ЮРИДИЧЕСКАЯ ПРАКТИКА

Рисковое уведомление

«Киберугрозы — тренд цифрового мира, в который мы все начинаем погружаться», — Сергей Погребной и Александр Денисенко проанализировали, с какими рисками сталкивается украинский бизнес

«Сегодня бизнес должен защищать себя сам», — подчеркивают Сергей ПОГРЕБНОЙ (слева) и Александр ДЕНИСЕНКО

Что относится к основным бизнес-угрозам, кто и как может помочь бизнесу и какую роль в этом играет государство — об актуальных трендах в сфере корпоративной безопасности мы поговорили с **Сергеем Погребным**, партнером ЮФ **Sayenko Kharenko**, председателем Ассоциации профессионалов корпоративной безопасности Украины, и **Александром Денисенко**, директором по безопасности компании «Киевстар».

— Изменился ли перечень угроз, с которыми сталкивается украинский бизнес? Что, по вашему мнению, является основной угрозой?

Александр Денисенко (А.Д.): Безусловно, спектр и характер бизнес-угроз в последнее время изменились. Сейчас бизнес все больше внимания обращает на вопросы кибербезопасности. Мы все находимся в глобальном информационном поле, технологии стремительно меняются, и мы видим, какие риски это несет.

Сергей Погребной (С.П.): Ранее бизнес никогда не сталкивался с такими массированными атаками. Сейчас же это не одна компания, не две, а целые отрасли или даже страна.

А.Д.: Недавние события показали, что не все в этом плане просто и что бизнес и государство в целом не совсем к этому готовы.

— В нашей стране в принципе есть специалисты, которые могут противодействовать киберугрозам?

А.Д.: Конечно, есть. В частности, у нас в Ассоциации профессионалов корпоративной безопасности создается специальный комитет по кибербезопасности. К его работе мы привлекаем лучших специалистов отрасли.

— Какова роль государства в противодействии киберугрозам?

А.Д.: С большим уважением отношусь к подразделениям киберполиции, там есть хорошие специалисты — не много, но есть. Мы очень тесно с ними сотрудничаем, определенные наработки (с учетом технологического лидерства нашей компании) трансформируются в конкретные решения для рынка в целом. Вырабатывается стратегия поведения в киберпространстве. Киберполиция и Служба безопасности Украины принимают в этом очень активное участие.

С.П.: К слову, на конференции по корпоративной безопасности, которую мы проводим 18 октября, выступит известный бизнесмен и эксперт **Александр Кардаков** на тему «Кибербезопасность, кризисное реагирование и непрерывность бизнеса». Возглавляемые Александром компании сейчас очень активно занимаются этими вопросами, насколько мне известно, они принимали участие в защите ряда банковских структур, пострадавших от хакерских атак.

— Сергей Петрович, каков ваш топ-список бизнес-угроз?

С.П.: Во-первых, киберугрозы — тренд цифрового мира, в который мы все начинаем погружаться.

Второе — отношения правоохранительных органов и бизнеса. Сейчас наблюдается активность со стороны правоохранителей, появляются новые правоохранительные органы, такие как НАБУ, мы ожидаем создания Государственного бюро расследований и Государственной службы финансовых расследований. Усилила свои позиции Государственная служба финансового мониторинга. Все это в той или иной мере задевает бизнес. Часть претензий правоохранительных органов справедливы. Вместе с тем есть и очень много случаев, когда претензии необоснованны, и это реальная бизнес-угроза, к которой бизнес не готов. Много новых трендов возникло в вопросах взаимоотношений с новыми правоохранительными органами. Они поднимают пласт правоотношений периода 2010 — 2012 годов, и на их основе у бизнеса возникают новые проблемы — это новая волна, риск, которого бизнес не видит и просчитать который невозможно.

Третий громадный риск — рейдерство, постоянно меняющее свою форму. Рейдерство эволюционирует вместе с экономической жизнью, политическими событиями и развитием бизнеса в стране. Современное рейдерство многолико: псевдоактивисты, явный криминал и коррупционеры во власти, экономические мошенники. Плюс современные технологии: государство облегчило бизнесу ведение дел, отменив печати, нотариальное удостоверение, создав электронные реестры, но одновременно бизнес стал и более уязвимым. Ты никогда не знаешь, откуда возникнет угроза, если специально не готовишься к отражению рейдерской атаки.

Четвертая топ-угроза — участившиеся убийства бизнесменов. Я не помню, чтобы такое большое количество людей убивали за столь короткое время. И это только случаи, которые попадают в прессу.

Да, наше государство переживает очень сложные времена, да, у нас все еще сохраняется обостренная ситуация на востоке страны. Хотя Киев этого практически не ощущает — и никто думать об этом не хочет. Такая ситуация порождает массу последствий: нелегальное оружие, массовая безработица, миграция, бизнес сжимается. Правоохранительные органы, подверженные перманентному реформированию, реально не справляются. Отсюда простой вывод: сегодня бизнес должен защищать себя сам. Он должен инвестировать в безопасность, в том числе платя налоги государству и требуя, чтобы эти средства шли на развитие правоохранительных органов.

— Какие направления бизнеса больше всего подвержены рейдерским атакам? Актуально ли это для крупных компаний уровня «Киевстара»?

А.Д.: В крупных компаниях, как правило, внедрены международные стандарты безопасности и существует очень хорошая юридическая поддержка. Но даже они уязвимы, нельзя сказать, что они защищены на 100 %. Мелкий и средний бизнес уязвим очень сильно, особенно если это украинские предприятия.

Со случаями рейдерства мы, специалисты по безопасности, сталкиваемся буквально каждый день. Не хочется говорить, что правоохранительная система бездействует, это будет некорректно. Люди пытаются что-то делать, но, к сожалению, у многих, кто должен исполнять свои прямые функциональные обязанности, не совсем это получается. Очень большие риски у сельхозпредприятий, у металлургов, в телекоммуникационной отрасли, у грузоперевозчиков. Я активно взаимодействую с парламентским комитетом по вопросам информатизации и связи, мы поднимаем очень много вопросов в связи с кражами телекоммуникационного оборудования: масштабы хищений выходят за все разумные рамки. Это характерно и для других отраслей. Проблемы у бизнеса очень большие.

— Кто и как может помочь бизнесу? Что подразумевается под построением системы безопасности?

А.Д.: По мнению всего бизнеса, безопасность — это бывшие работники правоохранительных органов, которые за достаточно небольшие средства организовали пропускную систему на предприятии. На самом деле безопасность — комплекс мер: невозможно сделать что-то одно и достичь результата.

С.П.: Есть 20 отдельных направлений безопасности: кадровая, экономическая, финансовая, радиологическая, пожарная, экологическая и т.д. Кто у нас когда-либо проверял офис на радиологическую безопасность? Никто. Кого ни спрошу, слышу в ответ: «А что, надо?» А ведь не составит особой проблемы найти радиоактивное вещество (у нас под боком Чернобыль и много военного имущества, в котором используются радиоактивные элементы), оставить его в кабинете — и через три месяца человек заболеет раком.

Многие просто не понимают, что такое корпоративная безопасность. Если упростить, то корпоративная безопасность — это частная безопасность — бизнеса, собственника и наследования. Людей, которые об этом задумываются, всего 5–7 % в стране. А действительно компетентных структур топ-уровня, способных защитить бизнес и собственников, намного меньше: они есть, пожалуй, только у двух-трех человек.

— Как у нас обстоят дела с регламентированием детективной деятельности?

А.Д.: Это отдельная история. Сегодня такая деятельность ничем не регламентируется. Мы принимали участие в подготовке законопроекта. Мы очень благодарны народным депутатам из парламентского комитета законодательного обеспечения правоохранительной деятельности, возглавляемого **Андреем Кожемякиным**, а также народным депутатам **Николаю Паламарчуку** и Андрею Тетеруку за то, что они обратили внимание на эту проблему и дали возможность внести свои предложения. Нам этот закон не совсем нравился, но лучше плохой закон, который можно доработать, чем никакого. Самое главное, что народные депутаты услышали нас и согласились с тем, что регулятором детективной деятельности должен выступать Минюст, как это происходит во всем цивилизованном мире. Но этот закон был ветирован Президентом, отправлен на доработку, в том числе в этой части. Я не против того, чтобы государство контролировало частных детективов (оно должно контролировать, причем достаточно жестко), но делать это должен все-таки Минюст, а не МВД. Можем провести параллели с охранной деятельностью: в 2013 году был принят соответствующий закон (плохой и не соответствующий сложившимся реалиям), которым функции регулятора были предоставлены МВД. Но при этом МВД само является участником этого рынка, предоставляя охранные услуги. То же хотят сделать с детективами. Это неправильно. Пока у нас закона нет, но мы активно обсуждаем эти вопросы: к примеру, 19 октября в Киеве состоится Международный конгресс частных детективов. К нам приедут представители международного детективного сообщества, надеемся, будут и представители украинской власти.

С.П.: Получается, что государство решило не легализировать целую отрасль, которая де-факто работает.

А.Д.: Она работает точно так же, как работает охранная сфера. В то же время сами по себе существуют телохранители и частные военные компании, сами по себе живут те, кто имеет оружие, которое, как правило, не легализовано. Что говорить, закона об оружии у нас нет. Мы все живем сами по себе.

— Подводя итоги, скажите: на ваш взгляд, государство выступает преимущественно оппонентом или союзником бизнеса?

А.Д.: В определенных вопросах можно говорить о содействии.

С.П.: Разные представители государственных органов ведут себя по-разному, где-то оппонируя бизнесу, а где-то содействуя ему. Генеральное направление таково: государство поняло, что без бизнеса оно не проживет. Первые лица страны стараются максимально идти навстречу бизнесу. Как это все реализуется на местах — уже другой вопрос.

(Беседовал Алексей НАСАДЮК,

«Юридическая практика»)