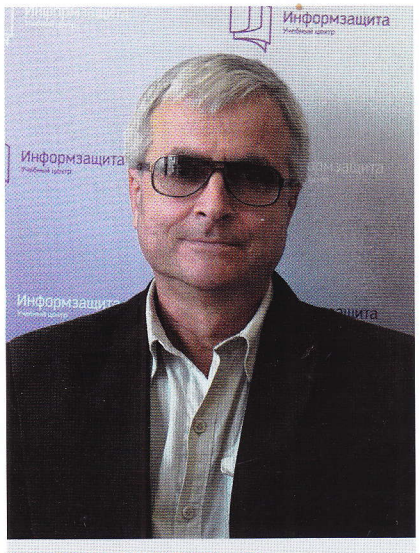
Полковника никто не ждет?

Недавно мне позвонил старый знакомый, озабоченный поисками нового заместителя по безопасности, — не сработались с прежним. Он попросил порекомендовать кого-нибудь и добавил: «Только, знаешь, полковников не надо...». То, что человек с погонами теперь зачастую оказывается ненужным в качестве безопасника, уже стало тенденцией. И дело, конечно, — не в том, что у всех генеральных директоров внезапно началась аллергия на бывших полковников. Просто изменилась жизнь, а с нею — и требования к таким сотрудникам.



РАШИД НУГАЕВ

Преподаватель УЦ «Информзащита»

Безопасность на базе коррупции

В начале 1990-х гг. обязанности безопасника были, в принципе, незамысловатыми, как и действия основных источников опасности — братвы, т. е. бандитов. Требовалось пресечь попытки «крышевания», обеспечить надежную физическую охрану объектов, первых лиц, членов их семей и имущества, установить контакты с бывшими коллегами, еще остающимися на службе. Контакты устанавливались легко, ибо руководители оперативных подразделений были людьми в возрасте, которые прекрасно понимали, что скоро — на пенсию, а на соответствующие выплаты жить трудно. Вот они и подрабатывали, предупреждая о готовящихся проверках, закрывая уголовные дела, проверяя контрагентов и предоставляя силовую поддержку. Многие из них потом пересаживались из государственного служебного кресла в более комфортабельное и безопасное кресло зама по безопасности руководителя какого-нибудь АО.

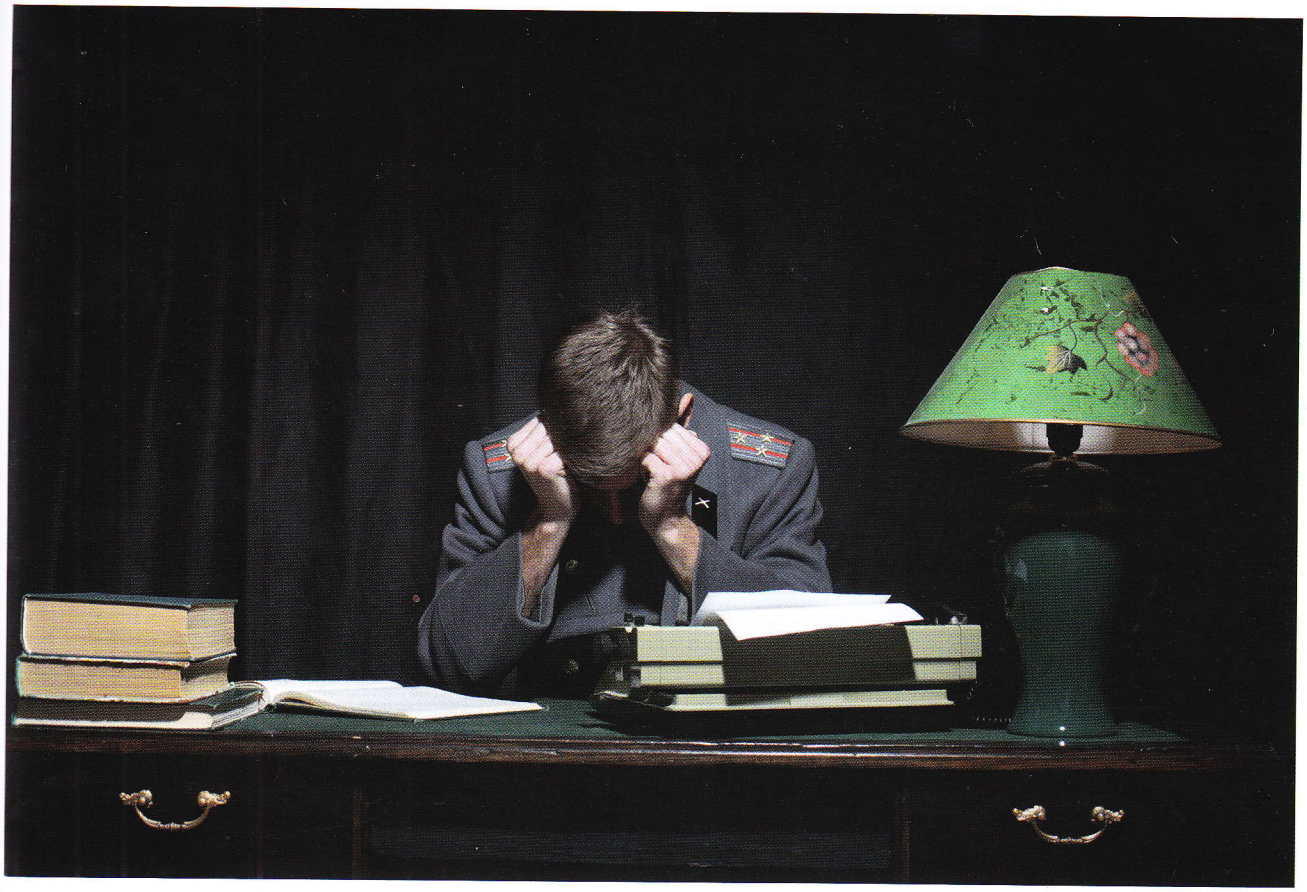
В эту схему бывший полковник прекрасно вписывался, и не имело значения, чем он занимался на прежней работе. Он мог быть оперативником или чиновником, сохранившим деловые контакты с действующими коллегами и, главное, возможность «порешать вопросы». Руководители предприятий на такую «работу» денег не жалели, понимая, что если не подкармливать личные связи бывшего полковника, они проживут недолго. Другими словами, большинство руководителей тех лет решало вопросы безопасности, создавая коррупционные механизмы и финансируя коррупцию.

Механизмы эти окончательно сформировались в «нулевые» годы, проникнув в суды, прокуратуру и следственные органы. Их «носители» начали жить самостоятельной жизнью, и у них появились собственные имущественные интересы. А некоторые бизнесмены на собственной шкуре — потеряв бизнес или свободу — испытали полную непробиваемость ими же созданных структур и механизмов.

Потом ситуация стала быстро меняться. В 2008 г. уже расформировали УБОПы. Борьба с бандитами, вроде бы, закончилась — полных отморозков посадили, а остальных поставили под контроль. При этом некоторые подконтрольные занялись отмыванием и легализацией денежных средств, другие — организацией рейдерских захватов. Отметим, коррупционная поддержка таких процессов осталась, а коррупция — тоже деятельность организованной преступности.

По новым правилам

Сейчас, как и прежде, активно продолжается передел собственности (другими словами, остается неизменной цель завладения чужим имуществом), но радикально изменились условия и правила «работы». Бандитские разборки лихих 1990-х сменились



разборками в арбитражных судах, где стороны именуются не бандитами, а «хозяйствующими субъектами». Но теперь вместо автомата АК-74 «хозяйствующий субъект» размахивает решением суда, вступившим в законную силу. А наши законы дают предостаточно возможностей для злоупотребления правом.

Да, бывает и иначе. Например, если в регламентах организации предусмотрены обязательные процедуры, без выполнения которых не может быть заключен какой-либо договор, то предоставленный на суде фальшивый документ, не прошедший этих процедур, будет воспринят добросовестным судьей как сомнительный. Подчеркнем: регламенты являются нормативно-правовыми документами, обладающими юридической силой. И это делает соблюдение действующего законодательства одной из важнейших задач обеспечения безопасности компании.

Кроме того, изменились технические принципы и способы обмена информацией. Электронные технологии быстро встроились в повседневную жизнь. Деньги, общение и даже искусство стали «цифрой», социальные сети — обыденностью. И теперь даже ИТ-специалисты не совсем представляют себе истинного масштаба новых угроз.

Изменились технические принципы и способы обмена информацией. Электронные технологии быстро встроились в повседневную жизнь. Деньги, общение и даже искусство стали «цифрой», социальные сети — обыденностью. И теперь даже ИТ-специалисты не совсем представляют себе истинного масштаба новых угроз.

Во время 30-й международной выставки CeBIT, состоявшейся в марте 2015 г. в Ганновере, был организован видеомост с разоблачителем тайн информационной разведки Сноуденом. Он предупредил ИТ-специалистов, что именно они (а не журналисты, политики и чиновники) являются главной целью спецслужб. Цитирую: «Спецслужбы ищут людей, у которых есть доступ к инфраструктуре, администраторов, инженеров, сотрудников сервис-провайдеров. Они ищут вас не потому, что вы — террористы или подозреваемые, а потому, что у вас есть доступ к конфиденциальным записям, к частной жизни. ИТ-специалисты

часто недооценивают важность информации, которой владеют, и не применяют какие-либо средства ее защиты. Например, они хранят важную информацию на своем мобильном устройстве или в личной почте, не используя шифрование и двухфакторную аутентификацию».

Чаще всего атакам подвергаются мелкие и средние компании, ущерб которых не может вызвать широкого общественного резонанса. По данным Symantec, более трети атак приходится на предприятия, имеющие менее 250 сотрудников. При этом специалисты констатируют: «Тезисы Сноудена косвенно подтверждаются опросом ИТ-специалистов, проведенным нами в конце 2014 г. По мнению 46% респондентов, потеря их мобильного устройства и кража корпоративной информации из его памяти подвергнут риску их компании» (Газета.Ru, руководитель отдела технического и маркетингового сопровождения ESET Russia Алексей Оськин).

Итак, сегодня условиями выживания предприятия в целом и безопасника в частности являются строгое соблюдение законодательства и учет угроз, исходящих от ИТ-технологий. А обязанностью генерального директора, который уже не хочет, чтобы его заместителем по безопасности был полковник, является управление бизнесом, персоналом и безопасностью.

Что значит «управлять безопасностью»? Прежде всего, ставить корректные задачи безопаснику. И вот тут-то начинаются проблемы. Сегодня практически все, что подлежит защите, — это информация. Физическая охрана объекта подразумевает информацию о типах и расположении систем охраны, наблюдения и контроля. Телохранители должны знать маршруты и время передвижения охраняемого лица. Документооборот — электронный, средства связи — тоже. И угроза несанкционированного съема информации весьма актуальна.

В 2011 г. МВД России заявило, что за предыдущие три года число зафиксированных преступлений, соответствующих ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений», выросло в 75 раз. Естественно, руководитель компании хочет знать, все ли в ней в порядке с защитой информации. Он обращается к безопаснику и с удивлением выясняет, что тот не в курсе. Да, он способен «закошмарить» сотрудников, «чтобы муха не пролетела», и защитить бумажный документооборот, но речь-то идет о безопасности «цифры»... Руководитель ощущает угрозу для бизнеса, а любую угрозу, понятно, надо оценить.

Задача анализа рисков сразу упирается в риски защиты информации. В 1990-е гг. на соблюдение требований законодательства руководители смотрели сквозь пальцы — всегда была возможность договориться. Теперь появились новые законы, которые необходимо безусловно исполнять. Знаковым является ФЗ-152 «О персональных данных», и выполнение его императивных требований — это отдельная линия работы, которую надо организовать и финансировать. Оставим в стороне расплывчатость формулировки термина «персональные данные», делающую объект защиты неопределенным. Имеются тщательно проработанные руководящие документы ФСТЭК (Приказы № 17 и № 21) и ФСБ (Приказ № 378), есть методическая база. Вопрос — в другом: сможет ли бывший полковник, заместитель по безопасности, выполнить эти требования?

Что может полковник

В первую очередь, все зависит от того, какие перед ним стоят задачи. А они, в свою очередь, зависят от типа предприятия.

Вариант 1 — самый распространенный. Если предприятие выпускает серийную продукцию (стройматериалы, колбасу, книги) по открытым технологиям, у него нет проблем с защитой технологических или управленческих секретов, а ИТ преимущественно обеспечивают производственный процесс, то задачи безопасника сводятся к контролю над периметром, защите коммерческих секретов и предотвращению хищений. Со всем этим бывший полковник прекрасно справится, ведь основой его деятельности будут известные организационные меры и работа с информаторами.

С персональными данными — тоже просто. Руководитель компании, рассмотрев требования законов к защите, прикинув размеры расходов и оценив неопределенность формулировок, озвучивает предельно бюджетную постановку задачи: «Проверка должна пройти без замечаний!». Бывший полковник реализует набор организационных мер и контроль, а технической работой занимаются ИТ-специалисты. Требования выполнены формально, контроль — формальный, но претензий от регуляторов нет.

Вариант 2: ИТ-ресурсы предприятия сами являются производственными ресурсами. Таких предприятий (банки, телекоммуникационные компании, провайдеры, ЦОДы) — много и становится все больше. Одних только провайдеров, судя по количеству выданных лицензий, в России насчитывается около 11 тыс.

Понятно, что в этом случае формальный подход к обеспечению безопасности может привести к крушению бизнеса. Значит, безопасник должен знать ИТ-технологии — пусть ограниченно, на уровне требований регуляторов (ФСТЭК, ФСБ, РКН). Только при этом условии он сможет выполнять свои функции — анализировать риски, измерять угрозы и искать уязвимости.

Однако большинство заместителей по безопасности — бывшие офицеры

МВД и спецслужб, имеющие, как правило, юридическое образование (лишь изредка — техническое). А значит, безопасник вынужден действовать формально: он подписывает регламентирующие документы, разработанные ИТ-специалистами, не имея возможности вникнуть в их суть и не представляя себе механизма их реализации. В результате, понятно, возникает нешуточная угроза для безопасности.

Решение проблемы, казалось бы, — простое: обучить его ИТ. На это уйдет года четыре (второе высшее образование и опыт практической работы). Однако, как ни печально, ИТ-образование поверх гуманитарного ложится с трудом (обратное — намного легче).

Теперь поговорим о задачах главного безопасника. Это — управление безопасностью, собственным персоналом и минимизация негативного влияния на бизнес деятельности по обеспечению безопасности.

Большинство полковников прекрасно справляются с первой задачей, но со второй возникают проблемы. Руководство подразделением спецслужбы сильно отличается от руководства отделом безопасности юридического лица или ИП. Прежде всего, возникает иная мотивация: я несу полную ответственность за своих сотрудников, а мотивировать их, как в спецслужбе, угрозами санкций (сниму звезду, уволю без пенсии) не получится. На службе полковник может быть менеджером по персоналу, а на гражданской работе должен стать управленцем.

Отсутствие навыков управления приводит к тому, что главный безопасник акцентируется на карательных мерах. Однако они эффективны лишь на этапе наведения элементарного порядка. Затем нужно организовать контроль над соблюдением этого порядка, его «углубление», и тогда карательные меры становятся антиэффективными. Постоянное напряжение мешает людям работать, растет текучка кадров, осложняется работа с внутренними информаторами.

Основной акцент должен делаться на профилактике и воспитании, а это — кропотливая небыстрая работа. В первую очередь, нужно «грузить» сотрудников ответственностью. В России формулировка «нести ответственность» зачастую воспринимается негативно (мол, ответишь!), поскольку мы забываем о мерах поощрения. Задача безопасника — обеспечить «неотвратимость» поощрения. Сотрудники должны знать, что руководство видит не только плохую работу, но и хорошую, в том числе промежуточные результаты.

Наконец, третья задача безопасника. Любой регламент, связанный с защитой какого-либо технологического процесса, замедляет его выполнение. Нужно обеспечить корректность вмешательства в технологии, чтобы безопасность не стала тормозом. А для этого, опять-таки, требуется профессиональное образование безопасника или наличие экспертов, подсказывающих, что и как делать. Но если платить экспертам, зачем нужен полковник?

Получается, что на ИТ-ориентированных предприятиях целесообразно назначать на должность заместителя генерального директора по безопасности именно ИТ-специалиста. Опасения, что он слабо владеет организационными мерами и не имеет опыта оперативной работы, несостоятельны.

Означает ли это, что бывшие полковники больше не нужны? Разумеется, нет. В некоторых областях люди с опытом оперативной или следственной работы — вне конкуренции. Это, прежде всего, противодействие мошенничеству, служебные проверки и расследования. Именно в данных случаях оказывается востребованной и базовая юридическая подготовка. Какой заместитель по безопасности добровольно откажется от власти и перейдет в подчинение к новому заму? Многое зависит от меры ответственности безопасника, которую он должен осознавать, и от позиции руководителя предприятия.

Кроме того, если предприятие работает в стрессовом режиме (неустойчивое положение на рынке, угроза рейдерской атаки, давление криминала или правоохранительных органов), то от главного по безопасности требуются как раз навыки бывшего полковника. Это — умение работать в столь некомфортных условиях без риска потери управления и возможности анализировать действия противника, способность принимать неординарные, зачастую жесткие меры.

И — последнее. История, которая стала поводом для наших рассуждений, закончилась так: бывший полковник прошел курс обучения ИТ-технологиям, а руководитель организации — основам управленческой безопасности. И пока они друг на друга больше не жалуются.

Руководство подразделением спецслужбы сильно отличается от руководства отделом безопасности юридического лица или ИП. Прежде всего, возникает иная мотивация: я несу полную ответственность за своих сотрудников, а мотивировать их, как в спецслужбе, угрозами санкций не получится.