Кадровый авитаминоз

Ситуация в сфере ИБ постоянно меняется. Вузы за переменами не успевают, а учебные материалы стремительно устаревают. Как объединение усилий образовательных организаций и экспертов-практиков может помочь переломить негативную ситуацию? Какие внутренние возможности для добора компетенций и повышения мотивации компании могут предложить ИБ-сотрудникам?

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

Банки и ИБ-компании в вузах

Представители финансового сектора, который входит в число отраслей, где дефицит ИБ-специалистов ощущается особенно остро, активно включаются в решение задачи подготовки «безопасников» для отрасли. Так, Газпромбанк в лице заместителя начальника департамента защиты информации **Алексея Плешкова** вносит значимый вклад в обеспечении служб информационной безопасности банков молодыми сотрудниками. «Я более 10 лет работал по совместительству на кафедре № 44 «Информационная безопасность» в Московском инженерно-физическом институте, — рассказал Алексей Плешков. — Не понаслышке знаю, как обстоит дело с подготовкой кадров по направлению ИБ и какие существуют трудности и нерешенные задачи. За время работы в МИФИ я подготовил и выпустил более 500 молодых специалистов, часть из которых пригласил для работы в ИБ-команде Газпромбанка. Мои выпускники успешно трудятся практически во всех крупнейших ИБ-командах в России и во многих известных ИБ-компаниях и международных ИБ-проектах».

Большинство игроков российского рынка информационной безопасности понимают, кто может спасти экономику от нехватки кадров, и с середины 2010-х годов выстраивают отношения с высшими учебными заведениями, готовящими молодых специалистов в этой сфере.

В СМИ можно найти новости от многих компаний разработчиков, поставщиков, интеграторов ИБ-решений, посвященные их взаимодействию с учебными заведениями как высшего, так и среднего профессионального образования.

Вот заголовки только некоторых из них: «Компания BI.ZONE и кафедра информационной безопасности Национального исследовательского университета "Московский институт электронной техники" (НИУ МИЭТ) запустили совместный проект», «Тинькофф и Positive Technologies объявляют о сотрудничестве в области подготовки специалистов по кибербезопасности на базе Центрального университета», «Национальный исследовательский университет МЭИ и российский разработчик систем кибербезопасности компания R-Vision договорились о совместной подготовке специалистов по информационной безопасности», «РТУ МИРЭА и компания BSS запустили для студентов совместный курс по информационной безопасности».

Некоторые игроки пошли еще дальше. Так, ГК «Солар» еще в 2023 году завершила первую волну проекта профориентации детей, которая длилась восемь месяцев и включала в себя обучение основам ИБ и развитие soft skills. А «Лаборатория Касперского» и образовательный комплекс «Воробьевы горы» в конце лета 2024 года подписали соглашение о намерениях о повышении уровня образования в сфере информационной безопасности. В частности, стороны предусмотрели дополнительную общеразвивающую программу в сфере кибербезопасности и информационных технологий, основанную на материалах, разработанных «Лабораторией Касперского».

Компания RTM Group, по словам ее управляющего **Евгения Царева,** сотрудничает с десятками вузов, обучающих ИБ. Совместно с ними она готовит образовательные программы, а ее сотрудники участвуют в образовательном процессе. «Самый крупный проект — обучающий курс по КИИ и ПДн с применением платформы MEDOED, бесплатной для студентов. Мы вышли за рамки строго нормативных требований и привносим в учебный процесс практику соответствия законодательству», — рассказал Евгений Царев. Помимо этого RTM Group выступает спонсором и соорганизатором студенческих программ Career and Technology Foundations (CTF) и ежегодно проводит студенческую олимпиаду RTM Challenge. Как отметил эксперт, некоторые ее победители работают сейчас в компании на ведущих должностях.

В компании UserGate взаимодействием с вузами и учебными центрами занимается специальное подразделение — Академия UserGate. Основные направления ее деятельности — разработка учебных курсов по решениям UserGate, создание и развитие сети авторизованных учебных центров, сотрудничество с вузами, взаимодействие с профессиональным сообществом. Сегодня все они очень востребованы и активно развиваются. «Кроме того, ряд сотрудников UserGate, в том числе я, являются преподавателями в вузах по специальности "Информационная безопасность"», — отметил **Дмитрий Кузеванов,** директор по информационной безопасности, руководитель центра мониторинга и реагирования UserGate.

Образовательное направление есть и в «Группе Астра». Это проекты «Астра-университет» и «Астра-колледж», в рамках которых образовательные учреждения — партнеры Группы — осуществляют подготовку специалистов по таким специальностям, как «Компьютерная безопасность», «Информационная безопасность телекоммуникационных систем», «Применение и эксплуатация автоматизированных систем специального назначения» в сфере высшего профессионального образования и «Обеспечение информационной безопасности автоматизированных систем» в сфере среднего профессионального образования.

«Кроме того, — поделилась с нами подробностями **Марина Яловега,** директор по персоналу «Группы Астра», — ежегодно наша компания совместно с образовательными учреждениями проводит различные мероприятия по информационной безопасности: хакатоны, CTF-соревнования, образовательные интенсивы, "Летние школы". По ее словам, сотрудники департамента образования в качестве главных и индустриальных экспертов принимают участие в проведении демонстрационных экзаменов для студентов колледжей, а также в проведении Всероссийского чемпионата по профессиональному мастерству «Профессионалы» в рамках конкурсного направления «Информационная безопасность».

Компания SecWare пока ограничивается приемом студентов на практику, но специалисты этой компании тоже проводят занятия в университетах.

В сообществах профессионалов в сфере информационной безопасности, на отраслевых мероприятиях игроки рынка делятся своими мнениями о том, какие изменения нужно внести в образовательный процесс, чтобы усовершенствовать подготовку молодых специалистов в этой сфере. «Но, к сожалению, — констатировала **Наталия Чумаченко,** HR-директор компании «Информзащита», — такие пожелания не всегда возможно реализовать. И дело тут часто далеко не в нежелании руководителей вузов и направлений по ИБ. Мы понимаем, что они во многих решениях скованы требованиями и стандартами, поэтому не могут, например, выделять больше времени на практические занятия в ущерб теоретическим. Рынок ИБ постоянно развивается, и пока вуз внедряет наши пожелания в учебную программу, акценты уже сместились».

Вместе с тем, по ее словам, компания «Информзащита» считает работу с вузами стратегически важной. Тесные связи уже налажены с НИУ Пермского государственного университета, недавно подписано соглашение о сотрудничестве с Московским техническим университетом связи и информатики (МТУСИ).

Специалисты компании читают лекции и в других высших учебных заведениях.

Сотрудники компании «КриптоПро» тоже включились в образовательный процесс в некоторых вузах, но не только с целью донести до руководства вузов свои требования к подготовке студентов. По мнению **Павла Луцика,** директора по развитию бизнеса и работе с партнерами этой компании, важнее ориентироваться на фундаментальные направления знаний, чтобы выделять и привлекать на работу наиболее ярко проявивших себя на занятиях студентов.

Стратегические партнерские отношения связывают компанию УЦСБ, российского системного интегратора, с Уральским федеральным университетом (УрФУ). На разных факультетах университета этот системный интегратор открыл две лаборатории кибербезопасности: на радиофаке (ИРИТ-РТФ) — NEO, на матмехе (ИЕНиМ) — TRINITY. Здесь студенты знакомятся с самыми современными технологиями и инструментами в области кибербезопасности, пробуют строить собственные стенды. «На радиофаке УрФУ у нашей компании есть собственная образовательная программа по подготовке бакалавров по информационной безопасности, — рассказал **Евгений Баклушин,** заместитель директора Аналитического центра УЦСБ, — а также мы являемся партнерами магистерской образовательной программы по подготовке специалистов, призванных защищать государственные информационные системы и критическую информационную инфраструктуру РФ. Помимо этого компания УЦСБ ежегодно проводит летнюю школу, на занятиях в которой будущие ИБ-специалисты могут поработать бок о бок с нашими специалистами и приобрести опыт решения прикладных (боевых) задач».

Иногда участники рынка объединяются, для того чтобы наиболее широко представить студентам технических вузов весь спектр проблем и задач, стоящих сегодня в сфере кибербезопасности. К примеру, в последнюю неделю октября в Москве прошла Неделя кибербезопасности, организатором которой выступила ГК «Солар».

Масштабное мероприятие началось с серии образовательных лекций для студентов и молодых специалистов «Кибербезликбез», ориентированных как на будущих специалистов по ИБ, так и на учащихся непрофильных специальностей. В течение четырех дней октября специалисты из крупнейших российских ИБ-компаний — ГК "Солар", UserGate, "Лаборатория Касперского", Positive Technologies — читали лекции в РТУ МИРЭА, МГТУ им. Баумана, РЭУ им. Плеханова. Их рассказ дополняли представители IT-компаний «ЕДИНЫЙ ЦУПИС» и Makves, а также Музея криптографии. Практики отражения DDoS-атак, актуальные способы онлайн-мошенничества, способы шифрования, применявшиеся в прошлом веке, карьерные возможности в кибербезопасности — вот далеко не полный перечень вопросов, которые освещались на лекциях, а завершил Неделю кибербезопасности День открытых дверей в ГК «Солар».

Обучение и киберучения

Все это прекрасно, но, по данным исследования Центра стратегических разработок «Северо-Запад» и компании Positive Technologies «Рынок труда в информационной безопасности в России в 2024–2027 годах: прогнозы, проблемы и перспективы», российские вузы выпускают всего по 10–15 тыс. молодых ИБ-специалистов в год, и не все из них устраиваются на работу по специальности. В то же время потребность в ИБ-специалистах в 2023 году составляла примерно 50 тыс. человек, а в 2027 году прогнозируется на уровне 54–65 тыс. Таким образом, даже плотного сотрудничества игроков рынка информационной безопасности с высшими учебными заведениями недостаточно, для того чтобы этот дефицит пополнить.

Еще один прогноз: вместо ИБ-специалистов широкого профиля через три года на рынке будут востребованы узкоспециализированные профессионалы — архитекторы, инженеры, аудиторы, консультанты и аналитики. А это значит, что параллельно сотрудничеству с вузами необходимо уделять внимание программам переквалификации, развития и повышения квалификации. Важную роль тут могут играть киберучения — мероприятия для проверки и оценки уровня навыков отражения кибератак у ИБ-специалистов.

«Повышение квалификации ИБ-специалистов в банках — это необходимая вещь, так как в финансовой сфере тактики злоумышленников совершенствуются с завидной скоростью. Специалистов по информационной безопасности обязательно надо отправлять на повышение квалификации в компании, предоставляющие такие услуги. Специалисты компаний, предоставляющих сервисные услуги ИБ, имеют большую насмотренность, так как работают с инцидентами в разных компаниях и разных сферах, поэтому могут передать этот опыт специалистам по ИБ, работающим в рамках одной организации», — убеждена Наталия Чумаченко.

Также эксперт уверена в пользе киберучений, которые нужно проводить не реже раза в год. Благодаря этим мероприятиям в банке складывается понимание слабых мест и уязвимостей системы, в ликвидацию которых нужно инвестировать средства. Также киберучения показывают реальный уровень подготовки команды ИБ, позиции, которые требуют усиления, то есть поиска новых специалистов или повышения квалификации тех, кто уже есть в коллективе.

Банки, в которых обеспечение ИБ поставлено правильно, так и делают. Специалисты и руководители по ИБ в команде Газпромбанка проходят регулярное, чаще одного раза в год, повышение квалификации по направлению работы, а также по требованиям к квалификации лиц, ответственных за сопровождение участков защиты информации на объектах КИИ. По словам Алексея Плешкова, это может быть как внутреннее (в корпоративном университете), так и внешнее обучение. «Чаще всего наши специалисты направляются на курсы повышения квалификации в профильные учебные центры по всей России, — рассказал эксперт. — Это особенно актуально

в рамках реализации стратегии импортозамещения до 2025 года всех СЗИ в организации — субъекте КИИ. Нам крайне важно знать и понимать все особенности сопровождения отечественных решений в области защиты информации, которые в перил с 2022 по 2024 год были успешно интегрированы в инфраструктуру Газпромбанка без деградации производительности основных бизнес-процессов».

Регулярно совместно с партнерами по ИБ Газпромбанк проводит киберучения. С коллегами из ФИНЦЕРТ ЦБ РФ банк участвует в отраслевых киберучениях, в которых стабильно демонстрирует самые высокие результаты.

Киберучения всех уровней помогают ГПБ поддерживать стабильно высокий уровень кибербезопасности и защищенности IT-ресурсов в Газпромбанке, причем подтверждать его не только теоретически, в рамках регулярных комплаенс-проверок со стороны государственных регуляторов, но и на деле: отсутствием актуальных уязвимостей и умением своевременно, профессионально и адекватно реагировать на возникающие инциденты информационной безопасности.

Киберучения — очень важная часть процесса обеспечения информационной безопасности абсолютно любой организации, независимо от профиля работы и индустрии, считает Дмитрий Кузеванов. «Безусловно, обладая необходимыми компетенциями и уделяя вопросу кибербезопасности самое пристальное внимание, мы проводим киберучения на регулярной основе. Причем делаем это не только внутри UserGate, но и помогаем с организацией другим компаниям, для которых ИБ не является профильным направлением», — поделился опытом работы по повышению ИБ эксперт. По его словам, анализ результатов киберучений позволяет объективно оценить уровень ИБ в компании, выявить сильные и слабые места, понять, чему еще нужно обучить сотрудников и как подготовить их к эффективным действиям во время кибератаки.

Практика проведения киберучений существует в компании SecWare. **Андрей Попов,** руководитель отдела аналитики и аудита ИБ этой компании, напомнил о необходимости проводить внутреннее обучение (к слову, прописанное в стандартах и нормативных документах). «Наша компания небольшая, поэтому нам проще это организовывать», — заметил он. В добавление ко всем вышеперечисленным положительным эффектам от этих мероприятий Андрей Попов назвал выработку персональной ответственности за обеспечение ИБ у каждого сотрудника, что в итоге повышает уровень ИБ в компании.

«Сегодня банки — это огромная инфраструктура с сотнями продуктов, которые нужно защищать. Банковская отрасль находится в авангарде развития информационных технологий в нашей стране, поэтому в банке сегодня есть огромное количество возможностей для развития специалистов ИБ по любому из направлений, — констатировал Евгений Баклушин. — Киберучения в некоторых случаях идут в постоянном режиме. Это отличный инструмент держать команду ИБ в тонусе и помогать ей развивать свои навыки, а для обычных пользователей — повышать осведомленность в вопросах ИБ». Б.О