу, а то и вовсе уходят в теневой сектор экономики, используя имеющиеся знания для обхода систем информационной безопасности. В хакинге хотел бы попробовать себя каждый пятый, особенно молодые люди в возрасте от 18 до 24 лет[13].

Можно выделить и высокую ответственность специалистов ИБ. Ошибки в сфере ИБ могут иметь крайне серьезные последствия и нанести финансовый, репутационный или иной ущерб организации. При этом отмечается, что ответственность в сфере ИБ часто перекладывается на специалистов, несмотря на отсутствие у них полномочий или ресурсов. Кроме того, в сфере ИБ предусмотрена административная и уголовная ответственность за нарушение правил безопасности. Все это может отталкивать специалистов от работы в сфере ИБ и мотивировать выбрать иную сферу деятельности.

02

РЫНОК ТРУДА В ИБ ОЖИДАЕТ ДВУХКРАТНЫЙ РОСТ СПРОСА НА СПЕЦИАЛИСТОВ И ИЗМЕНЕНИЕ СТРУКТУРЫ

К 2027 году общая потребность рынка в специалистах может увеличиться до 235–261 тыс. человек (умеренный и динамичный сценарий) в зависимости от динамики изменений в экономике, геополитике и технологической сфере. Описание сценариев представлено в Приложении А.

Большая часть потребности может быть закрыта за счет наращивания объемов подготовки кадров, внедрения технологий автоматизации труда и расширения состава потенциальных сотрудников. При этом занятость в 2027 году составит лишь 181–196 тыс. человек, то есть существующий на рынке дефицит увеличится в абсолютных значениях до 54–65 тыс. (рисунок 8), сократившись в значениях относительных.

Рисунок 8. Количество занятых и потребность на рынке труда в ИБ, тыс. рабочих мест — в умеренном и динамичном сценарии (2023–2027) гг.

Источник: ЦСР «Северо-Запад»

Потребность в сотрудниках на рынке распределена по пяти функциональным группам. Методика распределения представлена в Приложении Б. Наиболее крупной группой на рынке по состоянию на 2023 год являлись низкотехнологичные рабочие места, а также многофункциональные специалисты без определенных профессиональных ролей. Доля такой занятости составила более 40% рынка.

К 2027 году структура российского рынка труда в ИБ станет в большей степени похожа на структуру рынков технологически более продвинутых стран, таких как США и Германия[14], что будет выражаться в более явном распределении функциональных ролей (рисунок 9). Этот тренд обусловлен факторами, описанными в разделе 3 данного доклада.

Рисунок 9. Потребность рынка труда в ИБ в разрезе функциональных групп работников в 2023 и 2027 гг., тыс. чел.

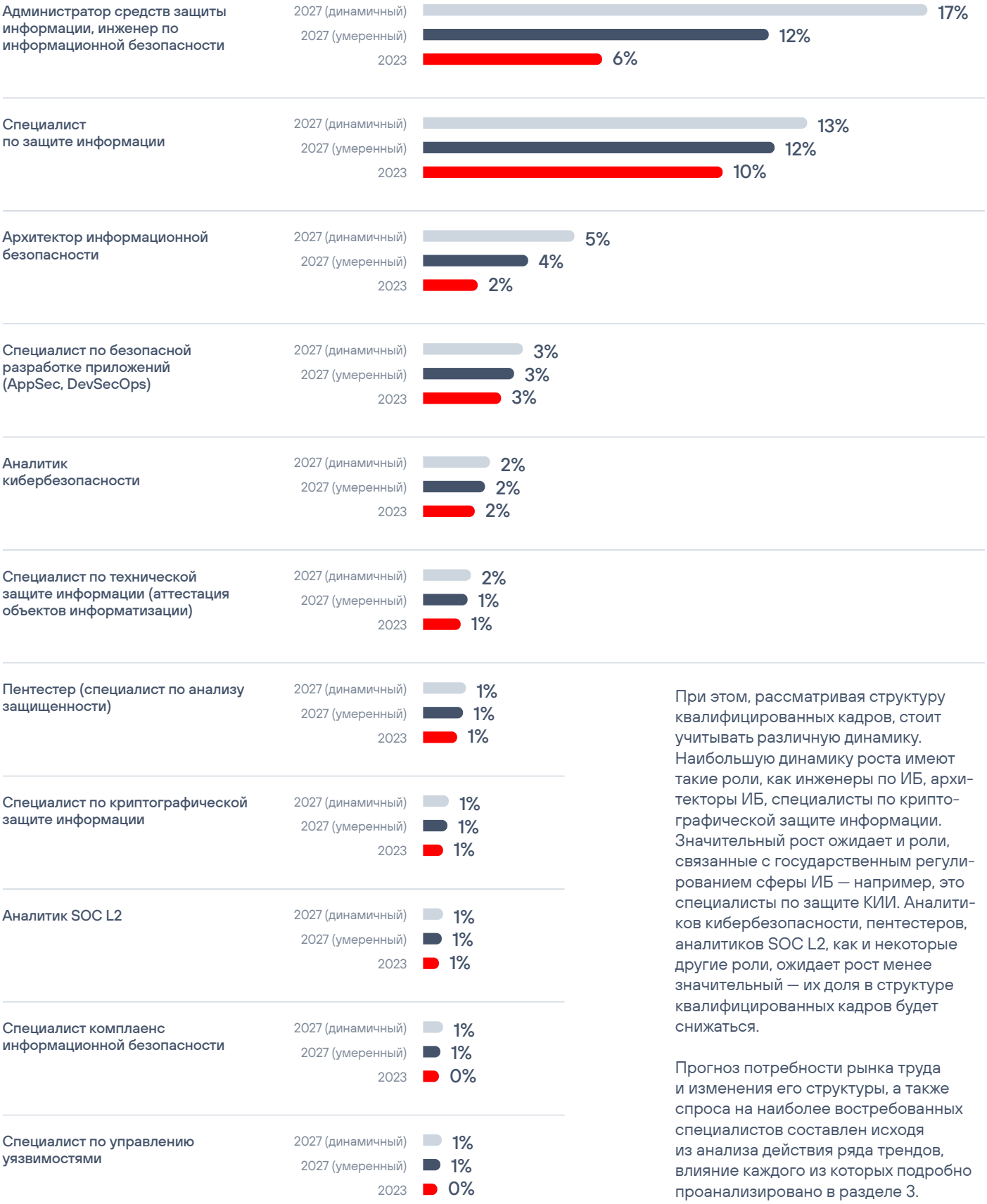
Источник: ЦСР «Северо-Запад»

В обоих сценариях предусмотрено сокращение формальной занятости, формируемой за счет найма сотрудников на позиции, связанные с ИБ, при низких профессиональных требованиях, за счет повышения глубины разделения труда и найма профессионалов, специализированных в той или иной позиции. Многофункциональные специалисты будут замещаться путем вынесения функций ИБ на аутсорсинг — в пользу специализированных поставщиков ИБ-услуг[15]. При этом допустима ситуация, когда для закрытия всех кадровых позиций, которые необходимо создать в связи с ужесточением законодательства, организации начнут решать вопрос формально, что приведет к дополнительному росту потребности в многофункциональных, порой низкоквалифицированных специалистах в отдельные годы. Тем не менее в долгосрочной перспективе рынок будет стандартизироваться и технологизироваться, а функции ИБ будут переходить в руки профессионалов, сокращая долю потребности в многофункциональных специалистах.

Все это скажется и на конкретных функциональных ролях в сфере ИБ. Ожидается существенный рост доли квалифицированных кадров на рынке труда, связанный с описанной выше трансформацией рынка труда. В первую очередь данная тенденция затронет базовые позиции — инженера по ИБ и специалиста по защите информации, то есть функциональные роли, близкие к статусу многофункциональных специалистов в сфере ИБ, но все же с более четко выраженным набором задач и требований (рисунок 10).

Рисунок 10. Наиболее востребованные ИБ-специалисты в 2023 и 2027 году, % от общего числа вакансий на рынке труда ИБ

Источник: ЦСР «Северо-Запад»

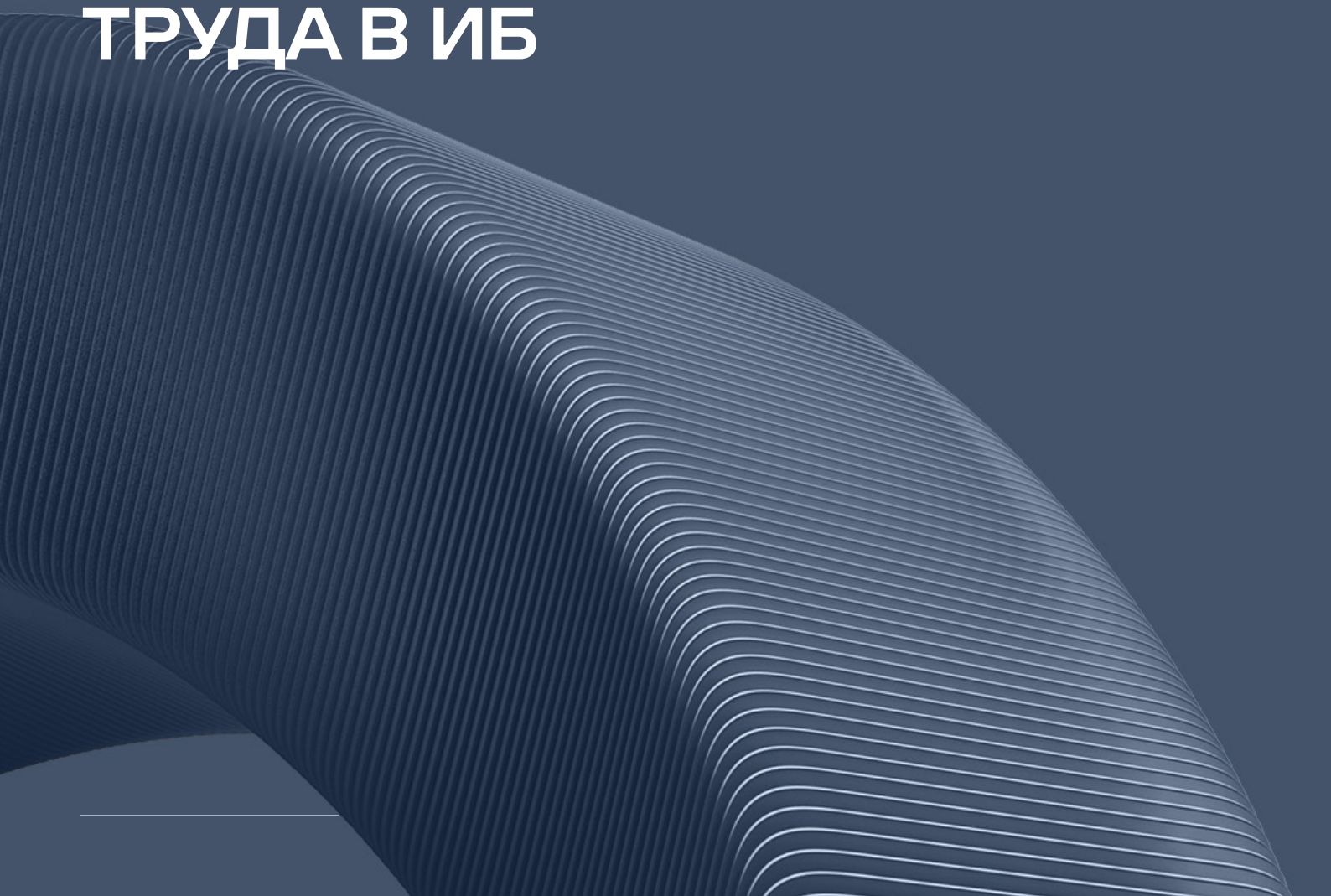


При этом, рассматривая структуру квалифицированных кадров, стоит учитывать различную динамику. Наибольшую динамику роста имеют такие роли, как инженеры по ИБ, архитекторы ИБ, специалисты по криптографической защите информации. Значительный рост ожидает и роли, связанные с государственным регулированием сферы ИБ — например, это специалисты по защите КИИ. Аналитиков кибербезопасности, пентестеров, аналитиков SOC L2, как и некоторые другие роли, ожидает рост менее значительный — их доля в структуре квалифицированных кадров будет снижаться.

Прогноз потребности рынка труда и изменения его структуры, а также спроса на наиболее востребованных специалистов составлен исходя из анализа действия ряда трендов, влияние каждого из которых подробно проанализировано в разделе 3.

03

ТРЕНДЫ РЫНКА ТРУДА В ИБ



3.1

Развитие ИИ позволит автоматизировать как низкотехнологичные, так и сложные задачи. Часть позиций потеряет актуальность, но будут созданы новые рабочие места

Искусственный интеллект — основной технологический тренд, влияющий на рынок труда в области информационной безопасности в ближайшие три года и на долгосрочную перспективу. Рост роли ИИ может быть более масштабным трендом по сравнению с другими технологическими тенденциями, такими как развитие облачных архитектур, развитие специализированного аутсорсинга и увеличение количества кибератак, которые также повлияют на рынок ИБ.

Но влияние ИИ на рынок труда ИБ будет иметь разносторонний характер. Три ключевых аспекта этого влияния:

1. Автоматизация бизнес-процессов с использованием искусственного интеллекта приведет к сокращению некоторых вакансий и кадровых позиций на рынке труда в области информационной безопасности. Это особенно актуально для аналитиков SOC первого и второго уровня.
2. Создание новых видов бизнес-процессов приведет к увеличению количества профессий и объема занятости, в первую очередь среди архитекторов и инженеров.
3. Трансформация бизнес-процессов с помощью искусственного интеллекта потребует изменения профессиональных компетенций сотрудников в области информационной безопасности. Это повлечет за собой необходимость их переобучения и перемещения между кадровыми позициями внутри рынка труда. Кроме того, использование инструментов искусственного интеллекта повысит эффективность работы начинающих специалистов, что снизит порог входа в профессию.

Автоматизация бизнес-процессов

Автоматизация бизнес-процессов будет осуществляться путем масштабирования решений, которые позволят сократить объем необходимого человеческого труда для выполнения задач в ИБ. Глобальные вендоры разрабатывают и выпускают продукты, основанные на использовании генеративного искусственного интеллекта, машинного обучения и других преимущественно программных методов и архитектур, ориентированных на автоматизацию процессов[16].

Так, развитие систем на основе генеративных сетей позволит автоматизировать и повысить продуктивность труда аналитиков, архитекторов, инженеров, аудиторов, консультантов и менеджеров в области информационной безопасности. Наибольшее влияние автоматизация окажет на мониторинг, обнаружение и оценку угроз, аномалий и уязвимостей, реагирование на инциденты безопасности и их расследование, обнаружение и классификацию вредоносных программ, тестирование на проникновение и другие задачи аналитиков. Использование искусственного интеллекта в этих областях может привести к сокращению занятых в соответствующих бизнес-процессах на 50%[17].

Российские вендоры также разрабатывают и внедряют в практику технологии, способствующие автоматизации ИБ-процессов. Примером такого метапродукта является автопилот MaxPatrol O2, разработанный Positive Technologies. Использование данного инструмента позволяет повысить эффективность аналитиков в 30–50 раз, высвобождает до 64 человеко-часов в неделю, ранее необходимых для обработки подозрительной активности аналитиками SOC, а также снижает требуемый уровень квалификации ИБ-специалистов, так как самостоятельно формирует и выполняет сценарии реагирования на угрозу.

Таким образом, многие компетенции специалистов в области информационной безопасности в ближайшие три года могут быть в некоторой степени автоматизированы. Так, в умеренном варианте прогноза к 2027 г. ожидается снижение потребности в кадрах на 14 тыс. человек за счет фактора автоматизации, динамичный сценарий предполагает автоматизацию 39 тыс. рабочих мест. При этом автоматизация будет стимулировать и создание новых рабочих мест — преимущественно архитекторов и инженеров.

Однако есть и компетенции, полная автоматизация которых в ближайшее время маловероятна: в первую очередь это задачи архитекторов, инженеров и менеджеров, связанные с настройкой автоматизированных систем и работой с людьми.

Артем Сычев,
советник генерального директора Positive Technologies

«Автоматизированы будут задачи специалистов первой и второй линии SOC, они не будут нужны в таком объеме. Из двух аналитиков SOC останется один. Но кто-то все равно должен смотреть в монитор, а при необходимости — пойти и разобраться, что произошло. По другим ролям будет другое требование к качеству. Инструментарий для автоматизации разнообразен и охватывает множество задач, но ручные операции останутся. Точно не будет автоматизировано расследование инцидентов, задачи по разработке архитектуры безопасности, менеджмент. Важным требованием станет понимание предметной области. Автоматизация приведет к тому, что "универсальных солдат" будет становиться меньше».

Создание новых видов бизнес-процессов

Внедрение искусственного интеллекта приведет к открытию новых вакансий на рынке труда, многие из которых сейчас являются нишевыми. В частности, существенно расширится сегмент специалистов по машинному обучению в информационной безопасности. Ожидается, что к 2027 году появится около 12 тысяч новых рабочих мест для таких специалистов. Часть из них будет создана за счет перетока специалистов из других сегментов рынка труда — автоматизирующихся позиций аналитиков и группы «многофункциональные специалисты».

Алексей Тотмаков,
технический директор
VK Tech

«Перемещения Security Analyst в AppSec или архитекторы возможны, и такие переходы периодически происходят, экспертиза Security Analyst крайне полезна при таком переходе. При прочих равных, на позицию AppSec я предпочту взять человека с опытом Security Analyst. Такие перемещения обычно работают в одну сторону — в AppSec перетекают из Security Analyst, обратный переход случается крайне редко».

Трансформация бизнес-процессов

Внедрение искусственного интеллекта привлекает внимание к этим технологиям как работодателей, так и соискателей. Для работодателей внедрение искусственного интеллекта может означать повышение общей инвестиционной привлекательности проектов и решение конкретных бизнес-задач. Например, задач по снижению барьера входа в специальность для доступа к более обширным источникам кадров. По прогнозам Gartner, внедрение генеративного искусственного интеллекта поможет устранить дефицит кадров, позволив половине людей, занимающих должности начального уровня в области кибербезопасности, обходиться без специального образования[18]. Исследование Microsoft показало, что пользовавшиеся ИИ-продуктом Copilot for Security аналитики-новички в ИБ повысили точность выполнения задач на 44%[19]. В ближайшие три года темп роста потребности в ИБ-специалистах, владеющих компетенциями в ИИ, сохранится на уровне +30% в год. Именно такой темп был зафиксирован в 2023 году в совместном исследовании hh.ru и МТС RED[20].

В горизонте ближайших трех лет также можно ожидать появления новых профессий и ролей, связанных с применением искусственного интеллекта в ИБ — например, MLSecOps, которые фокусируются на проблемах безопасности, возникающих в процессе разработке и внедрения систем машинного обучения. Это выходит за рамки деятельности DevSecOps, осуществляющих обеспечение безопасности процессов разработки ПО без привязки к системам машинного обучения, и MLOps, не специализирующихся на вопросах безопасности, и требует использования специализированных инструментов и наличия особых навыков.

Анна Прабарщук,
руководитель службы управления персоналом «Газинформсервис»

«Уже в ближайшие два года будет увеличиваться востребованность ролей, связанных с разработкой ИИ и применением больших языковых моделей в ИБ, в том числе инженеров данных. В более отдаленной перспективе трех-четырех лет сформируется запрос на навык промпт-инжиниринга. Если говорить о совсем новых ролях — это MLSecOps. Сам ИИ подвержен атакам, и нужен совсем другой механизм защиты от них. Это сильно отличается от имеющейся сейчас позиции DevSecOps».

Учитывая спектр задач, поддающихся автоматизации, можно отметить, что автоматизация имеет разное влияние на конкретные профессии в информационной безопасности. Профессии и роли в ИБ можно разделить на три группы по уровню влияния автоматизации — он отражает долю задач специалиста, которая потенциально может быть автоматизирована.

Таблица 1. Оценка влияния применения ИИ на автоматизацию труда в области информационной безопасности

	Степень влияния	Функциональные группы
1	**Сильное влияние ИИ на профессию** (уровень автоматизации 50%)	• Аналитики • Многофункциональные специалисты
2	**Умеренное влияние ИИ на профессию** (уровень автоматизации 25%)	• Аудиторы и консультанты • Менеджеры
3	**Незначительное влияние ИИ на профессию** (уровень автоматизации 10%)	• Архитекторы и инженеры

Источник: ЦСР «Северо-Запад»

Учитывая процессы, связанные с внедрением ИИ в сферу информационной безопасности, можно уверенно сказать, что ИИ существенно повлияет на рынок труда ИБ. Совокупное влияние процессов автоматизации, создания новых рабочих мест, связанных с ИИ, и трансформации имеющихся может стать причиной структурной перестройки.

В умеренном сценарии данная перестройка затронет преимущественно многофункциональных специалистов: автоматизация приведет к снижению востребованности данных специалистов (ожидается снижение потребности на 15 тыс. человек), однако существенно вырастет потребность в квалифицированных аналитиках и инженерах (ожидается рост потребности на 13 тыс. человек).

В динамичном сценарии ожидается более радикальная трансформация компетентностного профиля: автоматизация затронет не только многофункциональных специалистов, но и некоторых аналитиков. В условиях автоматизации ряда задач будет параллельно расти спрос на высококвалифицированных аналитиков, имеющих компетенции в сфере ИИ, инженеров и архитекторов, и снижаться востребованность специалистов, чья деятельность более подвержена автоматизации, — аналитиков SOC1, многофункциональных специалистов и так далее. Учитывая данные процессы, ожидается общее снижение потребности в кадрах, связанное с внедрением ИИ (рисунок 11).

Рисунок 11. Влияние развития искусственного интеллекта на рынок труда в сфере ИБ, 2024—2027 гг., тыс. чел.

Источник: ЦСР «Северо-Запад»

3.2

Облачные технологии формируют новые позиции для архитекторов и аналитиков, а также ведут к увеличению потенциала ИБ-аутсорсинга

Облачная безопасность является одним из ключевых технологических трендов 2024 года на мировом рынке ИБ. Облачные технологии являются одновременно главной областью угроз, ключевым направлением инвестиций и наименее контролируемой сферой с точки зрения внедрения планов по управлению рисками в крупнейших компаниях мира[21]. Компетенции, связанные с облачной защитой (cloud computing security), были наиболее востребованы у мировых компаний-работодателей в ИБ в 2023 году[22].

Что касается России, запрос на ИБ-специалистов, способных работать в облачных средах, будет расти с масштабированием облачной инфраструктуры и снятием ограничений на применение облаков в госкорпорациях и крупном бизнесе. В настоящее время средний уровень облачной зрелости российских компаний составляет 35%, и только около 3% компаний применяли облачные сервисы в 2022 году. Однако уже к 2025 году этот показатель должен составить уже около 6% рынка — около 130 тыс. компаний[23]. Например, существенный импульс на переход к использованию облачных сервисов получит банковский и финансовый сектор — регуляторные механизмы по применению облачных сервисов в кредитно-финансовой сфере планирует в ближайшие годы внедрить Банк России[24].

Ответственность за обеспечение облачной безопасности несет не только провайдер облачных услуг, но и пользователь[25,26]. В случае если компаниям придется самостоятельно нести ответственность за информационную безопасность в облаке, количество требуемых к 2027 году специалистов по облачной безопасности может составить до 84 тыс. человек — с учетом того, что количество компаний, имеющих стратегию безопасности и использующих облачные сервисы, будет расти.

В связи с указанными выше трендами на рынке труда складывается потребность в новых специалистах — инженерах по облачной защите (Cloud Security Engineer). Это специалист по ИБ с опытом создания и эксплуатации разнообразных облачных сервисов. В задачи такого специалиста входит[27]:

1. Анализ и предотвращение рисков облачных сред.
2. Разработка и развертывание безопасной облачной инфраструктуры.
3. Управление идентификацией и доступом пользователей в облаке.
4. Мониторинг и реагирование на угрозы в рамках облачных платформ.
5. Разработка и контроль за соблюдением политик безопасности в облаке.
6. Контроль комплаенса и аудит рисков в облаке.
7. Интеграция безопасности в разработку облачных сервисов (DevSecCloudOps).
8. Внедрение и управление инструментами безопасности в облаке.

Развитие облачных технологий также формирует существенный потенциал аутсорсинга ИБ*. Ожидается, что аутсорсинг будет расти быстрее общего рынка ИБ[28]. При условии, что аутсорсинг вырастет до 15% от общего рынка ИБ к 2027 году, потребность в специалистах, обеспечивающих безопасность подключившихся к облаку организаций, может существенно снизиться. В динамичном сценарии аутсорсинг позволит снизить потребность в ИБ-специалистах на 81 тыс. человек к 2027 году, в умеренном — на 12 тыс.

Таким образом, совокупно облачные технологии и аутсорсинг трансформируют структуру занятости в ИБ, сокращая низкотехнологичные рабочие места и позиции аналитиков в организациях — клиентах облачных провайдеров, одновременно увеличивая потребность в инженерах и архитекторах на стороне клиента. При этом количество рабочих мест в ИБ на стороне провайдера не покажет существенный рост благодаря повышению эффективности труда.

* Под аутсорсингом в докладе понимается передача части задач по ИБ непрофильных организаций-клиентов специализированным ИБ-компаниям и провайдерам облачных сервисов.

Артем Калашников,
управляющий директор Центра информационной безопасности дочерних и зависимых обществ АО «Газпромбанк»

«Сколько бы компаний-потребителей ни подключалось к облаку, центральное ядро, которое обеспечивает безопасность, по сути управляется одним и тем же составом людей и тем же набором средств автоматизации. Даже если будет вал подключений к облаку, количество специалистов, обеспечивающих безопасность на стороне провайдера, увеличится несущественно».

Учитывая разнонаправленные тенденции, когда, с одной стороны, облачные технологии требуют новых квалифицированных специалистов, а с другой — позволяют снизить потребность в ИБ-специалистах за счет аутсорсинга, все же стоит отметить, что развитие облачных технологий стимулирует создание новых рабочих мест: — в динамичном сценарии совокупный рост потребности составит 11 тыс. человек, в умеренном — около 2 тыс. При этом как в умеренном, так и динамичном сценариях ожидается снижение востребованности многофункциональных специалистов и рост спроса на труд аналитиков, инженеров и архитекторов, а также аудиторов и консультантов (рисунок 12).

Рисунок 12. Влияние облачных технологий на рынок труда в сфере ИБ, 2024—2027 гг., тыс. чел.

Источник: ЦСР «Северо-Запад»

3.3

Внедрение цифровых валют и новых финансовых технологий будет обеспечивать рост потребности в ИБ в банковском и финансовом секторе

Применение цифровых валют и развитие финансовых технологий увеличит запросы на ИБ-специалистов со стороны банковского и финансового сектора, который уже является одним из крупнейших работодателей для специалистов ИБ. По имеющимся оценкам, российские банки потратят на внедрение цифрового рубля 30–50 млрд, значительная часть из которых уйдет на создание систем ИБ и кадровое обеспечение[29].

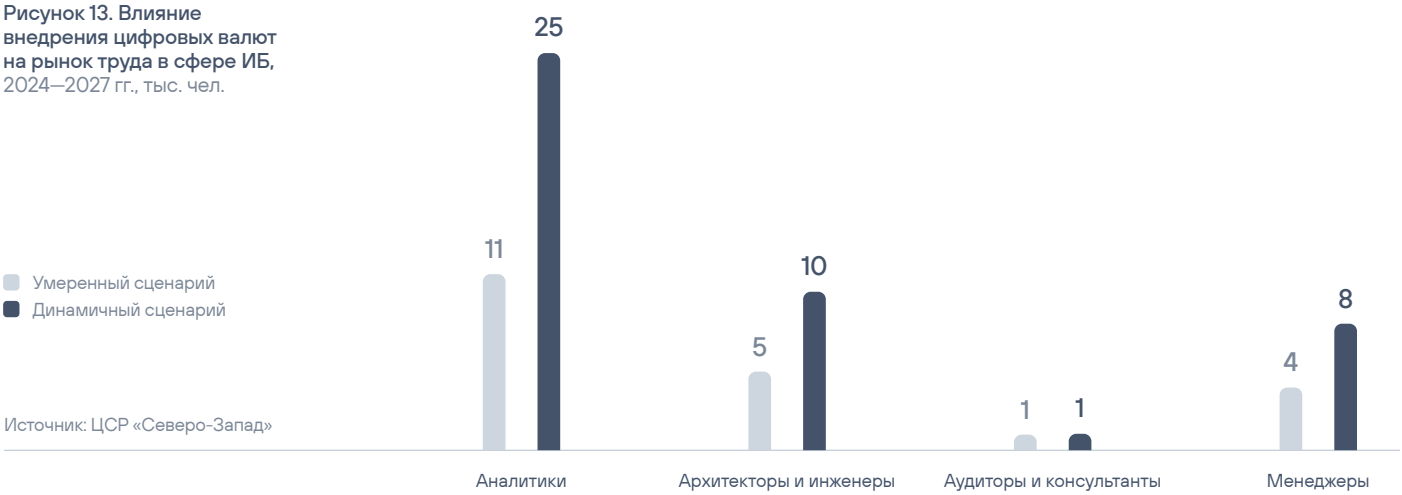
В части развития финансовых технологий Банком России помимо цифровых валют планируется реализовать широкий набор мер по контролю рисков ИБ в сфере банковских и финансовых услуг, в том числе:

1. Создать дополнительные механизмы аудита в части защиты информации и операционной надежности, облачных сервисов и безопасности приложений, что приведет к росту спроса на специалистов-аудиторов ИБ по данным направлениям.
2. Обеспечить механизмы анализа инцидентов ИБ и операционной надежности, проведения киберучений по расширенным сценариям.
3. Создать правовые условия для аутсорсинга информационных технологий и использования облачных услуг финансовыми организациями.

Внедрение цифровых валют и финансовых технологий обеспечит формирование

44 **тыс. новых позиций в ИБ в динамичном варианте прогноза (рисунок 13).**

Рисунок 13. Влияние внедрения цифровых валют на рынок труда в сфере ИБ, 2024—2027 гг., тыс. чел.



Источник: ЦСР «Северо-Запад»

3.4 Растущее внимание государства к проблемам ИБ выльется в рост рабочих мест как для разработчиков отечественных решений, так и для менеджеров в ряде госкомпаний и стратегических предприятий

Импортозамещение и государственное регулирование оказывают значительное влияние на рынок труда в области информационной безопасности. Это влияние проявляется как в увеличении спроса на специалистов в данной области, так и в изменении требуемых компетенций.

В условиях санкций и ухода с российского рынка некоторых иностранных вендоров возникает потребность в качественных решениях в области информационной безопасности. Так, несмотря на наличие на рынке российских ИБ-решений всех определенных ЦКИТ классов, 24% российских компаний в 2023 году отметили отсутствие отечественных решений, способных решить их задачи. Эта ситуация способствует развитию российских компаний, занимающихся разработкой и внедрением продуктов в области информационной безопасности. Ожидается стабильный рост российского рынка разработки решений в области информационной безопасности в период с 2024 по 2027 год, примерно на 22% ежегодно. Доля отечественных вендоров также значительно возрастет: если в 2023 году она составляла 70%, то к 2027 году она достигнет 95%[30].

Государственное регулирование отрасли информационной безопасности оказывает значительное влияние на рынок труда. Важным событием стало издание Указа Президента № 250[31], согласно которому все субъекты критической информационной инфраструктуры, государственные и системообразующие организации должны создать структурные подразделения и назначить ответственного сотрудника в области информационной безопасности к 2025 году.

Влияние на рынок труда оказывают и процессы, связанные с развитием системы ГосСОПК А. Подключение хостинг-провайдеров к системе с параллельным наложением на них обязательств по борьбе с вредоносными узлами, а также децентрализация системы, выраженная формированием групп реагирования на киберинциденты в регионах, будут способствовать росту востребованности ИБ-специалистов.

Потенциальное изменение порядка категорирования объектов КИИ также окажет существенное влияние на рынок труда. Если сейчас субъекты КИИ могут сами категоризировать значимость своих объектов, то в случае внедрения нового порядка подразумевается формирование органами власти (по согласованию с ФСТЭК России) перечней типовых отраслевых объектов КИИ, включающих в себя типы информационных систем и выполняемых ими функций и видов деятельности. Подобное решение может повлиять на количество объектов КИИ, что будет способствовать и росту потребности в ИБ-специалистах.

Указанные меры и решения существенно увеличивают потребность в специалистах в области информационной безопасности. Ожидается, что с 2024 по 2027 год потребность в архитекторах и инженерах, занятых в разработке отечественных решений в области информационной безопасности, увеличится на 19 тысяч человек. Также ожидается увеличение потребности в менеджерах — их понадобится еще 14 тысяч, главным образом из-за требований, содержащихся в Указе Президента № 250. Таким образом, ожидаемый прирост потребности в кадрах составит до 33 тысяч специалистов. Но появление соответствующего числа занятых на рынке труда ИБ вряд ли будет носить скачкообразный характер в силу необходимости поиска средств на их содержание.

Помимо количественного роста потребности в специалистах в области информационной безопасности, наблюдается и изменение требований к их компетенциям. В связи с отказом от решений глобальных вендоров ожидается увеличение спроса на специалистов, работающих с отечественными решениями в области информационной безопасности, а также с решениями на основе открытого исходного кода.

Андрей Арефьев,
директор по инновационным проектам InfoWatch

«Компании не смогут быстро импортозаместиться, они будут жить в гибридном мире. Возникнет тренд на специалистов, которые будут владеть лучшими практиками работы с отечественным стэком операционных систем, корпоративными каталогами, с отечественными DNS и так далее. Людей, которые понимают, как безопасно реализовать импортозамещение, как обеспечить безопасность гибридной инфраструктуры, недостаточно. Поэтому данное направление будет расти».

Необходимо учесть и обратное влияние государственного вмешательства в сферу информационной безопасности, выраженное созданием государственных платформ. Одной из целей создания государственных платформ является попытка решить проблему дефицита кадров и уязвимости государственной информационной инфраструктуры. Это может привести к снижению потребности в специалистах в области информационной безопасности.

Так, в текущий момент 80% функционала действующих государственных информационных систем совпадает, при этом нет возможности его переиспользования. В условиях нехватки квалифицированных кадров независимое создание информационных систем и строительство ЦОД каждым органом власти признано неэффективным. Проблемой является и существенная зависимость от решений глобальных вендоров — более 50% государственных информационных систем подвержено критическим информационным рискам[32].

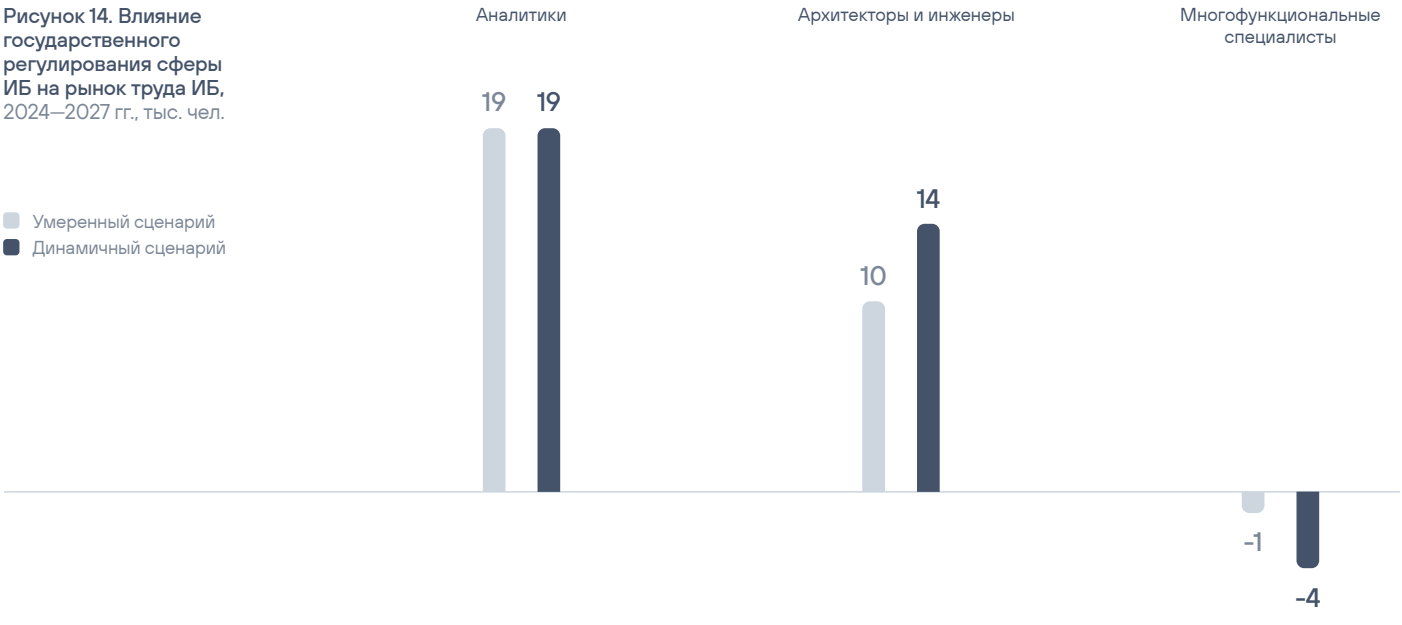
Создание платформы «Гостех», предназначенной для быстрого и эффективного создания государственных информационных систем и цифровых сервисов, нацелено на повышение информационной безопасности органов государственной власти и снижение потребности в специалистах за счет эффекта масштаба. В рамках реализации данного проекта создаются 7 взаимосвязанных центров обработки данных и единый центр реагирования и мониторинга кибератак, представляющий собой единую согласованную систему обеспечения информационной безопасности платформы, осуществляющую в том числе мониторинг и реагирование на инциденты ИБ[33]. Подобная мера станет причиной высвобождения кадров, задействованных в обеспечении информационной безопасности государственных информационных систем.

При этом в первую очередь будут ликвидированы низкотехнологичные и не требующие высокой квалификации рабочие места — усиление контроля и проверок соответствия систем ИБ потребует не просто формального соблюдения регуляторных требований, но и реального создания работающих ИБ-подразделений с прошедшими специальную подготовку специалистами[34].

Общий объем сокращений низкотехнологичных рабочих мест в результате государственного регулирования может составить до 4 тыс. человек.

Таким образом, государственная политика в сфере ИБ в контексте импортозамещения и государственного регулирования имеет разнонаправленный характер. С одной стороны, меры, призванные стимулировать развитие отечественных решений и повысить безопасность критической информационной инфраструктуры, стимулируют создание новых рабочих мест в сфере ИБ. С другой стороны, деятельность, направленная на повышение производительности труда и безопасности государственных сервисов, приводит к высвобождению рабочей силы. Тем не менее количество создаваемых рабочих мест, связанных с данным фактором, превысит число ликвидируемых рабочих мест: в динамичном сценарии в связи с государственным регулированием рост потребности в ИБ-специалистах составит 29 тыс. человек, в умеренном — 28 тыс. (рисунок 14).

Рисунок 14. Влияние государственного регулирования сферы ИБ на рынок труда ИБ, 2024—2027 гг., тыс. чел.



Источник: ЦСР «Северо-Запад»

3.5 С учетом развития российских платформ багбаунти можно ожидать увеличения количества багхантеров

В сфере информационной безопасности активно развиваются цифровые платформы для поиска услуг пентестеров — платформы багбаунти.

Российский рынок платформ багбаунти сформировался около 10 лет назад и продолжает развиваться. Крупнейшими платформами багбаунти в России на сегодняшний день являются Bug Bounty RU, Standoff 365 Bug Bounty и BI.ZONE Bug Bounty. Общее число багхантеров на данных платформах, по данным 2023 г., составляет порядка 20 тыс. чел.

В число российских организаций, запускающих программы багбаунти, входят: «Яндекс», Rambler&Co, VK group, «ПИК», Ozon, Wildberries, «СберМаркет», «Азбука вкуса», «Авито», «ЮMoney», «Альфа-Банк», «Тинькофф», банк «Точка», «Лаборатория Касперского», «СКБ Контур», Минцифры России и другие.

С учетом развития российских платформ багбаунти можно ожидать соответствующего роста количества багхантеров, предоставляющих свои услуги на данных площадках. Способствовать развитию багхантинга и выхода его из «тени» в России может и принятие соответствующего закона. Так, в конце 2023 года в Государственную Думу внесены поправки в Гражданский кодекс, разрешающие внешним специалистам при поиске уязвимостей в информационных системах и IT-инфраструктурах изучать их компоненты без получения специального разрешения от каждого правообладателя. Эксперты отмечают, что данного закона недостаточно для легализации багхантинга, однако и этот шаг может позитивно сказаться на данном формате деятельности.

Важным шагом для багбаунти является и активное участие Минцифры в развитии багхантинга. Так, в конце 2023 года был запущен второй этап программы по поиску уязвимостей на портале «Госуслуги». В июне же 2023 года Минцифры предложило всем желающим записаться на бесплатный учебный онлайн-курс «Профессия — белый хакер».

Учитывая все это, ожидается, что к 2027 г. число багхантеров, зарегистрированных на специализированных платформах, увеличится на 4 тыс. чел. как в динамичном сценарии, так и в умеренном — около 27% по сравнению с 2023 г., и составит около 24 тыс. чел.

Таким образом, в краткосрочной перспективе такой вариант заработка может привести к замедлению темпов роста найма аналитиков ИБ в компаниях, которые все чаще будут пользоваться услугами багхантеров.

3.6 Развитие квантовых вычислений и коммуникаций

Применение квантовых технологий может существенно трансформировать киберугрозы и технологии киберзащиты. Эксперты Агентства национальной безопасности США считают, что уже в течение ближайших 3–5 лет квантовые компьютеры будут применяться для решения задач, связанных с информационной безопасностью, в том числе для защиты и атаки объектов критической инфраструктуры и других информационных систем в киберконфликтах[35]. Наличие подобных технологий в США неизбежно потребует и от российских специалистов по ИБ навыков работы с квантовыми технологиями. Кроме того, с развитием квантовых технологий может быть получен доступ к уже собранным противником или злоумышленником зашифрованным данным (store now — decrypt later), что делает методы постквантовой криптографии актуальной компетенцией уже сейчас[36]. Так, в США уже введены требования, согласно которым информация уровня top secret должна быть зашифрована по стандартам постквантовой криптографии[37].

В настоящее время в России ведется разработка образовательных стандартов для подготовки специалистов по информационной безопасности с перечнем знаний по квантовым вычислениям и коммуникациям[38]. Однако спрос на таких специалистов в горизонте до 2027 года, вероятно, будет ограничен сферой национальной безопасности: в том числе компетенциями в сфере квантовой информационной безопасности и постквантовых методов защиты должны будут овладевать специалисты по криптографии, специалисты по противодействию иностранным техническим разведкам, сотрудники, задействованные в обеспечении безопасности объектов КИИ. Учитывая ограниченность применения данных технологий, существенного влияния на рынок труда в сфере ИБ развитие квантовых вычислений и коммуникаций не окажет.

Масштабирование же применения квантовых технологий в сфере информационной безопасности для бизнеса является более долгосрочным трендом, который начнет существенно влиять на рынок не ранее чем через 5 лет[39]. Учитывая это, в долгосрочном горизонте могут возникнуть новые специфические роли и профессии, связанные именно с кибербезопасностью в постквантовом мире.

04

ПОТЕНЦИАЛ СИСТЕМ ПРИВЛЕЧЕНИЯ И ПОДГОТОВКИ КАДРОВ В ИБ ДЛЯ РЕАГИРОВАНИЯ НА ВЫЗОВЫ РЫНКА ТРУДА

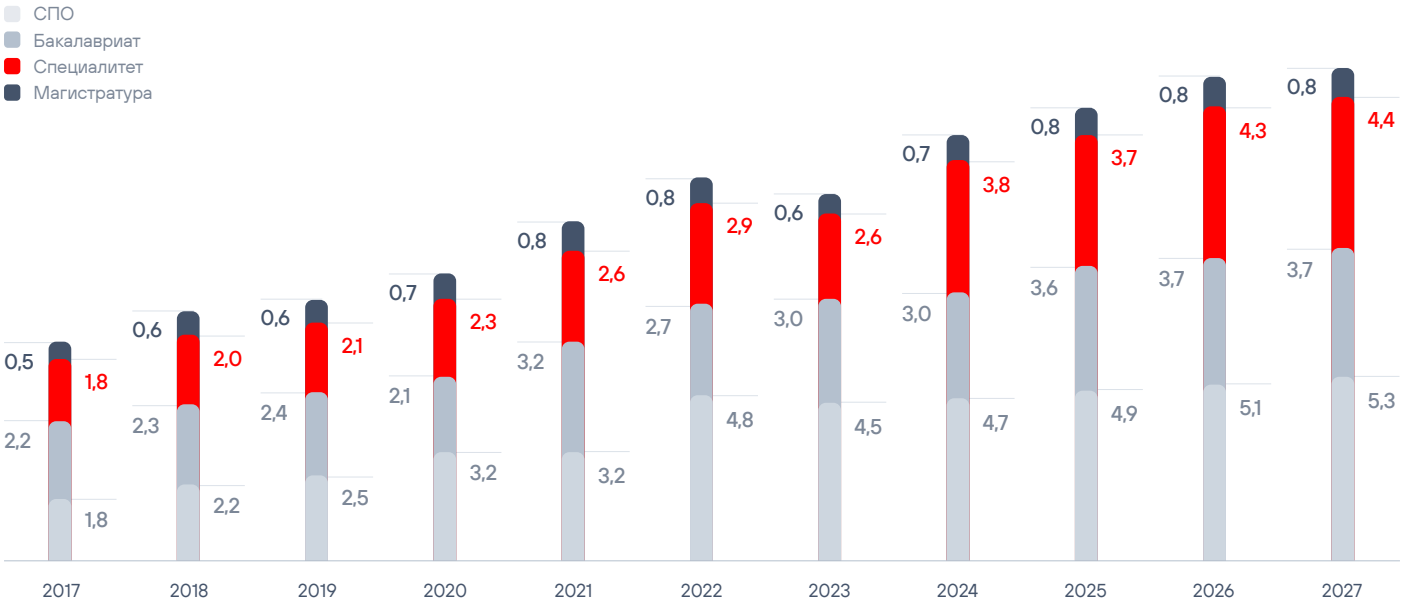
4.1

Объемы подготовки кадров растут, но темп роста и качество образования отстает от динамики рынка труда

За период с 2017 по 2023 год число выпускников, получивших образование в сфере ИБ, выросло на 69%. В дальнейшем ожидается сохранение позитивной динамики — к 2027 году число выпускников ИБ-специальностей может превысить 14 тысяч человек в год (рисунок 15). Однако данные темпы отстают от темпов роста потребности. Более того, следует учитывать, что не все выпускники в результате трудоустроятся в секторе ИБ, так как имеется существенная конкуренция с рынком труда в ИТ-секторе. Кроме того, существует вероятность выхода численности выпускников на плато в горизонте 2–3 лет, то есть прирост может остановиться, если этому вопросу не будет уделяться должного внимания.

Рисунок 15. Выпуск специалистов по уровням подготовки в рамках направления «Информационная безопасность», тыс. чел.

Источник: ЦСР «Северо-Запад», по данным о контрольных цифрах приема Минобрнауки России и Минпросвещения России



Меняется и структура подготовки — за период с 2017 года по 2023-й доля выпускников среднего профессионального образования (СПО) выросла с 28,5% до 42. Это объясняется потребностью в кадрах, от которых не требуется высокая квалификация, а только навыки эксплуатации ИБ-решений. В долгосрочном горизонте (за рамками рассматриваемого периода) спрос на такие кадры на рынке будет снижаться вследствие автоматизации, а необходимость разработки импортонезависимых архитектур и решений потребует от специалистов более высокого уровня квалификации.

В ближайшие годы ожидается рост доли специалитета в общей численности обучающихся. Отказ от Болонской системы и возврат пятилетних программ может снизить скорость выхода молодого специалиста на рынок труда. В случае массового разворачивания этого сценария участникам рынка предстоит более плотная интеграция с университетами, в том числе с целью имплементации корпоративных стандартов, требований и содержания в образовательные программы, реализуемые государственными вузами и колледжами.

Помимо недостаточных объемов выпуска специалистов, проблемой является и разрыв образования и рынка. Отмечается, что качество подготовки не всегда соответствует запросам рынка труда, хотя в последние годы удовлетворенность работодателей качеством выпускников в целом повысилась[40]. Образовательные и профессиональные стандарты, которые определяют содержание образовательных программ, фиксируют консервативный набор навыков и компетенций. В существующих профессиональных стандартах прописаны лишь обобщенные трудовые функции и отсутствуют упоминания конкретных технологий и методов, используемых специалистами в области информационной безопасности. Отмечается и отсутствие деталей, связанных с особенностями практической работы, например программным и аппаратным обеспечением, оборудованием для лабораторий. Все это не позволяет применять стандарты как единую методическую рамку для определения квалификации специалистов. Как следствие, это с одной стороны обеспечивает большую гибкость для образовательных учреждений, однако с другой стороны приводит к тому, что во многих вузах ресурсная и материально-техническая база не соответствует реалиям рынка труда, а качество подготовки специалистов находится на низком уровне.

Кроме того, отмечается проблема неравномерного качества преподавания в сфере информационной безопасности. Связана данная проблема с тем, что в условиях такой динамичной сферы, как ИБ, внедрять передовой опыт в обучение может только преподаватель-практик, владеющий навыками работы с современными СЗИ. Это касается и новых актуальных технологий, таких как искусственный интеллект и машинное обучение, которые только внедряются в сферу ИБ и пока не упоминаются ни в одном образовательном стандарте.

Однако существует ряд факторов, мешающих появлению таких преподавателей в нужном количестве. Так, с одной стороны, отмечается низкая заинтересованность практиков в передаче знаний будущим специалистам — уровень оплаты труда в образовательных учреждениях значительно ниже, чем в ИБ-компаниях, при этом преподавание может отнимать существенное время[41]. С другой стороны, участники отрасли указывают, что и академическое сообщество крайне консервативно и не готово к активному сотрудничеству с практиками из отрасли[42].

Проблемой является и существующая система повышения квалификации профессорско-преподавательского состава. Отмечается необходимость развития практики прохождения преподавателями стажировок в ИБ-компаниях. В текущий момент данный механизм носит эпизодический характер, не оказывая существенного влияния на качество преподавания.

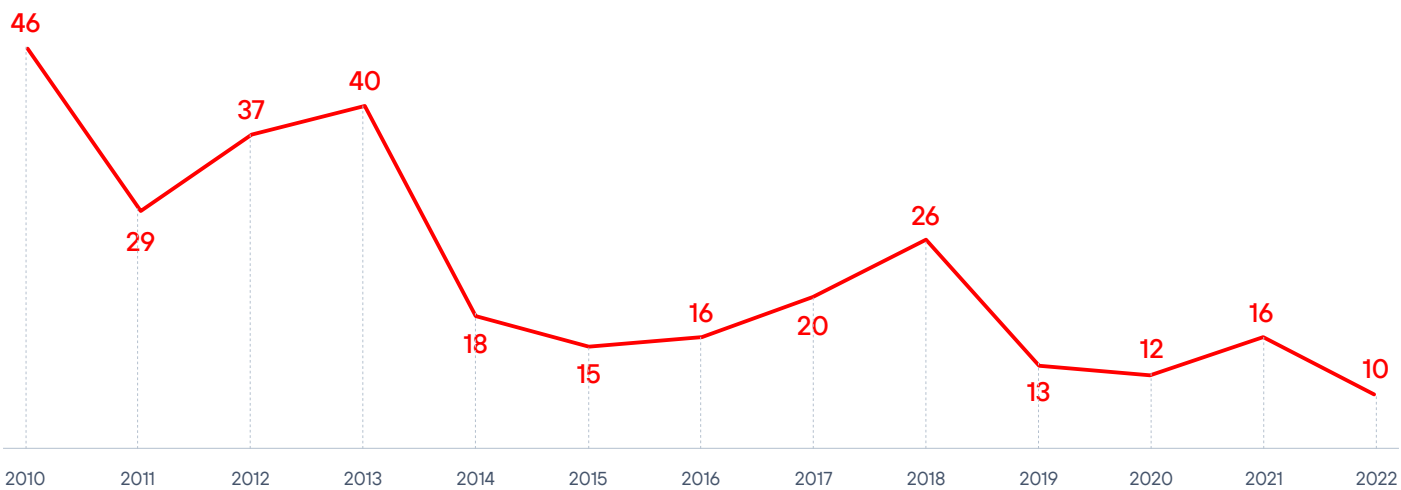
Более того, в условиях роста числа обучающихся, требующего увеличения числа преподавателей в сфере ИБ, число потенциальных преподавателей, напротив, снижается.

Так, в соответствии с пунктом 4.4.6 действующих ФГОС, должны иметь ученую степень не менее 50% в случае бакалавриата и 55% в случае специалитета от общей численности педагогических работников образовательного учреждения, участвующих в реализации образовательных программ. При этом в реализации программ высшего образования в сфере информационной безопасности должен участвовать как минимум один педагогический работник, имеющий ученую степень или ученое звание по научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

При этом заметно устойчивое снижение числа диссертаций, защищаемых по данному направлению. Если в 2010 их число составляло 46 единиц, 45 из которых были кандидатскими, то в 2022 году — лишь 10, 8 из которых были кандидатскими (рисунок 16).

Рисунок 16. Число диссертаций, защищенных по специальности ВАК РФ 05.13.19 «Методы и системы защиты информации, информационная безопасность», ед. в год

Источник: ЦСР «Северо-Запад», по данным электронной библиотеки диссертаций DisserCat



Таким образом, в условиях снижения количества лиц, обладающих профильной степенью, учебные заведения могут столкнуться с невозможностью реализации программ в сфере информационной безопасности.

Эксперты отрасли также выражают неуверенность в том, что специалисты, защитившие кандидатские диссертации, выберут преподавательскую карьеру. В качестве причин отмечается низкая заработная плата, практика заключения срочных трудовых договоров с профессорско-преподавательским составом, а также специфика работы со студентами.

Кроме того, отдельными участниками отрасли отмечается оторванность работ и науки в целом от реальных потребностей рынка. Конференции и форумы, по словам участников отрасли, существуют параллельно: мероприятия ИБ-компаний практически не включают выступлений ученых, академические конференции — практиков. Асинхронность наблюдается и в сфере публикаций: в сфере ИБ очень мало специализированных журналов, а многие известные отраслевые тематические журналы не учитываются в публикационной активности преподавателей. В связи с этим преподаватели вынуждены публиковаться в изданиях, где их статьи не достигают целевой аудитории и не могут быть адекватно оценены[43]. В качестве проблемы также отмечается несовершенство самой методологии исследования и обеспечения информационной безопасности, лежащей в основе современной академической науки в сфере ИБ[44].

Примером реакции на указанные проблемы являются практики взаимодействия работодателей, образовательных организаций и государства с целью повышения практикоориентированности образования и науки для их соответствия рыночным требованиям. Например, многие крупные вендоры тесно сотрудничают с системой высшего образования, реализуя обучающие курсы по применению собственных продуктов[45].

Руслан Рахметов,
CEO Security Vision

«Отрасль ИБ достаточно молодая, учебные программы еще недавно очень явно не успевали за развитием технологий, методов противодействия кибератакам и эволюцией киберугроз. Работодателям приходилось первые 1–2 года доучивать молодых специалистов — то, чему их учили в вузах, либо было далеко от практики, либо было устаревшим на несколько лет. Однако за последние несколько лет сформировался тренд на сотрудничество вузов и крупных компаний-работодателей, которые ведут занятия и приглашают студентов на оплачиваемые стажировки в свои компании. На таких стажировках студенты могут окунуться в мир «реальной ИБ», познакомиться с новыми технологиями защиты, подтянуть свои знания и наметить пути для дальнейшего обучения. Поэтому можно с радостью отметить, что в последнее время качество выпускников растет — и не в последнюю очередь за счет таких партнерств».

В случае системы СПО данная практика в первую очередь выражена фактом включения направлений подготовки в ИБ в программу «Профессионалитет»[46], подразумевающую повышение доли практических заданий в учебном процессе, организацию учебно-производственных мастерских, а также привлечение к преподаванию экспертов — сотрудников предприятий реального сектора.

В рамках системы высшего образования тенденция по повышению практикоориентированности образования также продемонстрирована повышением степени интеграции науки, обучения и производства. Например, участие высших образовательных учреждений в программе «Приоритет 2030» в контексте сферы ИБ предполагает не только подготовку высококвалифицированных ИБ-специалистов, но и разработку собственных ИБ-решений совместно с индустриальными партнерами[47]. Еще одним направлением сотрудничества является подготовка специалистов в передовых инженерных школах[48].

Отмечаются и иные формы сотрудничества, способствующие повышению качества образования и выходящие за рамки реализации совместных образовательных программ. Так, проблема низкой материально-технической базы отдельными участниками ИБ-рынка решается при помощи практик льготного или безвозмездного предоставления ПО и оборудования. Например, ОКБ «САПР» в рамках партнерского соглашения с ПНИПУ передал оборудование для преподавания предмета «Программно-аппаратные средства защиты информации»[49]. Можно отметить и возникновение базовых кафедр с университетами — примером такой практики является сотрудничество InfoWatch и ВШЭ.

Обновление и актуализация знаний и компетенций профессорско-преподавательского состава осуществляется на основе партнерских соглашений. Например, Positive Technologies в рамках проекта «Школа преподавателей кибербезопасности» обучает преподавателей вузов, предоставляя им необходимые знания о современных трендах в ИБ. Подобные школы имеются также у других вендоров, например InfoWatch. Тем не менее, масштаб влияния этих программ пока остается достаточно ограниченным.

Тенденция по выстраиванию сотрудничества с потенциальными работодателями характерна и для системы дополнительного профессионального образования. Так, в условиях роста спроса на образование в сфере информационной безопасности, при общем спаде интереса к дополнительному образованию в ИТ-сфере[50] интеграторы онлайн-курсов с целью повышения конкурентоспособности своих программ выстраивают стратегии по трудоустройству обучающихся, а также привлекают к реализации курсов университеты и профильные компании ИТ-сектора. Примером данной практики может послужить сотрудничество платформы Skillfactory, НИЯУ МИФИ и компании Positive Technologies[51].

Более того, программы дополнительного профессионального образования в сфере ИБ не только представлены онлайн-курсами, но и организуются высшими учебными заведениями, вендорами, разрабатывающими ИБ-продукты, а также различными отраслевыми центрами ДПО, что демонстрирует как высокую степень востребованности данных образовательных продуктов, так и готовность образовательных учреждений и работодателей участвовать в подготовке и развитии кадров для сферы ИБ[52].

Возникают и специализированные центры ДПО, обучающие исключительно или преимущественно специалистов в сфере ИБ. Данные центры часто сотрудничают как с ИБ-компаниями, так и с образовательными учреждениями. Примером такого центра может служить CyberEd, реализующий образовательные программы как для физических лиц, так и для юридических, в том числе университетов. При этом подобные организации часто тесно сотрудничают с ИБ-компаниями, привлекая экспертов для преподавания. В случае CyberEd преподавателями выступают сотрудники Positive Technologies, F.A.C.C.T., «Лаборатории Касперского» и так далее.

При этом стоит отметить способность системы ДПО более оперативно и гибко реагировать на требования рынка, способствуя устранению дефицитов и разрывов на рынке труда. Например, в связи с изданием Указа Президента № 250[53], подразумевающего наличие заместителя директора по ИБ, и постановления Правительства РФ № 1272[54], устанавливающего к нему требования, появился отдельный тип программ ДПО, направленный на подготовку требуемых специалистов.

Все это позволяет системе ДПО быть эффективным инструментом подготовки кадров в сфере ИБ: отмечается, что благодаря ДПО в 2023 году было подготовлено более 15 тыс. ИБ-специалистов[55], на онлайн-курсы приходится порядка 2–3 тыс. специалистов ежегодно*. При этом в условиях ограниченности расширения системы профессиональной подготовки ожидается и дальнейший рост рынка ДПО.

Реализация проекта «Цифровые кафедры» должна также способствовать развитию системы ДПО в сфере ИБ. А присвоение дополнительной ИТ-квалификации более чем 385 тыс. студентам к 2025 году[56] и обучение в партнерстве с потенциальными работодателями может вести к сокращению дефицита ИБ-специалистов.

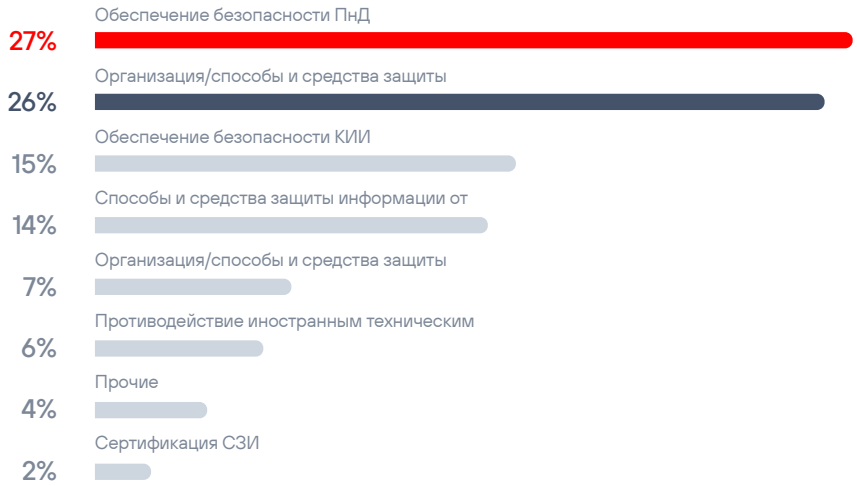
Так, в четырех университетах предусмотрено обучение по программам, связанным именно с информационной безопасностью. При этом стоит отметить различные подходы к обучению: так, в РГАУ — МСХА представлена отраслевая программа «Информационная безопасность в АПК»[57], в ТУСУР[58], КНИТУ[59] и МИЭТ[60] же предусмотрено получение дополнительного образования в сфере ИБ студентами, получающими ИТ-образование. Особый акцент в данных программах сделан на безопасности компьютерных сетей — программы КНИТУ И МИЭТ полностью посвящены данной теме, программа ТУСУР выделяет 130 часов на нее.

* Расчет на основе количества резюме на HeadHunter, упоминающих наличие сертификата об обучении в онлайн-школах.

Однако потенциал цифровых кафедр и ДПО в целом несколько ограничен необходимостью согласования программ с регуляторами в области ИБ, что, с одной стороны, уменьшает возможности быстрого масштабирования образовательных программ, а с другой — позволяет исключить откровенно «мусорные» курсы и образовательные программы.

Следствием данного факта является некоторая однотипность, стандартизация программ, представленных на рынке. Так, в случае с программами повышения квалификации доля оригинальных программ, не базирующихся на примерных программах, предлагаемых ФСТЭК России, достаточно мала (рисунок 17).

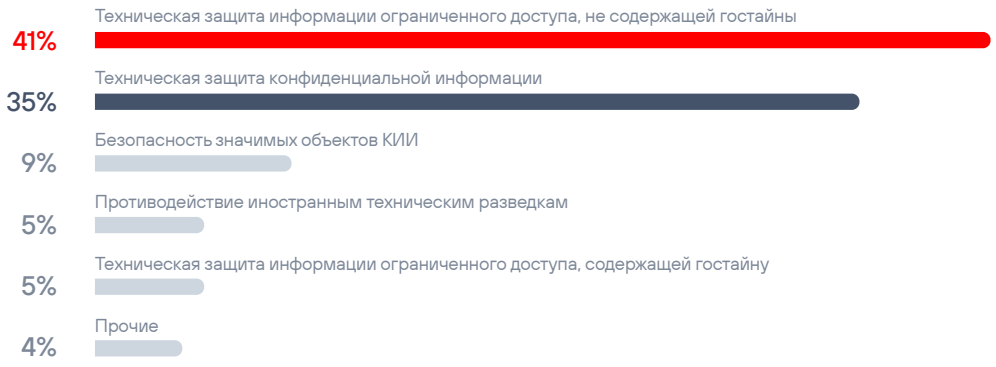
Рисунок 17. Структура программ повышения квалификации, согласованных ФСТЭК России



Источник: ЦСР «Северо-Запад», по данным ФСТЭК России

Аналогично можно сказать и о программах профессиональной переподготовки (рисунок 18).

Рисунок 18. Структура программ профессиональной переподготовки, согласованных ФСТЭ



Источник: ЦСР «Северо-Запад», по данным ФСТЭК России

Таким образом, учитывая ограниченность традиционной системы подготовки кадров, важным элементом формирования кадрового состава должна стать более гибкая система ДПО. В связи с этим ИБ-компаниям необходимо развивать собственные программы, отвечающие их потребностям, а также активно сотрудничать с существующими платформами и центрами. В рамках же классической системы образования игрокам рынка стоит стремиться к повышению практико-ориентированности образования.

4.2

Вовлечение новых возрастных когорт сотрудников и сохранение старшего поколения на рабочих местах способно внести существенный вклад в достижение кадровой стабильности в ИБ

По данным ISC2 для глобального рынка, в 2023 г. доля новых сотрудников в возрасте старше 50 лет в кибербезопасности выросла до 19% (в 2022 году доля таких сотрудников составляла 6%)[61]. Россия не является исключением. Напротив, в нашей стране проблема стоит наиболее остро. ИБ-компаниям придется брать на работу все больше людей старших возрастов. В долгосрочной перспективе изменится возрастная структура занятых в секторе, и требования к специалистам, программы обучения придется адаптировать для более возрастных сотрудников.

С учетом общей тенденции старения населения и дефицита кадров ожидается увеличение доли сотрудников старших возрастов не только в экономике страны в целом, но и в сфере ИБ в частности. Число новых сотрудников старше 50 лет в ИБ в России к 2027 г. может увеличиться на 12 тыс. чел.

Повышение возраста соискателей будет сопровождаться также приходом в отрасль неспециалистов, то есть соискателей без базового образования в сфере информационной безопасности. Это позволит решить ряд проблем дефицита кадров. Но не по всему спектру профессий в отрасли, а прежде всего по тем направлениям, для которых характерен более низкий уровень требований к знанию технологий.

Таким образом, для обучения данных категорий востребованным навыкам потребуется развитие системы образования. Так, некоторые зарубежные образовательные организации адаптируют свои программы, создавая курсы, где материал сильно упрощен, и предлагая их пожилым людям, заинтересованным в сфере ИТ. Отмечается и эффективность онлайн-курсов[62]. Учитывая это, российским участникам рынка следует популяризировать обучение востребованным и не требующим длительного обучения навыкам.

Проблемой является и страх людей среднего возраста[63]. В связи с этим необходимо демонстрировать успешные примеры, организовать мероприятия, где лица среднего возраста могли бы обмениваться опытом и навыками. Подобные меры будут способствовать разрушению сложившихся стереотипов и страхов, а также привлечению людей среднего возраста в ИБ.

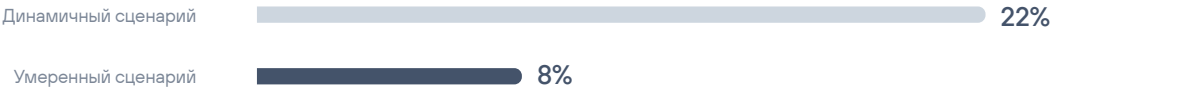
За базовую модель обучения лиц среднего возраста может быть взята «Школа 21», организованная Сбером (или ее французский аналог L'Ecole 42). Геймификация образовательного процесса, подход peer-to-peer (обучение друг у друга без участия преподавателей), командная работа и другие методы, используемые в данном формате обучения, показывают высокое качество и скорость подготовки в сочетании с высокими показателями трудоустройства выпускников. Данный формат не всеми признается, является альтернативой высшему образованию и не может рассматриваться как потенциально массовый. Однако он демонстрирует востребованность рынком ИТ новых подходов к обучению специалистов, которые, вероятно, следует внедрять и в сфере ИБ.

4.3

За счет роста вовлечения женщин будет закрыто от 8 до 22 тыс. новых вакансий на рынке труда в ИБ к 2027 году

В последние годы наблюдается увеличение доли женщин в сфере ИБ. За последние годы доля женщин в сфере ИБ в мире значительно выросла — с 11% в 2017 г. до 25% в 2021 г.[64] Ожидается, что к 2025 году этот показатель составит уже 30%[65]. Вовлечение женщин в сферу ИБ является одним из факторов сокращения дефицита кадров. Так, число женщин в ИБ в России может увеличиться на 22 тыс. чел (рисунок 19).

Рисунок 19. Прирост числа женщин в ИБ, 2024—2027 гг., тыс. чел.



Источник: ЦСР «Северо-Запад»

Кроме того, западные исследования показывают, что привлечение девушек может способствовать повышению эффективности работы — отмечается, что женщины могут иначе подходить к решению проблем[66].

В качестве существующих причин низкой заинтересованности девушек в сфере ИБ и информационных технологий в целом отмечаются такие факторы, как особенности воспитания, стереотипы, особенности организационной культуры в ИТ-компаниях и отделах. Решением же данной проблемы считается поощрение изучения девушками STEM-дисциплин, проведение информационных кампаний, разрушающих сложившиеся стереотипы, а также развитие образовательных, менторских и наставнических программ.

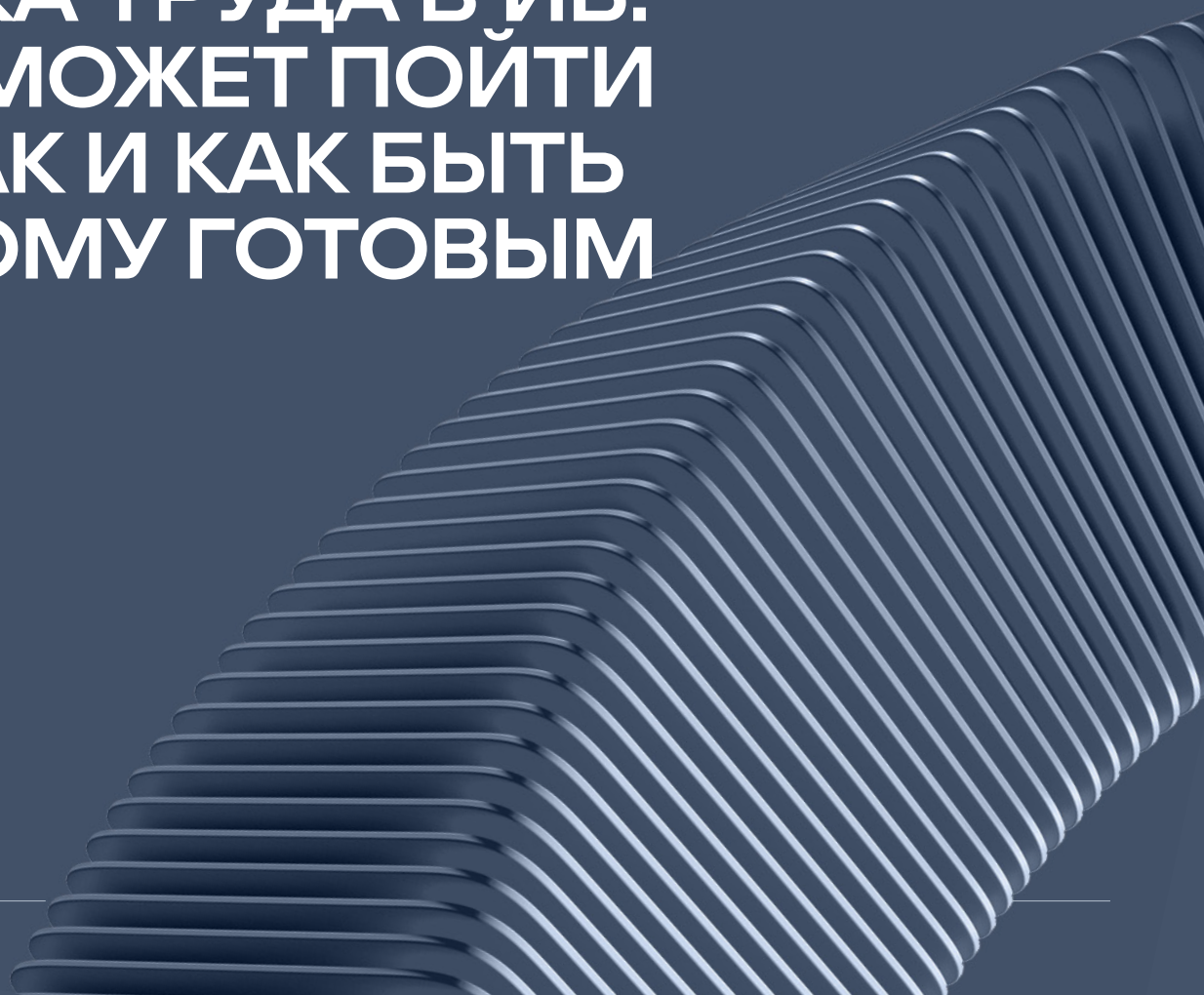
Для достижения данных целей участники рынка ИБ за рубежом предлагают различные решения, способствующие росту числа девушек в отрасли. Так, SANS Institute, являющийся крупнейшей исследовательской и образовательной организацией в сфере ИБ в мире, организует особые академии погружения в ИБ, разработанные специально для девушек[67]. Некоторые программы предназначены и для девочек в возрасте 8–12 лет. Так, компанией Mastercard разработана программа Girls4Tech, нацеленная на обучение STEM-навыкам и на мотивацию девочек изучать такие сферы, как криптология, обнаружение угроз, искусственный интеллект и машинное обучение[68].

Российским участникам сектора также требуется активное взаимодействие с женской аудиторией. Хотя в рамках сектора ИБ уже функционирует «Женсовет по ИБ»[69], нацеленный на создание среды, где женщины могли бы обмениваться опытом и экспертными знаниями, данного явления недостаточно — следует поднимать интерес к данному направлению у девушек, популяризировать его.

Для этого также необходимо способствовать разрушению стереотипов, а также содействовать в приобретении навыков, востребованных в ИБ. Достижению данных целей может способствовать и организация мероприятий, связанных с участием девушек в ИБ-сфере, и взаимодействие компаний отрасли с обучающимися в школах, колледжах и университетах, а также обучение заинтересованных в ИБ девушек, ранее выбравших иные направления обучения. За основу может быть взят опыт организации WiCyS, нацеленной на содействие участию женщин в сфере ИБ.

05

«ЧЕРНЫЕ ЛЕБЕДИ» РЫНКА ТРУДА В ИБ: ЧТО МОЖЕТ ПОЙТИ НЕ ТАК И КАК БЫТЬ К ЭТОМУ ГОТОВЫМ



5.1

Появление «сильного» ИИ может существенно сократить потребность в кадрах в сфере ИБ

«Сильный» искусственный интеллект, то есть такой, который способен выполнять различные задачи, взаимодействовать с человеком и самостоятельно адаптироваться к изменяющимся условиям, может появиться уже в горизонте ближайших трех лет[70]. Такие прогнозы дают некоторые визионеры. Эта технология может стать дестабилизирующим фактором для рынка труда в ИБ.

Внедрение «сильного» ИИ должно существенно повысить продуктивность труда в ИБ и значительно усилить потенциал автоматизации, описанной в разделе 3.1. При условии, что сильный ИИ не откроет новый класс задач в ИБ, в которых человек будет эффективнее машины, его масштабирование может привести к снижению темпов роста зарплат в отрасли и в конечном итоге к существенному замедлению темпов найма специалистов и даже масштабным сокращениям[71].

Однако наиболее вероятно, что «сильный» ИИ, превосходящий человека в любых задачах, не появится никогда или появится за горизонтом 2030-х гг.

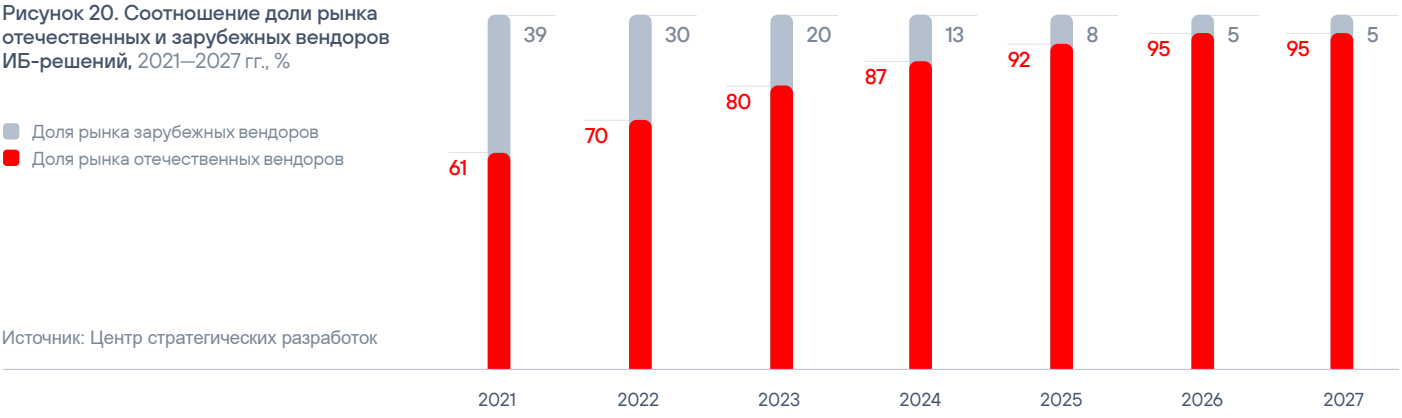
5.2

Глобальный рынок ИБ: изоляция vs реинтеграция

В настоящее время ситуацию на рынке решений в ИБ в России можно охарактеризовать как «изоляцию». Так, в 2023 году доля отечественных вендоров средств защиты составила около 80% рынка.

Ожидается, что доля отечественных вендоров будет расти и дальше — максимум будет достигнут к 2026 году на уровне 95% рынка в связи с окончательным уходом традиционных для российского рынка зарубежных вендоров (Cisco, IBM, Fortinet и других (рисунок 20). При этом влияние «серого» импорта предполагается на минимальном уровне. Причиной этому является отсутствие технической поддержки зарубежных решений[72], а также запрет на их применение в ряде компаний указом Президента России.

Рисунок 20. Соотношение доли рынка отечественных и зарубежных вендоров ИБ-решений, 2021—2027 гг., %



Источник: Центр стратегических разработок

Однако допускается возможность роста доли зарубежных вендоров до 8% — за счет экспансии на отечественный рынок компаний из дружественных стран, особенно Китая.

Таким образом, возможна обратная ситуация: насыщение российского рынка импортными решениями и услугами ИБ, в том числе из дружественных стран, может существенно — на 10–15 тыс. чел. — снизить потребность в архитекторах и инженерах.

Важно также отметить высокий экспортный потенциал российских компаний, который формируется в первую очередь в дружественных странах[73]. В случае роста экспортного рынка вдвое может понадобиться еще около 4 тыс. архитекторов и инженеров для обслуживания внешних заказчиков.

06

ДИНАМИЧНЫЙ РОСТ ПОТРЕБНОСТИ РЫНКА ТРУДА В ИБ ПОТРЕБУЕТ ДЕЙСТВИЙ СО СТОРОНЫ ИГРОКОВ РЫНКА

Прогноз потребности рынка труда, основанный на анализе воздействия трендов, представленный в разделе 3, показывает, что в случае, если отрасль ИБ в ближайшие несколько лет не получит существенного притока кадров, то дефицит специалистов обострится и может привести к кризису в отрасли. Для того чтобы избежать значительного дефицита кадров, который может привести к неадекватному «перегреву» зарплатных предложений и надуванию «пузыря» на рынке труда, участникам и регуляторам рынка необходимо предпринять ряд действий.

6.1

Масштабная экспансия игроков рынка ИБ в образовательный сектор

Нехватка кадров будет требовать более активного, чем сейчас, сотрудничества вендоров и крупных нанимателей в ИБ с образовательными учреждениями. Это касается как среднего профессионального образования, так и высших учебных заведений. Отдельным направлением можно также выделить вовлечение школьников в раннюю профориентацию и выполнение некоторых задач в ИБ.

В части СПО — в данный момент в рамках проекта «Профессионалитет» сфера ИБ представлена лишь в трех регионах, что дает потенциал для ее масштабирования ИБ-компаниями[74].

В высшем образовании высокий потенциал имеет создание передовых инженерных школ в сфере информационной безопасности, Центров искусственного интеллекта в сфере информационной безопасности, в том числе реализующих разработку решений и программы подготовки ИБ-кадров с навыками ИИ.

Потребуется и масштабирование существующих практик. Уже сейчас ИБ-компаниями активно привлекаются студенты на стажировки и практики, создаются базовые кафедры, организуются различные мероприятия, где студенты могут более подробно узнать о профессиях, востребованных компаниями, попробовать себя в роли ИБ-специалиста. В условиях растущего кадрового дефицита данные практики должны развиваться, привлекая все больше студентов в профессию. Большее развитие должны получить и практики предоставления оборудования, программного обеспечения образовательным учреждениям, программы повышения квалификации преподавателей на базе ИБ-компаний.

6.2

Участие в программах дополнительного профессионального образования и предложение новых форматов ускоренной подготовки

В условиях роста востребованности ИБ-специалистов на рынке труда наблюдается и увеличение спроса на онлайн-образование в сфере информационной безопасности. С целью повышения конкурентоспособности своих программ интеграторы онлайн-курсов выстраивают стратегии по трудоустройству обучающихся, а также привлекают к реализации курсов профильные компании ИТ-сектора. Подобное сотрудничество стимулирует развитие востребованных на рынке компетенций у потенциальных специалистов, позволяет проще и быстрее находить кадры для организаций. Таким образом, в условиях растущей нехватки ИБ-специалистов компаниям следует развивать сотрудничество с платформами, разрабатывать и реализовывать совместные программы подготовки ИБ-специалистов, обучая их навыкам, востребованным в организации.

Распространяется практика самостоятельного создания программ повышения квалификации и переобучения игроками рынка. 61% компаний уже организуют обучение по ИБ. Однако данные практики пока носят внутриорганизационный характер — они направлены на повышение квалификации действующих сотрудников, зачастую не предполагают внешней экспертизы[75]. Более активное применение программ профессиональной переподготовки игроками рынка позволит привлекать заинтересованные в обучении кадры, обучать их под свои задачи, тем самым минимизируя влияние проблемы дефицита кадров.

Перспективной является практика создания частных университетов и реализация образовательных программ в партнерстве вендоров и их клиентов, заинтересованных в специалистах, имеющих навыки эксплуатации конкретных решений. Однако фактором риска в этом случае является высокая мобильность сотрудников, которая может привести к тому, что инвестиции корпоративных игроков в обучение могут не окупиться.

6.3

Вовлечение школьников в профессию

Главными элементами вовлечения школьников в профессию ИБ-специалиста должны стать популяризация и геймификация получения знаний и навыков, необходимых в сфере ИБ.

Описывая популяризацию профессии, стоит отметить, что уже сейчас некоторые школы участвуют в программах профориентации, организуемых компаниями из ИТ-сферы. Развивается практика организации ИТ- и инженерных классов, ориентированных на практическое обучение учащихся навыкам, требуемым в ИТ-сфере[76].

Геймификация же, предполагающая использование игровых механик в обучении, позволяет продемонстрировать специфику деятельности и потенциально вовлечь школьника в профессию. Так, для школьников проводятся хакатоны, олимпиады и соревнования, в том числе и в области информационной безопасности. Развитие данных практик организациями ИБ-сферы позволит как заинтересовать молодое поколение в профессии, так и частично сформировать необходимый стэк навыков еще на уровне обучения в школе.

Кроме того, школьники могут вовлекаться через платформы самозанятости, например на платформы багбаунги, ведь поиск уязвимостей не всегда требует образования. Например, возраст самого молодого хакера в России — 11 лет[77].

6.4

Привлечение региональной рабочей силы в сферу информационной безопасности

В региональном разрезе сохраняется высокая доля Москвы в привлечении ИБ-специалистов — 46% вакансий во II квартале 2023 года пришлось на столицу. При этом доля вакансий с удаленным форматом работы достаточна низка[78]. Таким образом, в условиях преимущественного размещения ИБ-компаний в Москве, Санкт-Петербурге и иных крупных городах единственным возможным вариантом привлечения кадров из регионов остается переезд.

Особенно остро проблема стоит в регионах СКФО и ДВФО — при том, что в данных регионах живет около 12% населения страны, на них приходится менее 4% вакансий в сфере ИБ.

В данных регионах слабо представлены крупные работодатели — основными местами работы ИБ-специалистов являются государственные учреждения и органы власти. При этом в данных регионах сформирована система подготовки кадров — специалистов в сфере ИБ.

В условиях кадрового дефицита возникает потребность в развитии дистанционного формата работы, а также в открытии региональных офисов, что позволило бы привлечь потенциально заинтересованных в сфере ИБ жителей регионов к работе в компаниях, офисы которых находятся в Москве и Санкт-Петербурге.

Анна Прабарщук,
руководитель службы управления персоналом «Газинформсервис»

«Сейчас ИБ развивается по всей стране: компании, которые централизовано находятся в Москве и Санкт-Петербурге, будут открывать все больше площадок в регионах, в первую очередь в таких крупных городах, как Казань, Новосибирск, Екатеринбург — в агломерациях, где неплохо учат ИТ и ИБ, и где с развитием удаленной занятости концентрируется много людей».

Данные практики уже демонстрируются крупными ИБ-компаниями. Например, офисы Positive Technologies, помимо Москвы и Санкт-Петербурга, представлены еще в Новосибирске, Нижнем Новгороде, Самаре и Томске.

Развитие площадок в регионах может осуществляться в том числе путем развертывания коворкинговых пространств в кампусах университетов, в том числе в рамках создания новых университетских кампусов в России.

Мировая практика показывает, что создание университетских кампусов, в которых размещаются офисные площадки коммерческих компаний, позволяет увеличить интеграцию образования и рынка, в том числе через сотрудничество выпускников университетов и студентов. Кроме того, для студентов создаются возможности работы в коммерческих компаниях без необходимости покидать кампус, что упрощает их привлечение на рабочие места[79].

6.5

Развитие новых подходов к разработке стандартов для сертификации и подготовки специалистов в ИБ

Как было описано в п. 1.2, в настоящее время профессиональные и образовательные стандарты не успевают за динамичными изменениями рынка труда. Одним из путей решения проблемы разработки профессиональных стандартов может стать формирование негосударственной ассоциации или объединения крупнейших игроков рынка ИБ. Такая ассоциация способна сформировать собственные фреймворки и стандарты, которые были бы приняты на уровне индустрии наравне с государственными профессиональными стандартами.

В дальнейшем модель разработки таких независимых фреймворков могла бы лечь в основу методики разработки и обновления профессиональных и образовательных стандартов. Подобный подход в настоящее время реализуется в сфере развития искусственного интеллекта Альянсом в сфере ИИ.

Альянс в сфере ИИ разработал собственную базовую модель профессий и компетенций в сфере ИИ, охватывающую 36 ключевых компетенций по трем категориям, шесть семейств специальностей и ролевую модель специалиста по каждой из них. Альянс также проводит независимую аккредитацию вузовских программ по направлению искусственного интеллекта и формирует специализированные курсы для преподавателей по внедрению лучших практик обучения и научной деятельности в ИИ[80].

Отрасль ИБ может выступить с аналогичной инициативой при условии, что компаниям — участникам отрасли, включая крупных работодателей, вендоров и интеграторов решений, удастся сформировать устойчивые партнерства по развитию рынка труда.

Данные же модели профессий могли бы лечь в основу отечественной сертификации, предлагаемой Минцифры и призванной заменить сертификаты типа CISSP, CompTIA Security+, CCNA Security и другие. Проект по сертификации в России может способствовать развитию местных специалистов в области информационной безопасности и повысить их уровень квалификации.

Кроме того, необходимо продвижение и вендорских сертификатов, повышение их значимости на рынке труда.

ВЫВОДЫ

1. Общий прирост потребности в специалистах ИБ к 2027 году составит более 100 тыс. человек, и только 86 тыс. из них будет покрыто за счет подготовки и вовлечения новых специалистов.

2. Наиболее важными трендами по масштабам трансформации рынка труда станут облачные технологии (плюс 43 тыс. новых высокотехнологичных рабочих мест, минус 41 тыс. низкотехнологичных); внедрение цифровых валют (плюс 44 тыс. рабочих мест), а также регуляторика и импортозамещение (плюс 30 тыс. рабочих мест).

3. Ликвидация дефицитов на рынке труда, которые будут складываться под действием этих трендов, потребует активной позиции участников рынка по созданию системы сертификации и отраслевых стандартов подготовки и описания профессиональных ролей, развертыванию новых образовательных форматов в вузах и колледжах, а также вовлечению женщин, школьников и людей старшего возраста для замещения дефицитных позиций.

4. Возможно, сектора высшего и среднего профессионального образования отреагируют появлением специализированных образовательных учреждений по аналогии с ситуацией в США и других странах мира, где дефицит рынка труда конца 2000 — начала 2010-х годов привел к системной перестройке системы образования и существенному росту выпуска профильных специалистов.

5. К концу трехлетнего периода занятость на рынке труда должна существенно измениться в своей структуре — стать более технологичной и сформировать большой сегмент архитекторов и инженеров ИБ (почти 100 тыс. востребованных специалистов против 21 тыс. сегодня), способных работать в условиях сложных задач, высокого уровня автоматизации, постоянно меняющегося ландшафта киберугроз.

6. Эти тренды способны спровоцировать не только реорганизацию рынка труда ИБ и профильного сегмента сферы образования, но и повлиять на перестройку смежных рынков. Прежде всего, наработанные в ИБ навыки, компетенции и знания могут получить распространение в других секторах безопасности. Технологии предотвращения телефонного мошенничества могут быть использованы в других видах оперативно-розыскной деятельности, обеспечения государственной безопасности и тому подобного.

ПРИЛОЖЕНИЕ А

Описание прогнозных сценариев, представленных в докладе

Прогнозы количества занятых и потребности в специалистах на 2024–2027 гг. выполнены исходя из влияния ряда трендов, подробно рассмотренных в разделе 3.

Динамичный сценарий характеризуется высокой скоростью проникновения технологических инноваций и автоматизации, жестким контролем за внедрением регуляторных норм и в целом быстрым развитием сегмента новых игроков, включая облачные платформы, аутсорс и цифровые валюты.

Умеренный сценарий предполагает ограниченное, точечное влияние таких технологий, как ИИ и автоматизация, консерватизм рынка в переходе на аутсорсинг и облачные технологии.

В таблицах ниже представлено краткое описание влияния трендов по двум сценариям, с указанием количественного влияния на отдельные функциональные группы на рынке труда.

Тренд	Умеренный сценарий Влияние на функциональные группы, совокупно к 2027 году	Динамичный сценарий Влияние на функциональные группы, совокупно к 2027 году
1 ИИ-трансформация и автоматизация		
Аналитики	Рост спроса на аналитиков с навыками ИИ без значительной автоматизации бизнес-процессов в ИБ станет причиной роста потребности в 6 тыс. человек	Ускоренная автоматизация бизнес-процессов позволит снизить потребность в аналитиках на 6 тыс. человек.
Архитекторы и инженеры	Ожидается умеренный темп разработки и внедрения инструментов автоматизации. Ежегодный рост рынка — около 8%. Увеличение числа рабочих мест составит 7 тыс. человек	В условиях ускоренного развития и внедрения технологий потребность в архитекторах и инженерах возрастет и составит 9 тыс. человек
Аудиторы и консультанты	Развитие технологий и появление новых регуляторных требований, связанных с ними, потребует дополнительно 1 тыс. специалистов	Новые технологии не только станут новой областью компетенций, но и частично автоматизируют труд консультантов. Данные факторы уравняют друг друга
Менеджеры	Деятельность менеджеров будет частично автоматизирована к 2026 году — потребность снизится на 1 тыс. человек.	Частичная автоматизация затронет менеджеров уже в 2024 году — потребность снизится на 4 тыс. человек
Многофункциональные специалисты	Ожидаются умеренные темпы автоматизации, трансформация рабочих мест начнет влиять на рынок в 2025 году. Это позволит снизить потребность в кадрах на 15 тыс. человек	Ускоренные темпы автоматизации и трансформации рабочих мест позволят снизить потребность в кадрах на 26 тыс. человек

Тренд	Умеренный сценарий Влияние на функциональные группы, совокупно к 2027 году	Динамичный сценарий Влияние на функциональные группы, совокупно к 2027 году
2 Облачные технологии		
Аналитики	Число компаний, которым потребуется обеспечение облачной безопасности, вырастет в 2,4 раза, создав дополнительную потребность в 4 тыс. специалистов	Число компаний, которым потребуется обеспечение облачной безопасности, вырастет в 3,4 раза, создав дополнительную потребность в 11 тыс. специалистов
Архитекторы и инженеры	Увеличение числа заказчиков создаст дополнительную потребность в 8 тыс. человек	Увеличение числа заказчиков создаст дополнительную потребность в 28 тыс. человек
Аудиторы и консультанты	Увеличение числа заказчиков создаст дополнительную потребность в 2 тыс. человек	Увеличение числа заказчиков создаст дополнительную потребность в 4 тыс. человек
Многофункциональные специалисты	К 2027 году аутсорсинг не получит массового применения — потребность снизится на 3 тыс. человек	Массовое применение аутсорсинга позволит снизить потребность в кадрах на 41 тыс. специалистов
3 Цифровые валюты		
Аналитики	При способности банковской отрасли обеспечить построение информационной безопасности при внедрении цифровых валют в рамках минимальных прогнозируемых затрат дополнительная потребность в кадрах составит 11 тыс. чел.	В условиях построения информационной безопасности при внедрении цифровых валют в рамках максимально прогнозируемых затрат дополнительная потребность в кадрах составит 25 тыс. чел.
Архитекторы и инженеры	При экономном варианте обеспечения банками безопасности работы с цифровыми валютами дополнительная потребность в кадрах составит 5 тыс. чел.	При более дорогостоящем варианте обеспечения банками безопасности работы с цифровыми валютами дополнительная потребность в кадрах составит 10 тыс. чел.
Аудиторы и консультанты	При экономном варианте обеспечения банками безопасности работы с цифровыми валютами дополнительная потребность в кадрах составит 1 тыс. чел.	При более дорогостоящем варианте обеспечения банками безопасности работы с цифровыми валютами дополнительная потребность в кадрах составит 1 тыс. чел.
Менеджеры	При экономном варианте обеспечения банками безопасности работы с цифровыми валютами дополнительная потребность в кадрах составит 4 тыс. чел.	При более дорогостоящем варианте обеспечения банками безопасности работы с цифровыми валютами дополнительная потребность в кадрах составит 8 тыс. чел.
4 Государственное регулирование и импортозамещение, государственные платформы		
Архитекторы и инженеры	Рост спроса на разработчиков отечественных ИБ-решений в условиях роста рынка разработки и увеличения доли отечественных вендоров составит 19 тыс. человек в обоих сценариях	
Менеджеры	Рост числа менеджеров, связанных с разработкой отечественных ИБ-решений, а также постепенная реализация Указа № 250 с учетом активного повышения квалификации действующих менеджеров сформируют дополнительную потребность в 10 тыс. чел.	Рост числа менеджеров, связанных с разработкой отечественных ИБ-решений, а также активная реализация Указа № 250 сформируют дополнительную потребность в 14 тыс. чел.
Многофункциональные специалисты	Использование госплатформ не позволит в значительной степени сократить потребность в ИБ-специалистах в региональных органах власти, потребность сократится на 1 тыс. чел.	Активное использование госплатформ, нацеленных на централизацию обеспечения информационной безопасности органов власти, позволит снизить потребность в кадрах на 4 тыс. чел.
5 Платформы багбаунти	Ожидаемый рост числа зарегистрированных пользователей на платформах багбаунти составит 4 тыс. человек в обоих рассматриваемых сценариях	

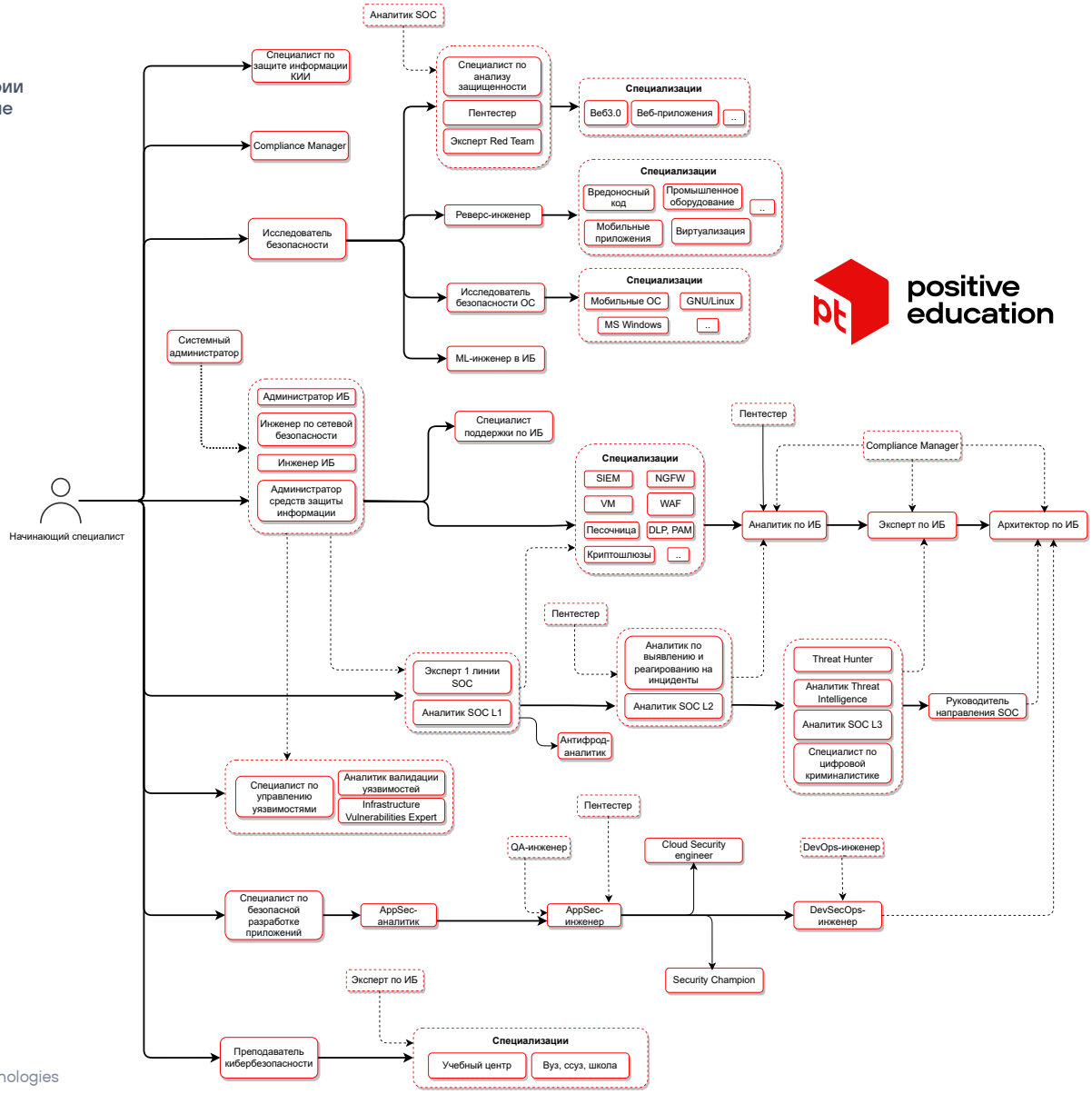
ПРИЛОЖЕНИЕ Б

Методика анализа вакансий и распределения работников на рынке ИБ по функциональным группам

Рынок труда в отчете сегментирован по пяти функциональным группам и составляющим их профессиональным ролям.

Разделение по профессиональным ролям подготовлено Positive Technologies[81] на основе анализа вакансий и накопленных компанией экспертных знаний в сфере информационной безопасности (рисунок 21).

Рисунок 21.
Схема развития карьерной траектории и профессиональные роли в ИБ



Источник: Positive Technologies

Далее профессиональные роли были объединены в функциональные группы на основе методики ОЭСР[82]. Это позволило осуществить сравнение показателей российского рынка с международными рынками труда, на основе чего были составлены прогнозы спроса на специалистов в ИБ по функциональным группам, а также выполнены оценки и прогнозы требуемых компетенций специалистов.

Ниже представлена таблица, поясняющая ролевой состав функциональных групп и методику определения принадлежности вакансий рынка труда к функциональным группам.

Функциональная группа	Ключевые слова	Примеры названия вакансий/должностей	Профессиональные роли, соответствующие группе
Аналитики	• Аналитик • Оператор • Специалист • Эксперт • Проникновение • Тестер • Уязвимость • Тестирование	• Аналитик ИБ • Аналитик безопасности • Аналитик кибербезопасности • Аналитик ИТ-безопасности • Сотрудник по ИБ	• Пентестер (специалист по анализу защищенности) • Исследователь безопасности ОС • Аналитик SOC L1 • Аналитик SOC L2 • Аналитик SOC L3 (аналитик Threat Intelligence) • Аналитик DLP-систем • Вирусный аналитик • Аналитик решений по противодействию мошенничеству (Антифрод) • Специалист по компьютерной криминалистике • Специалист по защите информации • Специалист по криптографической защите информации • и другие
Архитекторы и инженеры	• Инженер • Архитектор • Инжиниринг • Инфраструктура • DevOps	• Инженер по безопасности • Старший инженер по безопасности • Инженер ИБ • Инженер по сетевой безопасности • Архитектор по ИБ • Архитектор облачной безопасности	• Архитектор ИБ • Специалист по безопасной разработке приложений (AppSec, DevSecOps) Специалист по управлению уязвимостями • ML-инженер в кибербезопасности • Реверс-инженер (исследователь безопасности ПО) • Инженер по ИБ • и другие
Аудиторы и консультанты	• Аудитор • Аудит • Консультант • Советник	• ИТ-аудитор • Ведущий ИТ-аудитор • Старший ИТ-аудитор • Консультант по кибербезопасности • Консультант по безопасности • Советник по ИБ	• Методолог по ИБ • Консультант по ИБ • Аудитор по ИБ • Инспектор • и другие
Менеджеры	• Менеджер • Руководитель • Директор • Администратор • Президент • Вице (заместитель) • Лидер • Teamlead • Проект	• Менеджер по ИБ • Менеджер по ИТ-аудиту • Директор по ИБ • Менеджер по ИТ-безопасности • Руководитель по информационной безопасности • Менеджер по безопасности облака AWS/Azure	• Директор / заместитель директора по ИБ • Руководитель ИБ • и другие
Многофункциональные специалисты	• Техник • Мастер • Спикер • Преподаватель	• Техник • Верификатор данных • Техник группы информационных технологий, связи и защиты информации	• Техник • Специалист по ИБ (без конкретизации) • Тренер в учебном центре (преподаватель по изучению продуктов ИБ) • и другие

С помощью представленной выше методики распределения специалистов на основании описания вакансий была проанализирована выборка вакансий, представленная в аналитической базе «РосНавык»[83]. Данные «РосНавыка» основаны на базе данных HeadHunter, SuperJob, «Работа России» и «Работа.ру».

В общую выборку, охватывающую период с марта 2023 по март 2024, были включены вакансии, отнесенные «РосНавыком» к специальности «Специалист по информационной безопасности». Определение специальности осуществлялось аналитическими средствами «РосНавыка» на основе нейросетевого анализа баз данных вакансий, определения требуемых навыков и их группировки. Количество вакансий в проанализированной базе данных за указанный период составило 25 418 человек.

К многофункциональным специалистам были отнесены вакансии, не вошедшие в другие функциональные группы. Связано это с тем, что в результате анализа было выявлено, что к данной категории относятся в первую очередь специалисты, не имеющие четкой функциональной роли, к которым предъявляются широкие требования в сфере ИБ; от них часто не требуется высокая квалификация. В соответствии с классификацией ОЭСР данная группа относилась бы к «прочим».

Кроме разделения на функциональные группы, в рамках указанных групп был осуществлен анализ компетенций, востребованных специалистами каждой из групп.

В целом, ключевыми компетенциями для ИБ-специалистов в текущий момент являются знание и администрирование Unix-систем и подобных, знание и администрирование ОС Windows, знание и навыки разработки проектов на различных языках (Python, Bash, Powershell, javascript, PHP, C, C++ и других), а также знание законодательных актов РФ, нормативных и методических документов регуляторов, регламентирующих процесс обеспечения безопасности информации.

При этом стоит отметить, что администрирование ОС Linux встречается в требованиях чаще, чем ОС Windows, а Python или Bash встречаются чаще остальных скриптовых языков.

При этом к каждой конкретной специальности предъявляются уникальные требования. Тем не менее, обобщив, можно отметить, что для потенциальных архитекторов и инженеров, помимо навыков администрирования ОС и знания законодательства, важно знание одного или нескольких скриптовых языков, знание и администрирование систем класса SIEM и других, знание и понимание принципов атак.

Для консультантов и аудиторов важно знание российских и международных стандартов для оценки степени опасности уязвимостей, знание основ архитектуры СЗИ, понимание технологий обеспечения сетевой безопасности и умение работать с СЗИ.

Для аналитиков в сфере ИБ, помимо таких базовых компетенций, как знание и навык администрирования ОС и знание скриптовых языков, также важно знание и администрирование систем на платформах класса IRP/SOAR, знание и прогнозирование основных типов уязвимостей и атак, знание и применение инструментов автоматизированного поиска и анализа уязвимостей, знание и понимание работы сетевой инфраструктуры, базовые знания АСУТП, навык анализа бизнес-процессов.

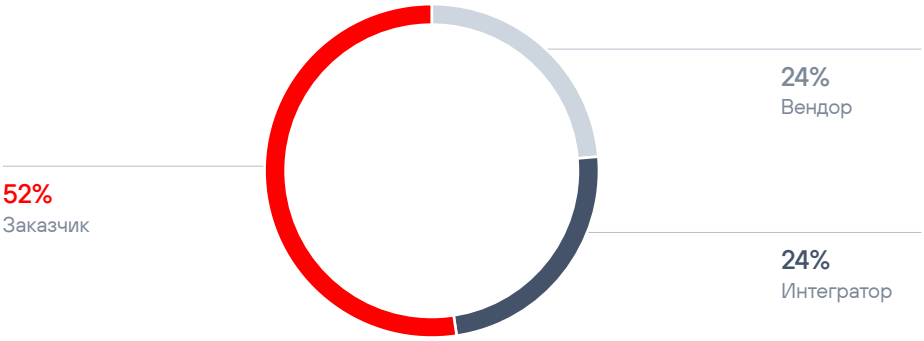
ПРИЛОЖЕНИЕ В

Отраслевое распределение спроса на рынке труда информационной безопасности

Условно можно провести разделение компаний на рынке на вендоров (специализированные компании, производящие собственные решения и ПО в области ИБ, а также предоставляющие сервисное обслуживание), интеграторов (компании-подрядчики, специализирующиеся на объединении различных решений и представлении услуг в области ИТ, и ИБ в частности) и клиентов (организации, закупающие ИБ-решения и ИБ-услуги, обеспечивающие собственную безопасность или безопасность своих клиентов).

Учитывая данное разделение, можно выделить следующую структуру спроса: 52% вакансий приходится на заказчиков, по 24% приходится на вендоров и интеграторов (рисунок 22).

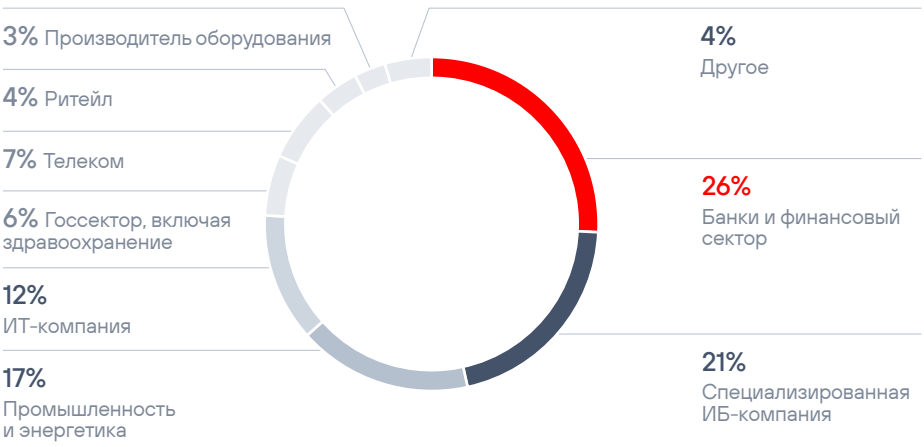
Рисунок 22. Распределение вакансий в области ИБ по типу игроков (ТОП-100 компаний по числу размещенных вакансий, март 2023 — март 2024 гг.)



Источник: ЦСР «Северо-Запад», по данным «РосНавыка»

Рассматривая структуру спроса с точки зрения распределения по отраслям, стоит отметить, что основная доля вакансий приходится на финансовый сектор — 26%. Доля же вакансий специализированных ИБ-компаний составляет лишь 21%. ИТ-компании занимают 4-е место — на их вакансии приходится 12% (рисунок 23).

Рисунок 23. Распределение топ-200 нанимателей в ИБ в России по секторам деятельности с марта 2023 г. по март 2024 г., % вакансий сегмента от общего числа вакансий, опубликованных топ-200 нанимателей



Источник: ЦСР «Северо-Запад», по данным «РосНавыка»

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Building a Skilled Cyber Security Workforce in Five Countries, OECD, 2023

2 Исследование: дефицит специалистов в области кибербезопасности снизился на 5% в 2020 году, CNews, 2020

3 Axenix открыла офис в Краснодаре, CNews, 2023

4 Эксперт назвал главную причину дефицита кадров в России, Газета.ру, 2023

5 Крупнейшие ИТ-компании начинают возвращать топовых специалистов в Россию. Эмиграция сходит на нет

6 Кадры проявили сверхтекучесть, «КоммерсантЪ», 2024

7 Об образовании специалистов информационной безопасности в Российской Федерации», 2024

8 В России к критической инфраструктуре допустят ИБ-специалистов без высшего образования, 2023

9 Сертификации ИБ-специалиста: Россия и международный рынок, Security Media, 2023

10 Зарплаты IT-специалистов во второй половине 2023, Хабр Карьера, 2024

11 Бороться с хакерами и много зарабатывать: зачем молодежь идет в кибербезопасность, Jetinfo, 2024

12 Не становитесь безопасниками, Skillfactory, Хабр

13 Каждый пятый россиянин признался в желании стать хакером, РБК, 2023

14 Building a Skilled Cyber Security Workforce in Five Countries, OECD, 2023

15 Российский и глобальный рынки ИБ разошлись в приоритетах, CNews, 2023

16 GenAI for cyber defence is on the rise, PwC, 2024

17 Generative AI and Cybersecurity: Strengthening Both Defenses and Threats, Bain, 2023

18 Gartner Unveils Top Eight Cybersecurity Predictions for 2024, Gartner, 2024

19 Randomized Controlled Trial for Copilot for Security, 2024

20 Спрос на ИБ-специалистов, умеющих работать с искусственным интеллектом вырос на 30%, 2024

21 The C-suite playbook: Putting security at the epicenter of innovation, 2024

22 ISC2 Cybersecurity Workforce Study, 2023

23 Облачная зрелость российского бизнеса, Технологии доверия и Cloud, 2022

24 Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 гг., Банк России, 2023

25 Безопасность в облаках и не только: исследование-прогноз для CISO на 2024 год, Яндекс и ДРТ, 2024

26 Платформы Cloud. Обзор подходов и средств безопасности, Cloud

27 Definition of a Cloud Security Engineer, Teal

28 Сервисы ИБ-аутсорсинга в России вырастут быстрее рынка, 2023

29 Кому достанутся цифровые рубли?, Яков и Партнеры, 2024

30 Екатерина Кваша: «Российские вендоры занимают 70% рынка ИБ», ЦСР, 2023

31 Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

32 Единая цифровая платформа РФ «ГосТех»: предпосылки создания, мировой опыт, ключевые преимущества, стратегические цели, Рахманов В. В.

33 Евгений Жмурин, НИИ «Интеграл»: Обеспечивать безопасность ГосТех будет единый Центр кибербезопасности

34 Прокуратурой округа в действиях ПАО «Юг-Инвестбанк» выявлены нарушения законодательства о безопасности критической информационной инфраструктуры

35 Practical quantum computing is coming in 3 to 5 years, but will be cloud based, NSA official predicts, 2024

36 Из выступления Жиляева Андрея, старшего исследователя ЦНИПР ИнфоТеКС, к. т. н., «Квантовое распределение ключей», 2023

37 The Biden White House Gets Quantum Right — At Last, 2022

38 Эксперты СБ РФ предложили развивать квантовые технологии в кибербезопасности, 2023

39 Why organizations should prepare for quantum computing cybersecurity now, Ernst&Young, 2023

40 Отчет об образовании специалистов по ИБ в Российской Федерации, НТИ «Энерджинет», 2024

41 Дефицит кадров в сфере ИБ и подготовка молодых специалистов, Information Security, 2019

42 Блеск и нищета ИБ-образования. Россыпь проблем глазами преподавателя вуза, BIS Journal, 2022

43 Блеск и нищета ИБ-образования. Россыпь проблем глазами преподавателя вуза, BIS Journal, 2022

44 О необходимости новой методологии информационной безопасности, Блог Атаманова Г. А., 2023

45 «Лаборатория Касперского» представляет масштабную международную программу сотрудничества с вузами, 2023

46 Сайт проекта «Профессионалитет»

47 Цифровой суверенитет: как вузы госпрограммы «Приоритет 2030» обеспечивают кибербезопасность

48 Передовые инженерные школы, Минобрнауки

49 Сотрудничество с учебными заведениями, ОКБ «САПР»

50 В 2023 году спрос на базовые курсы по программированию упал. В тренде — 1С, кибербезопасность и нейросети, 2024

51 Сайт программы «Информационная безопасность» Skillfactory, МИФИ и Positive Technologies

52 Перечень организаций, осуществляющих образовательную деятельность в ИБ, ФСТЭК России, 2024

53 Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

54 Постановление Правительства РФ от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»

55 ФСТЭК России: ДПО оказывает существенную поддержку в формировании кадров, BIS Journal, 2024

56 Дмитрий Чернышенко: до конца 2025 года «Цифровые кафедры» выпустят свыше 385 тысяч человек, 2023

57 Информационная безопасность, IT-академия ТУСУР

58 Информационная безопасность в АПК, ФГБОУ ВО РГАУ — МСХА имени К. А. Тимирязева

59 Компьютерные сети, ФГБОУ ВО КНИТУ

60 Проект «Цифровая кафедра», НИУ МИЭТ

61 ISC2 Cybersecurity Workforce Study, 2023

62 Some People Learn to Code in Their 60s, 70s or 80s, New York Times, 2017

63 Some People Learn to Code in Their 60s, 70s or 80s, New York Times, 2017

64 Женская доля: топ-5 крутых взлетов девушек в ИБ, 2022

65 Women in Cybersecurity Report, 2023

66 Живущая в сети: как женщины строят карьеру в кибербезопасности, Forbes, 2021

67 SANS Women's Immersion Academy, SANS Institute

68 Girls4Tech

69 Что такое «Женсовет по ИБ»?, Information Security, 2024

70 Is AGI Possible?, 2023

71 Scenario planning for an A(G)I future, IMF F&D, 2023

72 Прогноз развития рынка кибербезопасности в Российской Федерации на 2023–2027 годы, ЦСР, 2023

73 Экспорт ИБ-продуктов из России имеет шанс удвоиться, 2023

74 Сайт проекта «Профессионалитет»

75 Отчет об образовании специалистов по ИБ в Российской Федерации, НТИ «Энерджинет», 2024

76 Что такое ИТ-класс

77 Хакерам укажут альтернативный путь, 2024

78 Рынок труда во втором квартале 2023 года. Спрос растет, но ИБ-специалисты по-прежнему в дефиците

79 Students are the next target for co-working spaces. Campuses are taking note, 2021

80 Официальный сайт Альянса в сфере ИИ

81 Карьера в кибербезопасности, или Как расти в ИБ, Хабр, 2024

82 Building a Skilled Cyber Security Workforce in Five Countries, OECD, 2023

83 РосНавык