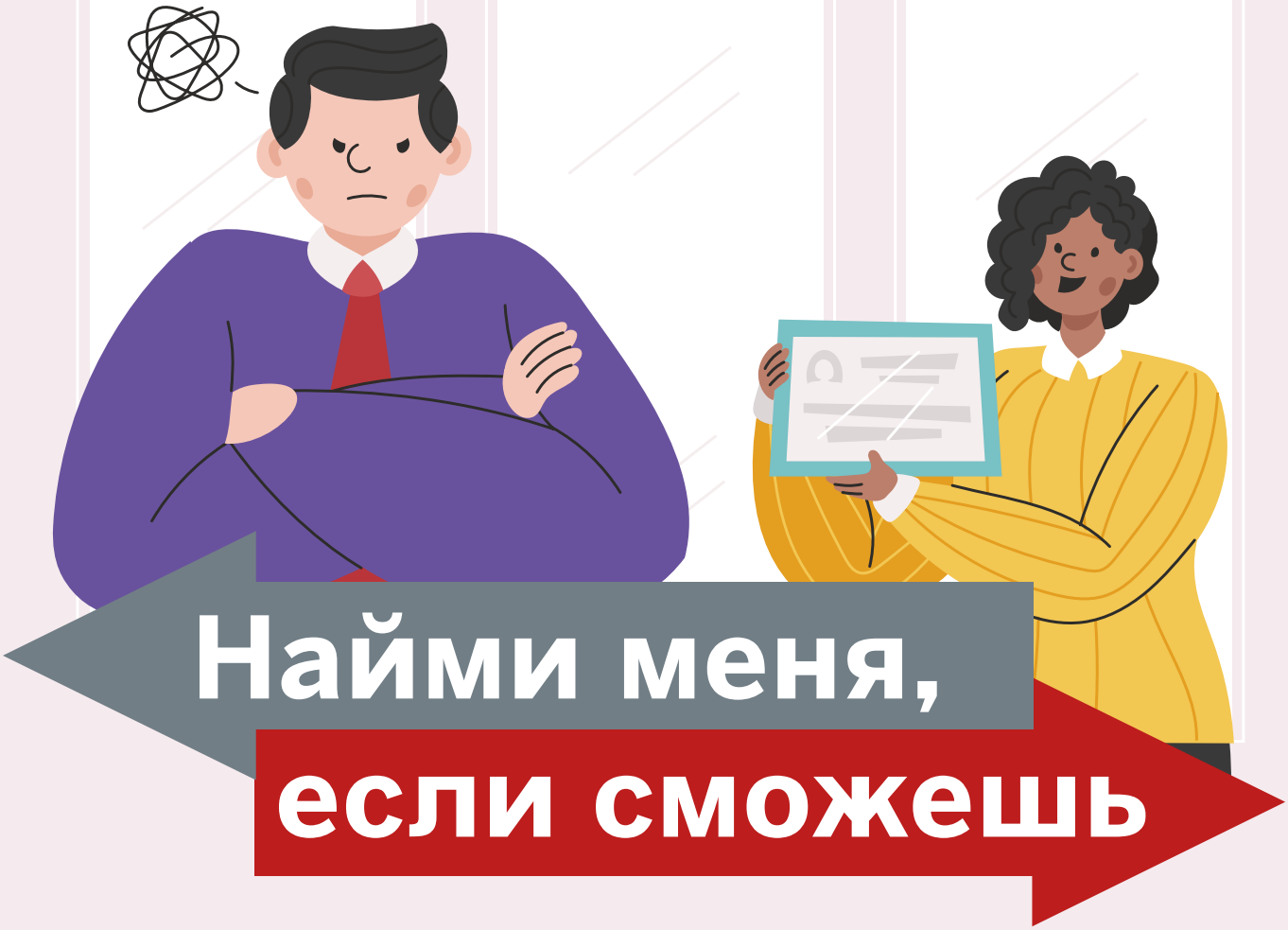


Найми меня, если сможешь

Для противостояния киберугрозам в России не хватает примерно 50 тыс. специалистов по информационной безопасности. Предлагаем присмотреться к явлению — найти его причины, уточнить, в каких ИБ-специалистах есть потребность и глазами экспертов взглянуть на готовность вузовских выпускников

Текст
АЛЕКСАНДРА КРЫЛОВА,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

Спусковые крючки дефицита ИБ-кадров

Об остроте проблемы, как отметил **Дмитрий Кузеванов,** директор по информационной безопасности, руководитель Центра мониторинга и реагирования UserGate, свидетельствует тот факт, что для ее решения участники рынка либо растят ИБ-специалиста из выпускника вуза «с нуля», либо переманивают опытных сотрудников у конкурентов.

Есть мнение, что специалистов по ИБ в России не хватало всегда и что за последнее время ситуация не изменилась ни в худшую, ни в лучшую сторону. «Возможно, это связано с особенностями системы образования», — полагает **Павел Луцик,** директор по развитию бизнеса и работе с партнерами компании «КриптоПро».

Но так думают далеко не все участники рынка, и их мнение подтверждается практикой. Например, по словам **Дмитрия Слободенюка,** коммерческого директора компании ARinteg, в последнее время срок поиска увеличился, на закрытие одной вакансии кадровой службе требуется два-три месяца.

Росту спроса на специалистов в сфере информационной безопасности способствуют несколько факторов. Самый понятный из них — кратный рост числа кибератак, с которым большинство российских компаний сталкивается с начала весны 2022 года. «С учетом постоянно изменяющихся векторов атак нужны специалисты в сфере информационной безопасности, которые будут вырабатывать новые способы защиты», — отметил **Михаил Хлебунов,** директор по продуктам компании Servicepipe. А поскольку киберугрозы эволюционируют стремительно, образовательные организации не успевают переориентировать подготовку специалистов, отмечает **Ольга Петрусевич,** HR бизнес-партнер компании Infosecurity. Как следствие на рынке возникает дефицит специалистов по всем ключевым направлениям ИБ.

Еще один фактор, способствующий нехватке ИБ-специалистов, — активно развивающееся в этой области законодательство, добавляющее сотрудникам служб информационной безопасности новые за-

дачи. «Это ведет к расту нагрузки на экспертов в сфере ИБ, а значит, возникает необходимость расширять штат», — констатировала **Алена Игнатьева,** руководитель направления консалтинга и аудита компании STEP LOGIC.

Обеспечение поступления в штат новых квалифицированных работников по направлению информационной безопасности и защиты от киберугроз в финансовом секторе традиционно является одной из важнейших задач. Кадров, к сожалению, не хватает, — заметил **Алексей Плешков,** заместитель начальника департамента защиты информации Газпромбанка. Он убежден, что это происходит из-за востребованности специалистов данного профиля практически во всех отраслях экономики. Интерес к этому вопросу существенно повысился с мая 2022 года, после выхода Указа Президента РФ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». «Эта дата стала переломным моментом», — отметил Алексей Плешков.

Несмотря на доступность для служб информационной безопасности современных средств автоматизации, к примеру технологии RPA, для решения многих задач в этих подразделениях «нужны руки». По словам **Евгения Баклушина,** заместителя директора Аналитического центра УЦСБ, для решения многих задач уже существует понятный алгоритм, но у специалистов просто не хватает времени.

С нехваткой кадров сегодня сталкиваются даже компании, специализация которых — аутсорсинг услуг в сфере ИБ. **Евгений Царев,** управляющий RMT Group, назвал дефицит кадров одной из самых больших проблем. «Мы наблюдаем дефицит специалистов у всех без исключения заказчиков», — заявляет он.

«Аутсорсинг ИБ достаточно востребован сегодня, и это происходит как раз потому, что компании (как крупные, так и малые и средние) ощущают острую нехватку специалистов разных направлений и разного уровня, но особенно middle и senior, — согласился с коллегой **Олег Кочетков,** генеральный директор и совладелец провайдера по информационной безопасности Simplity.

Кто в ИБ нужнее?

Отрасль информационной безопасности комплексная, объединяет множество направлений, и штат каждого из них должен быть полностью укомплектован. «Нельзя уверенно говорить, что одно из направлений более важное, чем другое, — заметил **Евгений Баклушин,** заместитель директора Аналитического центра УЦСБ. — Если сконцентрируешься на одном, хакеры могут воспользоваться другим».

В ответ на вопрос «ИБ-специалистов какого профиля вам сегодня не хватает?» эксперты назвали такие направления, как мониторинг информационной безопасности (реагирование и расследование инцидентов), управление уязвимостями, тестирование на проникновение, сетевая безопасность, риск-менеджмент.

«Стоит понимать, что на рынке не хватает специалистов на все позиции. Острее всего ощущается нехватка инженеров по информационной безопасности, архитекторов систем ИБ и архитекторов SOC, пентестеров, аналитиков второй и третьей линий SOC. Глобально существует дефицит мидл- и сеньор-специалистов разных профессий, и, к сожалению, пока тенденция такова, что нехватка кадров будет увеличиваться», — констатировала **Наталия Чумаченко,** HR-директор компании «Информзащита».

К этому списку представители банковского сообщества добавили менеджеров в области информационной безопасности. «Самая большая проблема заключается в том, что на рынке огромный дефицит грамотных и подготовленных руководителей (как технических, так и административных), способных оценить текущее состояние ИБ в организвции, спланировать модернизацию и развитие процессов, организовать деятельность по обеспечению ИБ в компании», — отметил **Алексей Ахмеев,** начальник управления информационной безопасности компании «Свой банк» (группа IDF Eurasia). По его словам, сегодня банкам нужны руководители, знающие, как грамотно расставить приоритеты, найти баланс между требованиями бизнеса и угрозами для бизнеса, обеспечить оптимальную защиту.

«Особо в контексте приближающегося 2025 года хотелось бы отметить востребованность проектных менеджеров по ИБ, способных организовать и руководить работой по поэтапному импортозамещению СЗИ», — добавил Алексей Плешков. Эксперт обратил внимание на два подхода к обеспечению информационной безопасности в банках: универсальный, при котором подбираются специалисты по ИБ с широким набором академических и практических компетенций, и специализированный, при котором в службу нанимаются узкопрофильные сотрудники. Выбор подхода зависит от масштабов бизнеса финансовой организации и уровня зрелости системы обеспечения информационной безопасности в компании.

А вот компаниям, работающим в сфере ИБ, только специализации сотрудника недостаточно, отметила Ольга Петрусевич. Им приходится адаптировать своих сотрудников к динамично меняющемуся ландшафту угроз. Так что в этой сфере ценится не только глубокий опыт, но и готовность к постоянному обучению и освоению новых инструментов.

Кто больше для службы ИБ ценен?

Знание о том, что рынку информационной безопасности нужны кадры, вдохновляет людей на переобучение, но зачастую найти работу по новой профессии непросто. СМИ регулярно объявляют, что специалисты начального уровня и без опыта работы не очень интересны работодателям.

С молодыми специалистами работать непросто, поскольку, по большому счету, у них не было возможности применить на практике полученные знания, умения и навыки. «Мы замечаем большое количество начинающих специалистов, которые в поисках первой работы не успевают углубиться в специфику на долгое время, и как следствие возникает несоответствие уровня знаний и ожидаемой заработной платы, — констатировала **Анастасия Семушкина,** руководитель рекрутинга компании «Бастион».

Однако, поскольку свободных ИБ-сотрудников с опытом самостоятельной деятельности, хорошо знающих специфику отрасли информационной безопасности, на рынке труда совсем немного, для решения отдельных задач в сфере информационной безопасности привлекаются даже учащиеся техникумов и студенты. «Мы пред-

почитаем нанимать начинающих специалистов, для того чтобы иметь возможность погрузить их в специфику работы в компании без противоречия с имеющимся опытом. При этом мы создаем хорошие возможности для роста и развития внутри компании», — поделился опытом Павел Луцик. Такая практика, считает Евгений Баклушин, дает очень хорошие результаты. «При грамотно спланированном погружении молодого специалиста в профессию через один-два года он уже может достичь уровня мидл. Наш мир очень быстрый», — пояснил он.

Немного иного подхода к найму придерживаются в компании Simplity. «Мы предпочитаем быть вторым работодателем, соответственно к нам попадают ребята junior-plus, — рассказал Олег Кочетков. — Сотрудники учатся друг и друга и растут, но для выполнения текущих задач нужны специалисты уровней middle, middle-plus и plus-plus senior. Именно последние могут полностью и без ошибок выполнить средний проект целиком, если говорить о пентесте, или закрыть крупный проект в группе специалистов».

Методы взращивания специалистов среднего и высокого уровней компетенции известны: наставничество и стажировки, которые хорошо комбинируются. Так, в команде, которая занимается развитием экосистемы НОТА-КУПОЛ (холдинг Т1), есть высококлассные специалисты, которые курируют и обучают молодых коллег. «Кроме того, в рамках холдинга Т1 мы запустили стажерскую программу по направлению информационной безопасности, где проводится обучение молодых специалистов, в том числе на практических кейсах. По результатам стажерской программы лучшие участники пополняют команду НОТА КУПОЛ», — рассказала **Мария Зализняк,** директор департамента развития продуктов этой экосистемы продуктов и услуг в сфере ИБ.

Компания «Информзащита» тоже проводит стажировку молодых специалистов и приглашает лучших выпускников в штат, отметила Наталья Чумаченко.

Похожие программы действуют в «Группе Астра», которая, по словам ее директора по персоналу **Марины Яловеги,** активно набирает молодых специалистов. «На стажировке они стремятся получить новые знания и развить свои технические навыки, применяют имеющиеся hard skills на практике, что помогает им лучше понять предмет и перейти от теории к реальным задачам», — отметила она и добавила, что в командной работе важно сохранить баланс между молодыми и опытными сотрудниками.

Чему не учатся в вузах?

Российские вузы, как столичные, так и региональные, в целом, обеспечивают высокий уровень знаний выпускников по направлениям информационной безопасности. В компаниях — участницах рынка активно нанимают выпускников вузов, особенно тех, кто сумел попасть к ним на стажировку и хорошо себя зарекомендовать. Это выпускники МИРЭА, МИФИ, МГТУ им. Баумана, МЭИ, МФТИ, ВШЭ, МГУПИ и некоторых других высших учебных заведений.

Особенно часто эксперты называют РТУ МИРЭА, студенты которого имеют возможность совмещать учебу с работой. Они используют эту возможность для приобретения практических навыков и, если процесс им нравится, рекомендуют компанию своим однокурсникам.

Впрочем, как считает Дмитрий Кузеванов, название вуза и его позиция в рейтинге особого значения не имеют. Главное — это желание конкретного молодого человека развиваться. «Как правило, именно такие специалисты имеют высокий уровень подготовки, быстро включаются в работу и растут в профессиональном плане», — подчеркнул эксперт.

С тем, что мотивация молодых специалистов должна носить персонализированный характер, согласен и Алексей Ахмеев. «Необходимо общаться, чувствовать, понимать каждого человека индивидуально. У молодых специалистов есть много скрытых интересов, культивируя которые можно получить очень ответственного и сильного эксперта», — утверждает он.

Информационная безопасность — сфера, подверженная изменениям и быстро развивающаяся. Помимо специальных теоретических знаний от молодых специалистов, которые хотят расти в ней, требуются компетенции в смежных отраслях знаний, таких как информационные технологии, в частности языки программирования. А с этим, как ни странно, у выпускников вузов есть проблемы. Так, технические специалисты «Группы Астра», довольно высоко оценивающие знание студентами теории в рамках курсов «Компьютерная безопасность» и «Безопасность автоматизированных систем», отмечают недостаток базовых знаний ОС, компьютерных систем, навыков разработки на языках типа C/C++, GoLang. В большинстве случаев отсутствует умение самостоятельно вести проекты, исследования.

На нехватку у молодых специалистов практики прикладной разработки на языках C/C++ и Assembler указал и Павел Луцик. Ликвидировать пробелы поможет посещение курсов, но для этого нужна мотивация.

Довольно тревожным знаком в условиях, когда безопасная разработка становится де-фактом стандартом, является недостаток знаний в области фаззинг-тестирования и экспертизы кода. А это один из видов динамического тестирования, который является неотъемлемой частью безопасной разработки, привела мнение технических специалистов «Группы Астра» Марина Яловега.

Помимо практических навыков у выпускников ведущих технических вузов эксперты отмечают недостатки других очень важных в сфере информационной безопасности навыков, многие из которых должны быть сформированы до выхода на первую работу. Это, например, отсутствие системного и комплексного подхода к рабочим задачам, неумение коммуницировать.

Также, по словам **Андрея Попова,** руководителя отдела аналитики и аудита ИБ в компании SecWare, у будущих «безопасников» есть проблемы с чтением технической документации. А Олег Кочетков сталкивался с выпускниками вузов, не имеющими навыка самостоятельно «нагуглить» решение.

Словом, опытным сотрудникам служб информационной безопасности и сеньорам в компаниях, работающих на этом рынке, приходится выделять силы и время на заполнение пробелов в образовании выпускников вузов, а также на повышение их мотивации постоянно получать новые знания в профессиональной области. Б.О