ДЫРА В ЗАЩИТЕ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОСТАЕТСЯ ОДНИМ ИЗ СЕГМЕНТОВ, ГДЕ СПРОС НА СПЕЦИАЛИСТОВ ПРОДОЛЖАЕТ РАСТИ, НЕСМОТРЯ НА ОБЩЕЕ ОХЛАЖДЕНИЕ РЫНКА ТРУДА В ИТ В 2026 ГОДУ. НА СЕВЕРО-ЗАПАДЕ ПРОБЛЕМУ ОБОСТРЯЕТ КОНКУРЕНЦИЯ С ФЕДЕРАЛЬНЫМИ РАБОТОДАТЕЛЯМИ И КОНЦЕНТРАЦИЯ КРУПНОГО БИЗНЕСА. ЛЮБОВЬ ВИКТОРОВА

Потребность в специалистах по информационной безопасности (ИБ) испытывают 80% организаций, а полностью укомплектовали штат только 11%, показало исследование «Инфосистемы Джет». За три года доля компаний, которым не хватает более 10 специалистов, выросла с 17 до 32%.

Количество вакансий в информационной безопасности в первом квартале 2026 года увеличилось на 24% год к году на фоне общего снижения ИТ-найма на 18%, сообщает SuperJob. Бизнес ищет сотрудников, способных не только поддерживать средства защиты, но и расследовать инциденты, работать со сложной инфраструктурой и быстро реагировать на новые типы атак.

«Специалистов среднего уровня и выше на рынке не так много, и их хорошо удерживают текущие работодатели»,— говорит старший консультант Selecty Владимир Трегубов. По его словам, специалистов начального уровня компании, напротив, нанимают неохотно из-за нехватки у кандидатов необходимых компетенций.

При этом проблема постепенно меняет характер. Сегодня это не просто нехватка людей, а дефицит нужной экспертизы и практического опыта, объясняет руководитель образовательных программ Positive Technologies Анастасия Федорова. По данным компании, только около 14% вакансий рассчитаны на начинающих специалистов, тогда как 47% предполагают опыт работы от одного до трех лет, еще 35% — от трех до шести лет. При этом система высшего и среднего профессионального образования обеспечивает приток порядка 8–10 тыс. специалистов ежегодно.

ОТ ДИПЛОМА К ПРАКТИКЕ

Одной из основных причин дефицита эксперты называют разрыв между образовательной программой и реальными задачами бизнеса. Выпускник может иметь профильную специальность, но работодателю требуется сотрудник, который уже умеет работать с современной инфраструктурой, облачными решениями, промышленными сетями, отечественными средствами защиты и расследованием инцидентов.

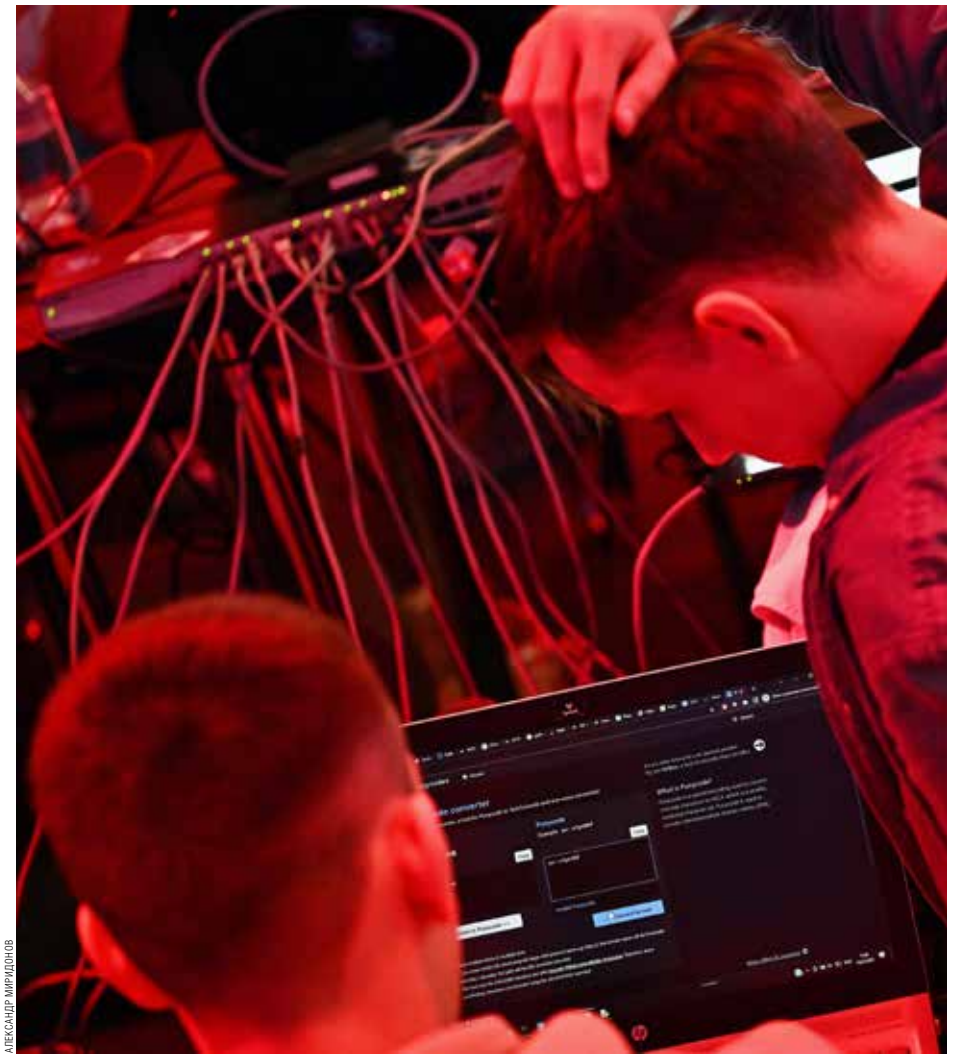
«Вузы выпускают кадры, которые приходится растить еще два-три года, а спрос заметно сместился к уровню middle и senior, поскольку растет и количество инцидентов, и интенсивность атак»,— говорит генеральный директор компании «САЙБЕР Бизнес Консалтинг» Дмитрий Лившин.

По словам эксперта по ИТ-консалтингу Дениса Еремеева, рынку нужны специалисты, которые одновременно понимают современную инфраструктуру, облачные решения и промышленные сети и умеют проводить расследование до корневой причины инцидента.

На Северо-Западе ситуация похожая, но здесь добавляется региональная конкуренция. Управляющий партнер Atsearch group Елена Морозова отмечает, что при сжатии ИТ-рынка выпускники и middle-специалисты уезжают в Москву, либо переходят на удаленную работу в федеральные компании. Местные работодатели в результате остаются без кандидатов. По ее оценке, опытных руководителей ИБ на рынке всего несколько сотен, причем почти все они уже трудоустроены.

Одновременно Петербург остается одним из крупных центров спроса на такие кадры. На город приходится около 9% вакансий в сфере ИБ против 42% в Москве, говорит Денис Еремеев со ссылкой на hh.ru.

Особенность Северо-Запада заключается и в структуре экономики. Здесь сосредоточены промышленные предприятия, транспортная и портовая инфраструктура, энергетика и финансовый сектор. Многие из этих компаний одновременно активно цифровизируются и становятся объектами атак, что усиливает потребность в квалифицированных специалистах, считает ментор стартап-акселератора Alchemist Accelerator Алексей Овсянников.



АЛЕКСАНДР МИРИДОНОВ

СИТУАЦИЯ НА РЫНКЕ В 2026 ГОДУ ХАРАКТЕРИЗУЕТСЯ НЕХВАТКОЙ ПРОФИЛЬНЫХ СПЕЦИАЛИСТОВ И ОТТОКОМ ПРОФЕССИОНАЛОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В финансовом секторе потребность ощущается острее всего, говорит директор процессинга Payzon Рустам Багаутдинов. Защита платежного шлюза или администрирование аппаратных модулей безопасности требуют редкой междисциплинарной экспертизы — инженер должен одновременно понимать архитектуру платежного ядра и векторы сложных кибератак.

ДЕФИЦИТ ПРЕВРАЩАЕТСЯ В РИСК

Для многих компаний кадровая проблема в ИБ выходит далеко за пределы HR. Если вакансия долго остается незакрытой, нагрузка перераспределяется между действующими сотрудниками, а вместе с ней растет вероятность ошибок и задержек при реагировании на инциденты.

«Возникают задержки в анализе инцидентов, ошибки настройки, сокращается профилактическая работа. Бизнес сильно рискует, когда подозрительная активность долго остается незамеченной»,— говорит ведущий аналитик «СерчИнформ» Андрей Головин.

По словам директора департамента информационной безопасности BPMSoft Дмитрия Цыганова, дефицит особенно заметен среди специалистов с высокой квалификацией и практическим опытом. После 2022 года, когда число и сложность атак выросли, ситуация дополнительно обострилась: на рынке встречаются случаи перехода между компаниями целых команд.

Для бизнеса это означает увеличение времени реакции на инциденты, рост стоимости ИБ и вероятность того, что уязвимость будет обнаружена слишком поздно, добавляет господин Цыганов. Последствиями могут стать утечки данных, простой систем и финансовые потери.

Есть и менее очевидный риск — перегрузка самих специалистов. По словам господина Еремеева, сотрудники устают от однотипных событий, отчетности и контроля требований и в результате могут уходить в архитектуру, инфраструктуру, разработку или консалтинг.

«ИБ из „поддерживающей функции“ превратилась в „функцию обеспечения непрерывности бизнеса“»,— говорит директор по персоналу BPMSoft Марина Максимова. Нехватка экспертизы, по ее словам, в конечно итоге способна замедлять запуск цифровых проектов.

ВЫРАСТИТЬ САМИМ

Быстро решить проблему за счет найма готовых специалистов рынок не может, поэтому компании делают ставку на внутреннее обучение и переход сотрудников из смежных ИТ-профессий. По данным «СерчИнформ», в СЗФО 56% компаний переобучают собственных сотрудников, 36% нанимают готовых специалистов, 19% привлекают подрядчиков или SOC (центр оперативного управления ИБ), а 17% работают со студентами и выпускниками.

«Администраторы и разработчики заходят в ИБ быстрее всего: они уже понимают инфраструктуру и код»,— говорит господин Лившин. Он предлагает плотнее связывать вузы с индустрией, чтобы выпускники приходили к работодателю с актуальным стеком, а не только с теоретическими знаниями.

Елена Морозова также считает перспективным переобучение системных администраторов и разработчиков. Компаниям, по ее словам, стоит расширять географию поиска и открывать позиции на регион, а работу с вузами начинать за два-три года до выпуска.

Марина Ларченкова, HR бизнес-партнер Compliance Control, считает одним из наиболее эффективных способов формирования кадрового резерва системную работу с выпускниками профильных вузов: организация стажировок, отбор наиболее перспективных специалистов и их дальнейшее развитие внутри компании. Господин Овсянников предлагает дополнять такую работу киберполигонами и внутренними программами подготовки.

При этом некоторым компаниям проще передать часть функций внешнему подрядчику. Это особенно актуально для малого и среднего бизнеса, который не всегда может конкурировать с крупными работодателями по зарплатам. По данным «СерчИнформ», 19% компаний в СЗФО уже привлекают подрядчиков или SOC.

ИИ В РУТИНЕ

Еще одним способом компенсировать дефицит становится ИИ. Пока речь не идет о замене специалистов, а о передаче машине повторяющихся операций. Как отмечают опрошенные эксперты, ИИ уже используется для первичного анализа событий, корреляции логов, сортировки и приоритизации алертов, поиска аномалий, выявления фишинга и подготовки аналитических сводок. В SOC это позволяет разгрузить первую линию и направить специалистов на расследование более сложных инцидентов.

«ИИ демонстрирует успехи в проактивном поиске угроз, построении графов атак, автоматическом анализе кода на уязвимости и адаптивном управлении доступом на основе анализа поведения пользователей. Главный эффект — повышение производительности существующих сотрудников»,— комментирует генеральный директор ИТ-компании УЦСБ Валентин Богданов.

И все-таки пока доверие к технологии остается ограниченным. По данным «СерчИнформ», в 2026 году 76% опрошенных российских ИБ-специалистов доверяют ИИ, но с осторожностью, 19% относятся к результатам скептически, а 5% не готовы доверять.

Кроме того, сам ИИ становится источником новых угроз. Господин Цыганов отмечает, что злоумышленники используют его для автоматизации поиска уязвимостей, персонализации фишинга, создания дипфейков и клонирования голоса. В результате атакующие могут увеличивать масштаб и скорость атак.

Поэтому внедрение ИИ само по себе не решает кадровый вопрос. Более того, появляются новые специальности и компетенции. Positive Technologies оценивает, что автоматизация с помощью ИИ может оптимизировать к 2027 году до 27 тыс. рабочих мест, однако одновременно будет расти спрос на специалистов по безопасности самих ИИ-систем, в том числе на специалистов направления MLSecOps (кибербезопасность и машинное обучение). ■