ЧЕРЕЗ УЧЕНИЕ К НОВОМУ
СТР. 39

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ
СТР. 43

ТЕМА НОМЕРА

ПРОФЕССИОНАЛЬНАЯ ПОДГОТОВКА В ОБЛАСТИ БЕЗОПАСНОСТИ

Через учение к новому

У каждого профессионала рано или поздно наступает момент, когда необходимо сделать паузу, осознать свои достижения и победы. поразмышлять о дальнейшем развитии карьеры. Такое развитие, в большинстве случаев, требует от человека приобретения каких-либо дополнительных знаний, получения дополнительного образования. Об этом – **в статье Михаила Савельева**

МИХАИЛ САВЕЛЬЕВ,
директор Учебного центра «Информзащита»

В последнее время все большее число моих знакомых, работающих в сфере информационной безопасности, начинает задумываться о своем профессиональном развитии. Вероятно, это связано с двумя факторами: кризис экономический и кризис, как это ни прискорбно, среднего возраста.

Причем оба фактора в плане профессионального самоопределения действуют сонаправленно: многим хочется осознать, чего они уже достигли, хотят ли развиваться дальше в имеющейся профессиональной области или желают большего, а то и, возможно, что-то поменять в карьере.

И если кризис среднего возраста требует разобраться в этом для принятия или переоценки ориентиров, то экономический кризис заставляет думать о том, как сохранить имеющееся или преобразоваться с выгодой для положения или кошелька.

Охватить все аспекты самоопределения нельзя, но порассуждать о том, в каких направлениях можно попробовать пройти профессиональную переподготовку и начать с условного нуля – возможно. Из всех путей стоит выбрать пять самых очевидных и не требующих совсем уж кардинальной переориентации (с той точки зрения, что мы остаемся примерно в рамках имеющихся навыков). Эти пять путей можно сформулировать так:

- Повышение в ИБ.
- Смещение в сторону ИТ.
- Смещение в сторону экономической безопасности.
- Уход в менеджмент.
- Смена стороны баррикад.

Понятно, что для думающего человека нет ничего невозможного, но всеже попробуем рассмотреть указанные переходы с точки зрения обучения и обучаемости, т. е. чему стоит поучиться человеку, задумавшему подобный переход, и чему, возможно, он уже обучиться не успеет.

Повышение в ИБ

Ограничивающим фактором на этом пути может стать условная «зрелость» компании, в которой мы трудимся, и для применения всех наших навыков потребуется смена масштаба предприятия. Но в любом случае зрелость самого специалиста по информационной безопасности состоит в правильном понимании смысла своей деятельности, в том, чтобы научится защищать не элементы инфраструктуры, а интересы компании и ее процессы, обеспечивать непрерывность этих процессов, уметь обрабатывать и расследовать инциденты.

В указанных областях накоплен достаточный опыт, который можно изучить. Что-то можно подчерпнуть из узкоспециализированных учебных курсов, которые читают истинные практики, однако с определенного момента придется перейти на самообразование: опыт – это то, что можно впитать из общения с коллегами, и вычленение зерен из плевел льющейся на нас информации.

Смещение в ИТ

Этот путь требует очевидной внутренней перестройки, особенно если до этого не удавалось наладить связи с соседним подразделением. Между задачами подразделений ИТ и безопасности есть много общего, но в то же время взгляд на один и тот же предмет – разный. Не секрет, что во многих компаниях этот самый различный взгляд приводит к множеству конфликтов.

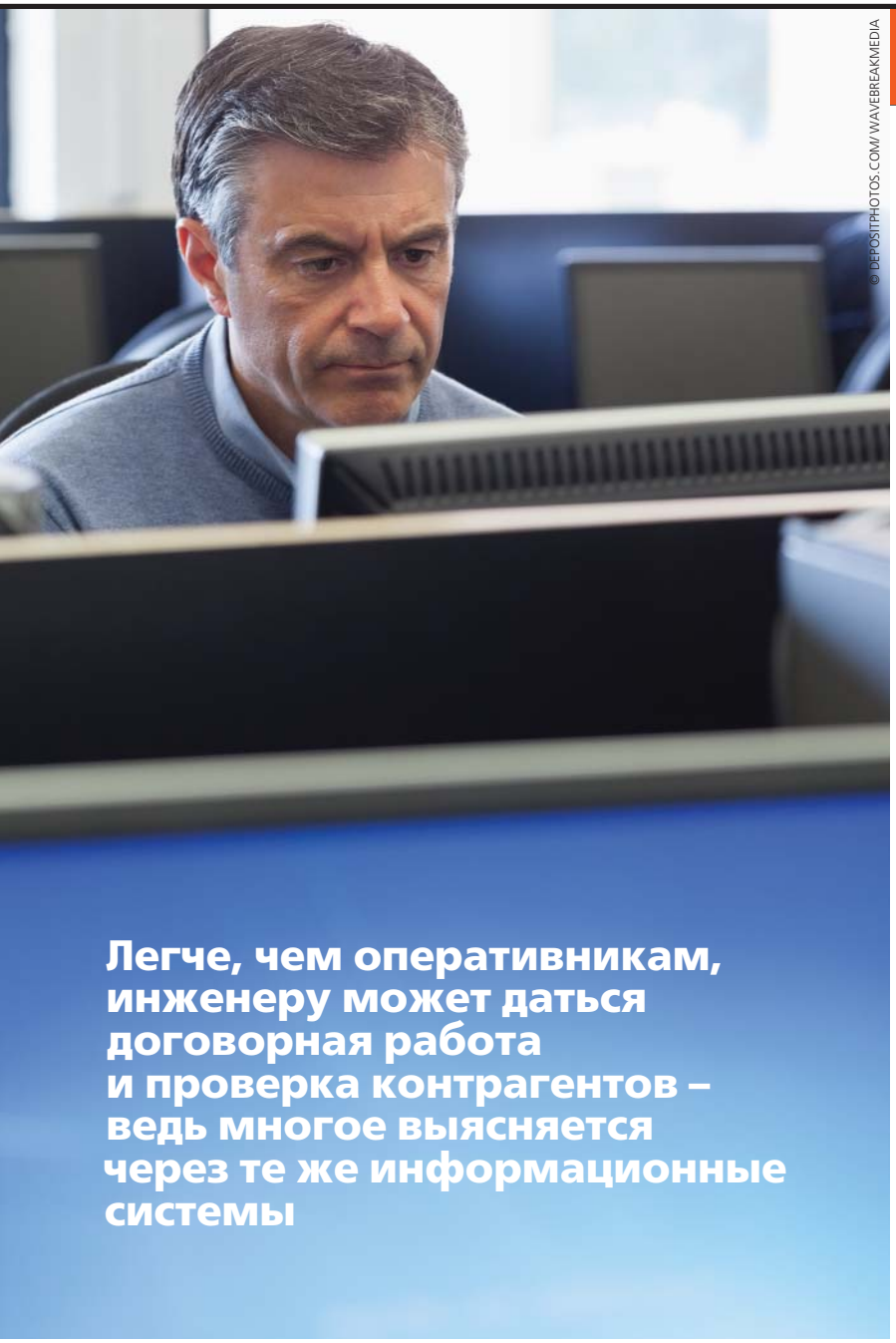
Для скорейшего вхождения в должность придется для начала изменить свою психологию и перейти от контроля процессов к их автоматизации, больше внимания уделять непрерывности процессов и восстановлению после сбоев, посвящать время технической поддержке. Помимо методов оптимизации сложных лицензионных политик различных вендоров учиться придется пониманию потребностей компании и навыкам убеждения менеджмента тому, какие технологические новинки окажут влияние на компанию в ближайшем будущем. Ведь ИТ уже давно не воспринимается как просто поставщик базовых работающих сервисов типа почты, офиса и 1С. От грамотного айтишника ожидают поставок конкурентных преимуществ.

Поэтому для полноценного соответствия ожиданиям, помимо техники, придется осваивать финансовый и управленческий учет, управление проектами, практики управления ИТ-инфраструктурами, дисциплины, связанные с внутренним маркетингом (для убеждения руководства и лучшего понимания ожиданий внутренних пользователей от процессов автоматизации) и стресс-менеджмент.

Из ИБ в ЭБ

Быть более полезным в кризис и уметь делать больше работы за ту же зарплату – это то, что нравится всем руководителям без исключения. Однако этот путь один из самых сложных, хотя, стоит признать, и самый интересный. Придется разбираться как с новыми угрозами, до этого вообще не попадавшими в поле зрения, так и под новым углом зрения взглянуть на те, которые рассматривались с точки зрения безопасности информационной.

Причем придется признать, что далеко не со всеми обязанностями может справиться бывший инженер-безопасник.



© DEPOSITPHOTOS.COM/WAVEBREAKMEDIA

Легче, чем оперативникам, инженеру может даться договорная работа и проверка контрагентов – ведь многое выясняется через те же информационные системы

В поле зрения экономической безопасности попадают вопросы договорной работы и проверки контрагентов, анализ финансовых рисков, возможное противодействие конкурентов, давление со стороны клиентов (от откровенного мошенничества до работы с задолженностью), необходимость решать возможные претензии со стороны рейдеров или бандитов, а порой – разрешать претензии правоохранительных органов, заниматься кадровой безопасностью, ограждая компанию от действий откровенных мошенников, обиженных или же просто низкокомпетентных сотрудников. Считать можно по-разному, но из девяти перечисленных угроз бывший инженер после цикла обучения, скорее всего, сможет так или иначе совладать лишь с пятью.

Инженер сможет овладеть можно вопросами кадровой безопасности (с оговоркой на его персональный талант умения общения с людьми, умения входить в доверие и «доставать» информацию). Может пригодится опыт прохождения проверок регуляторов, с оговорками на то, что напор налоговиков и полицейских может быть не в пример более жестким. Легче, чем оперативникам, инженеру может даться договорная работа и проверка контрагентов – ведь многое выясняется через те же информационные системы.

А вот финансовые вопросы, работа с должниками, рейдерами и бандитами, а также конкурентами потребуют как серьезной подготовки, так и определенного опыта. Утешением тут может служить то, что с этими угрозами умеют работать далеко не все, кто изначально работал в области экономической безопасности. Основным предметом для изучения здесь будет юриспруденция – как нападение, так и оборона тут завязаны только на тонкости, недосказанности, противоречивости законодательства.

Менеджмент

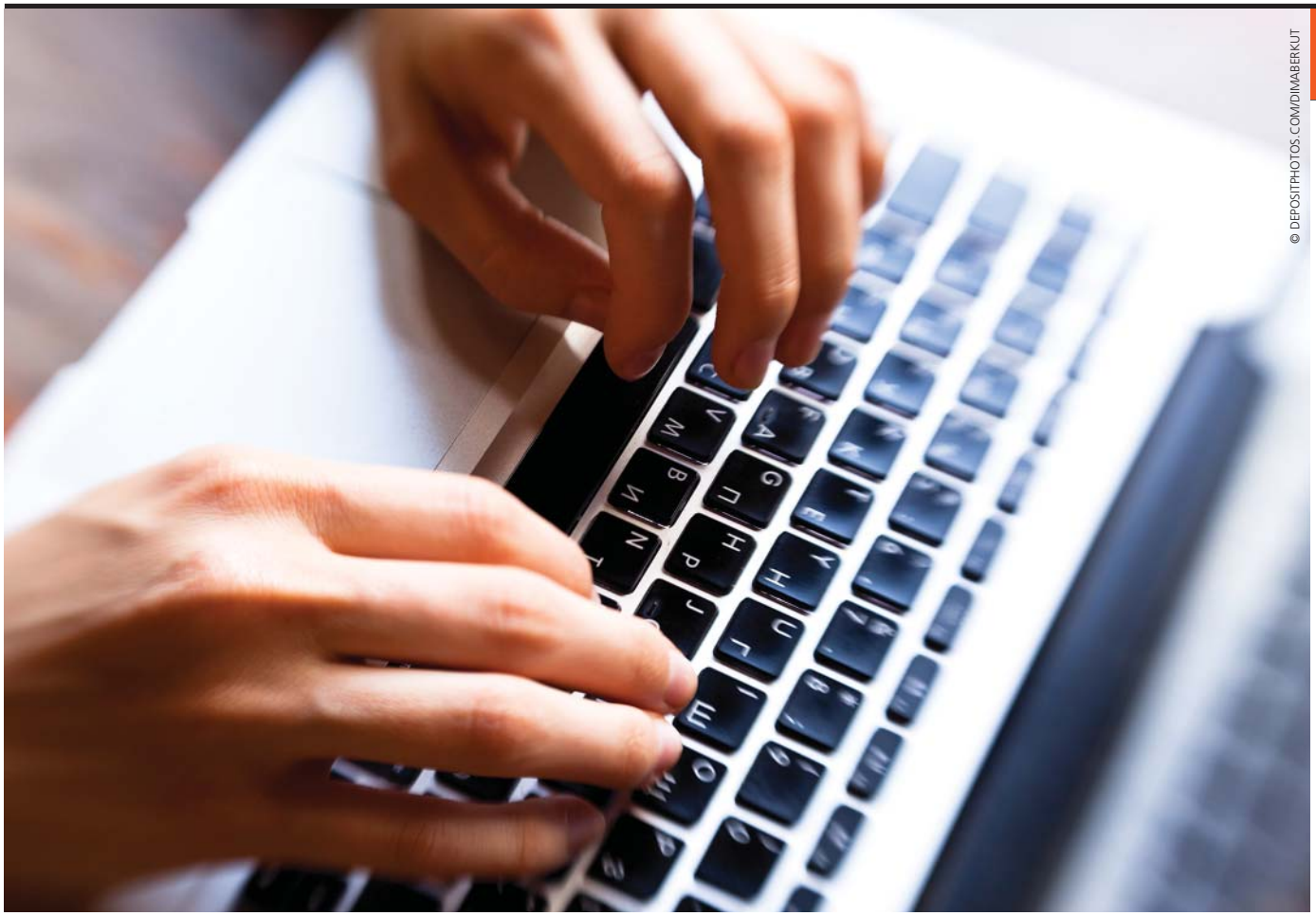
Этот путь труден не столько с точки зрения подготовки, сколько с точки зрения возможностей. ИТ- или ИБ-службы значимы только в тех отраслях, которые сами завязаны на информационных технологиях. Можно рассмотреть под «менеджментом» возможность занять пост CIO или CISO либо надо говорить о завершении карьеры в ИТ.

Что требуется для реализации первых двух возможностей, мы уже проговорили. Реализация «стороннего» пути – это скорее счастливый случай, требующей серьезной профессиональной перестройки. Хотя в зависимости от способностей человека она, вероятно, будет заключаться в изучении нового профессионального языка. Для этого, как ни странно, лучше всего подходят курсы типа MBA: они дают возможность узнать, из каких кирпичей складывается работа организации, расширить кругозор и погрузиться в одну из интересующих областей: финансы, маркетинг, управление.

Смена стороны баррикад

Под этим крылатым выражением понимается переход от стороны, реализующей безопасность, в сферу услуг – интеграцию или наоборот. Здесь почти нет сюрпризов с точки рения обучения: работа та же, навыки нужны те же.

На этом пути скорее стоит ожидать ломки с точки зрения психологии. По наблюдениям, сложнее дается переход именно со стороны «заказчи-



Обучиться, скорее всего, придется тонкостям тех технологий, которые до этого были знакомы только шапочно

ка» на сторону интеграции: несколько параллельных проектов, странновато-вычурные требования на каждом, сроки, конечность ресурсов исполнителя… Все это обеспечивает неплохую встряску.

Обучиться, скорее всего, придется тонкостям тех технологий, которые до этого были знакомы только шапочно. Как говорится, «о сколько нам открытий чудных» готовит взгляд с другой стороны… Тут даже привычные решения, которые ты эксплуатировал много лет, окажутся монстрами, готовящими сюрпризы на каждом шагу внедрения и запуска в эксплуатацию. Да, и будем считать, что проектное управление мы знаем «по основной» работе… а то и эти знания будут нуждаться в обновлении.

Переход же из интеграции в звено обеспечения корпоративной безопасности дается легче, но тут возникает вопрос специализации. Работая над однотипными проектами по внедрению чего-то там, поневоле приходится встать, оглядеться и начать глубоко разбираться сразу во всем: тут и трудности применения отдельных видов законодательства, и отраслевые требования, и вопросы бюджетирования и обоснования расходов.

С точки зрения обучения, сосредоточиться стоит на управленческом учете и т. п. вопросах, которые позволят аргументированно объясняться с руководством. На втором месте по востребованности, скорее всего, будут курсы по отдельным аспектам законодательства, а особенно – по тем его моментам, которые позволят без особенных затрат выполнить все требования закона.

В итоге

Если только не решить уйти в управдомы (хотя, если разобраться, и на этом пути нас ждет немало сюрпризов), что бы мы ни делали, нам придется учиться, доучиваться или переучиваться… Но это и прекрасно. Поскольку старость наступает тогда, когда мы теряем способность и желание к учебе, совершенствованию, изменению мира вокруг себя. А раз еще не все равно, значит не стоит бояться и стоит пробовать, стоит бороться, стоит учиться чему-то новому. ●