Охрана предприятия

№1 (47), 2016

Оглавление

Могут ли хакеры взорвать самолет?

За последние несколько лет, по меньшей мере, два известных хакера громогласно заявили об имеющейся у них возможности взломать компьютерную сеть современного гражданского самолета и взять полет под контроль. Однако до сих пор неясно, насколько подобные заявления имеют под собой реальную почву, пишет М. Лейтщух на сайте securitymagazine.com.

Компьютеры современного самолета настолько сложны, считают эксперты, что удачная хакерская атака возможна лишь при условии, что преступнику досконально известны все внутренние операции лайнера, архитектура его компьютерной сети. Контрольные системы и средства киберзащиты, применяемые сегодня в самолетостроении, технологически изощренны и автономны, и потенциальному хакеру не только вторгнуться, но и вообще понять эти системы не под силу без специального образования и фундаментальной подготовки.

Однако было бы ошибкой считать, что авиалайнер на все 100% защищен от удачных хакерских взломов. Специалисты по кибербезопасности, работающие в авиа индустрии, знают уязвимые места и соревнуются с преступным миром, постоянно совершенствуя системы защиты.

Современный самолет представляет собой комплекс взаимосвязанных компьютерных сетей, некоторые из которых имеют выход во внешний мир. Эксперты опасаются, что этими «окошками» могут воспользоваться умелые хакеры, чтобы проникнуть в заповедные компоненты, контролирующие управление авиалайнером.

Наиболее важные операционные и контрольные системы автономны, однако не полностью изолированы от сетей, имеющих внешние выходы. Точки соприкосновения первых и вторых систем имеются в каждой модели самолета. Хотя все они оснащены специальными фильтрами и другими средствами киберзащиты, теоретически допустимо, что умелый хакер, глубоко разбирающийся в технологиях современного самолета, может взломать защиту и взять под контроль жизненно важные функции.

Грубо говоря, все компьютерные сети, через которые преступники могут получить доступ к узлам управления, разбиты на две категории. Первая категория обслуживает пассажиров: Wi-Fi и развлечения (музыка, видео, прочее). Вторую категорию составляются системы, обеспечивающие внешнюю связь экипажа с авиакомпаний, аэропортами, диспетчерами. Именно эта категория компьютеров вызывает наибольшую озабоченность у специалистов, поскольку они так или иначе связаны с самыми чувствительными компьютерными компонентами, отвечающими за безопасность авиалайнера.

Эксперты в целом согласны, что в обозримом будущем хакеры не смогут взять под свой контроль гражданский самолет во время рейса. Однако, хакерам вовсе не обязательно добиваться доступа в важнейшие контрольные компьютерные схемы внутри авиалайнера. Создать угрозу пассажирам можно, действуя через наземные операционные системы. И тому уже есть недавние примеры.

В июне 2015 года хакеры вынудили польскую авиакомпанию LOT Polish Airlines отменить двадцать и отложить еще несколько рейсов, нарушив работу офисных

компьютеров в варшавском аэропорту. Одновременно злоумышленники овладели клиентской информацией ряда авиакомпаний, пользующихся этим аэропортом.

В апреле 2015 года правительственное контрольное ведомство США (U.S. Government Accountability Office) обнаружило, что компьютеры, отвечающие за планирование и контроль авиарейсов на территории США, уязвимы для хакеров. Успешная атака на эти компьютеры, последующая рассылка фальшивых инструкций, в том числе адресованных экипажам в полете, может привести к огромным бедам. Пока этого не произошло, но исключать подобное развитие в будущем никто из специалистов не решается.

Одновременно нельзя забывать и о менее технологичных способах создавать угрозы воздушному сообщению. Простое отключение электросети в Чикагском аэропорту в сентябре 2014 года, вызванное кибератакой, привело к настоящему хаосу в диспетчерской службе, контролирующей полеты.

По каким признакам можно опознать потенциального террориста-смертника

Этой актуальной теме посвящена статья в декабрьском выпуске за 2015 год журнала Security Magazine. Ее автор, Микаел Джипс, опирается на реальные факты обнаружения террористов по внешним признакам в Израиле и других странах.

Язык жестов и телодвижений (body language)

Охранник в тель-авивском баре, часто посещаемом иностранцами, Ави Табиб обратил внимание на подозрительное поведение молодого человека, тщательно прячущего от него свое лицо. Тот всякий раз стремился отвернуться, когда сотрудник по безопасности обращал на него свой взгляд. Охранник решил подойти к незнакомцу, но тот поспешил к выходу. Как позднее вспоминал Табиб, его фигура была явно напряжена, движения характеризовались нервозностью, глаза выражали обеспокоенность и тревогу. Почуяв недоброе, охранник попытался вытолкнуть подозрительного субъекта из переполненного посетителями бара, но тот увернулся и бросился назад в ресторан. Охранник схватил его за бедро и в этот момент прогремел взрыв, унесший жизни смертника, оказавшегося поблизости официанта и еще двух человек. Сам охранник чудесным образом был только ранен.

Одежда

Михаил Саркисов, российского происхождения и в прошлом служивший в российской армии и полиции, душным летним вечером находился в небольшом кафе в центре Тель-Авива, неподалеку от посольства США, когда обратил внимание на странную одежду одного из посетителей. Несмотря на жару, тот был одет в свободную куртку из плотного материала и шорты ниже колен. Когда Саркисов подошел к нему, незнакомец сунул руку в карман куртки. Саркисов попытался схватить за руку, но тот вырвался и выбежал на улицу. Саркисов рванул за ним с криком «держи террориста!». Дежурившие рядом с американским посольством полицейские помогли задержать парня, действительно оказавшегося террористом, но не сумевшего или не успевшего привести в действие бомбу.

Поведение

В лобби фешенебельного отеля JW Marriott в столице Индонезии Джакарте 18-летний юноша катил чемодан в направлении группы бизнесменов, собиравшихся на завтрак перед конференцией. Охранников насторожил вид и поведение юноши – он словно ничего не замечал вокруг и исступленно смотрел впереди себя. Его остановили. Он сказал, что направляется к своему боссу. «Кто твой босс? Как его фамилия?». Спустя мгновение прогремел взрыв, унесший 6 человек и ранивший десятки.

Странные обстоятельства

Зачем бедной ирландской гостиничной горничной, к тому же беременной, покупать в последнюю перед посадкой минуту билет из Лондона до Тель-Авива и лететь к тому же одной? Этим вопросом озаботилась служба безопасности израильской авиакомпании El AL. Еще больше офицеры по безопасности насторожились, когда услышали от молодой, весьма скромно одетой женщины, что в Тель-Авиве она собирается остановиться в дорогущем Хилтоне, где ее ждет некий иорданец. Тщательный обыск личных вещей помог обнаружить полтора килограмма пластичного взрывчатого вещества, достаточного, чтобы взорвать авиалайнер.

Подозрительные документы

На границе между Канадой и США задержан некий молодой человек, предъявивший служащему таможни поддельное водительское удостоверение. При обыске у него нашли еще одни права, с той же датой рождения, но на другое имя. Дальнейшее расследование показало, что задержанный оказался террористом и планировал взорвать бомбу в международном аэропорту Лос-Анджелеса.

Согласно исследованию Чикагского университета, с 1982 года по май 2015 года в мире зафиксировано 4 568 попыток смертников взорвать себя и окружающих. Только в 2014 году таких попыток было 545. География этой категории терроризма не ограничивается традиционно высоко рискованными странами (Израиль, Ирак, Афганистан, Пакистан, Сирия). Смертники явно нацелились на Европу, считает эксперт Зорий Кор. С ним согласны практически все аналитики, указывающие на более чем вероятную перспективу возвращения в европейские страны боевиков террористических организаций, воюющих сегодня на Ближнем Востоке.

При этом важно отметить, что террористы совершенствуют технологии убийств, все активнее используют для этих целей интернет. Именно так, дистанционно, были подорваны две мечети в йеменской столице Сана, в результате чего погибли 142 прихожанина и сотни были ранены.

Автор статьи подчеркивает, что наибольший опыт успешного противостояния терроризму накоплен в Израиле. Этот опыт может и должен быть использован другими странами.

Корпоративная безопасность требует фундаментального переосмысления в

свете террористических угроз

Так утверждает журналист и эксперт Билл Удел, делясь своими размышлениями относительно последствий терактов в Париже на сайте Forbes.com.

Он напоминает, что нью-йоркская трагедия 9/11, а также террористические акции в Мадриде и Лондоне уже заставили корпоративные службы безопасности внести существенные коррективы в собственные планы и программы. В частности, особое внимание стало уделяться охране здоровья и жизни сотрудников компаний, работающих или направляющихся в зоны повышенной террористической опасности. Однако все эти меры имели количественный, а не качественно иной характер. Так, например, резко сократилось число деловых поездок в страны Ближнего Востока и Западной Африки. После парижских акций отмечается падение потока приезжающих из Америки и в европейские страны.

Последние события, демонстрирующие активизацию терроризма по всему миру, заставляют заново осмыслить те действия, которые предпринимают службы безопасности для защиты бизнеса, имущества и персонала компаний.

Как же надо реагировать СБ на происходящее? На чем сосредоточить внимание в среднесрочной и долгосрочной перспективе?

Мониторинг угроз и рисков

Исламское государство продемонстрировало свое стремление расширять список объектов для террористических атак и географически, и по сферам деловой и общественной жизни. А это требует от офицеров по корпоративной безопасности пересмотреть методологию и стандарты оценки угроз, расширить перечень рисков, которые необходимо ежедневно отслеживать. Уровень и характер вносимых корректив всецело зависит от служб безопасности, учитывающих отраслевой профиль компаний, их географическое месторасположение, число и состав персонала. Сегодня для отслеживания террористических угроз достаточно информации, доступны изощренные технологии поиска и анализа данных. Пренебрежение имеющимися гигантскими возможностями мониторинга рисков ложится тяжелой ответственностью на СБ и топ-менеджмент за возможные трагедии.

Управление рисками

Здесь корпорациям необходимо внимательно присмотреться к вопросам защиты менеджеров во время зарубежных поездок. Прежде всего, подвергнуть инвентаризации технические средства сопровождения и отслеживания (tracking), а также пересмотреть планы обеспечения безопасности сотрудников компании в деловых поездках в сторону ужесточения мер и требований безопасности. Главное – всеминутно знать, где командированный находится, поддерживать непрерывную связь, вовремя сообщать о грозящей опасности. Когда задействованы все доступные механизмы защиты, следует вновь оценить, можно ли сократить число поездок без ущерба для бизнеса, особенно в регионы повышенной опасности. Кроме того, перед каждой поездкой с работниками надо проводить консультации и тренинги.

Расширение функции безопасности в деятельности компаний

Речь идет о том, чтобы усиливать меры защиты от террористических угроз на тех территориях, в тех зданиях и помещениях корпорации, которые до недавнего времени считались относительно безопасными. Необходимо повышать роль СБ в обустройстве новых помещений, в проведении регулярных бэкграундных проверок не только при заполнении вакансий, но и работающего персонала.

Программы поддержания устойчивости и выживаемости бизнеса (resilience programs)

Планы работы в чрезвычайных обстоятельствах, в том числе и вызванных террористическими актами, сегодня имеются у большинства компаний. Проблема в том, что эти планы не тестируются, годами не корректируются. Эксперты призывают руководителей компаний и их службы безопасности посмотреть на эти планы свежим взглядом, уточнить, усилить предлагаемые действия в форс-мажорных условиях (например, план эвакуации), а главное – протестировать программы на предмет их эффективности.

Как защитить бизнес и персонал компаний на Ближнем Востоке и в Западной Африке?

Несмотря на террористическую активность и вооруженные действия в этих двух регионах, они остаются привлекательными для международного бизнеса, который продолжает работу в неблагоприятных геополитических условиях.

Реально опасная, порой просто враждебная обстановка требует нетривиальных мер безопасности. И в первую очередь, советуют эксперты, надо обратить внимание на систему управления рисками. Конкретно рекомендуют:

Идентифицировать и анализировать угрозы и неопределенности, способные реально и потенциально нанести ущерб, в форме еженедельно распространяемого графика с выделением приоритетов. Особенно важно иметь допуск к надежным и проверенным ресурсам информации, которые бы обеспечивали высокий уровень достоверности выводов и прогнозов.

Измерять уровень террористических угроз путем обнаружения и сравнения уязвимостей системы безопасности с рисками. Определять степень вероятности реализации угроз, сопоставляя их с оценками потенциального воздействия на операционные, стратегические и репутационные аспекты деятельности компании.

Разрабатывать план конкретных действий, направленных на минимизацию или, что еще лучше, на предотвращение угроз бизнесу. Планы должны расписывать, что практически делать и кто будет выполнять.

Формировать в коллективе такой климат, такую корпоративную культуру, которая бы помогала переносить стресс, способствовала бы сохранению дисциплины и выдержки в трудные часы.

Диверсифицировать функции по реализации программы действий в форс-мажорных

обстоятельствах по вертикали и горизонтали, чтобы даже при разрушительных последствиях инцидента безопасности (каковым может быть террористическая атака или взрыв бомбы) на всех уровнях менеджмента принимались бы правильные решения, и каждый бы действовал по инструкции в зависимости от складывающейся ситуации.

Заранее наладить связи с партнерскими организациями, способными в трудную минуту оказать организационную и иную необходимую поддержку.

Предусмотреть избыточность (redundancy) операционных и управленческих систем (дублирование, резервирование) для минимизации ущерба, если что-то пойдет не так.

Тренинги, тренинги, тренинги!

В процессе кризисного управления важно поддерживать максимально тесные связи и взаимодействие с владельцами/акционерами бизнеса, что поможет устранить недоразумения и конфликты между ними и менеджментом.

Как частный бизнес может способствовать международной стабильности?

Ответ на этот вопрос пытаются найти авторы публикации А. Касперсен и И. де Сола на сайте agenda.weforum.org (October 8, 2015), рассматривая деятельность западных корпораций в регионах и странах, характеризуемых политической нестабильностью и высокими рисками терроризма.

Они отмечают, что бизнес не может здесь заменить государство, но вместе с обществом способен содействовать формированию климата, в котором борьба правительства с терроризмом будет более эффективной.

Бизнесмены понимают опасности, таящиеся сегодня в ландшафте международной безопасности. Согласно последним исследованиям, три четверти опрошенных топ менеджеров и владельцев бизнеса называют «геополитическую нестабильность» угрозой номер один для глобального роста. Но еще многие компании плохо представляют себе, как надо отвечать на эту угрозу. Разные подразделения внутри одной бизнес структуры зачастую имеют собственные, неодинаковые приоритеты, по-разному понимают и подходят к вопросам управления рисками. Перед руководителями компаний нередко стоит выбор между потенциальными прибылями и безопасностью.

На практике многие транснациональные компании вынуждены иметь дело с явлениями, которые лежат в основе мировой нестабильности – коррупцией, бедностью, неэффективным государством, разрывом между потребностями современной экономики и низкой квалификацией рабочей силы в развивающихся странах. Содействуя искоренению бед, например, обучая рабочих, заботясь о снижении загрязнения окружающей среды, помогая местным властям решать те или иные социальные задачи, корпорации вносят свой вклад в борьбу за международную стабильность.

Эффективность такой деятельности многократно умножается через разновидности партнерства – между компаниями и отраслями, местными властями, общественностью. Разумеется, активизация в этом направлении требует времени, денег, опыта и знаний. Необходимы новые модели партнерства, опирающиеся на общие интересы, ясные ожидания и доверие.

Именно взаимное доверие чаще всего недооценивается, подчеркивают авторы публикации. Чтобы преодолеть этот феномен, корпорациям следует придавать больше прозрачности своей деятельности в странах пребывания, чаще проводить аудиты и публиковать результаты в местной прессе.

Перестройка требуется, прежде всего, в умах бизнесменов, в поиске новых подходов и решений. К примеру, что делать, сталкиваясь с фактами вымогательства и шантажа со стороны местных партнеров по бизнесу? Как проводить вынужденные увольнения и сокращения, не вызывая раздражения среди местного населения? Как реагировать на возможные протесты и волнения, обеспечивая защиту и безопасность персонала? Как сохранять в условиях политической нестабильности хорошие отношения с местной общественностью? Как охранять права личности своих клиентов (privacy) в случае хакерского взлома корпоративных сетей и необходимости обращаться за помощью к местным специалистам по кибербезопасности? Подобных вопросов множество.

Тем не менее, новые формы партнерства постепенно пробивают себе дорогу. Например, в Колумбии американские компании, действующие в районах высокой нестабильности, успешно налаживают взаимодействие с местными силовиками. В Африке многие западные фирмы приняли на вооружение стратегию «be local» - адаптацию под местные условия, в частности, путем передачи части акций по разработке месторождений местному бизнесу.

И такие примеры можно продолжать.

Рецензия

The Business of Counterterrorism: Public-Private Partnerships in Homeland Security.
By Nathan E. Busch and Austen D. Givens.
Peter Lang International Academic Publishers; peterlang.com; 342 pages. $29.95

Авторы книги анализируют пять основных сфер национальной безопасности:

1. Защита критически важной инфраструктуры

2. Кибербезопасность

3. Обмен информацией

4. Защита границ

5. Защита от природных катаклизмов и стихийных бедствий

Авторы признают, что этими вопросами не покрывается весь спектр национальной

безопасности, однако они играют важнейшую роль, все еще недооцененную теоретиками и практиками безопасности. Свою задачу они как раз видят в том, чтобы преодолеть инерционность в подходе к обеспечению безопасности перечисленных сфер деятельности на основе развития частно-государственного партнерства. .

Наряду с анализом и выводами авторы книги предлагают свои рекомендации и провоцируют дальнейшее исследование этих проблем. Так, в частности, касаясь защиты критически важной инфраструктуры, они ставят, но не торопятся ответить на следующий вопрос: какие метрики годятся для измерения эффективности частно-государственного партнерства? Подумать предлагается самим читателям.

Главными недостатками частно-государственного партнерства в обеспечении национальной безопасности авторы считают:

- просчеты регулирования

- ошибки управления

- недостаточные бюджеты

- подстрекательство к войнам и конфликтам.

Рецензия

The Business of Counterterrorism: Public-Private Partnerships in Homeland Security.
By Nathan E. Busch and Austen D. Givens.
Peter Lang International Academic Publishers; peterlang.com; 342 pages. $29.95

Авторы книги анализируют пять основных сфер национальной безопасности:

1. Защита критически важной инфраструктуры

2. Кибербезопасность

3. Обмен информацией

4. Защита границ

5. Защита от природных катаклизмов и стихийных бедствий

Авторы признают, что этими вопросами не покрывается весь спектр национальной безопасности, однако они играют важнейшую роль, все еще недооцененную теоретиками и практиками безопасности. Свою задачу они как раз видят в том, чтобы преодолеть инерционность в подходе к обеспечению безопасности перечисленных сфер деятельности на основе развития частно-государственного партнерства. .

Наряду с анализом и выводами авторы книги предлагают свои рекомендации и провоцируют дальнейшее исследование этих проблем. Так, в частности, касаясь защиты критически важной инфраструктуры, они ставят, но не торопятся ответить на

следующий вопрос: какие метрики годятся для измерения эффективности частно-государственного партнерства? Подумать предлагается самим читателям.

Главными недостатками частно-государственного партнерства в обеспечении национальной безопасности авторы считают:

- просчеты регулирования

- ошибки управления

- недостаточные бюджеты

- подстрекательство к войнам и конфликтам.

Кибербезопасность

Второй год подряд «Security 500 members» называет киберугрозы проблемой номер один для корпоративных служб безопасности. 2015 год, по мнению экспертов, еще более сложный с этой точки зрения, чем предыдущий.

Исследовательская организация Ponemon Institute пришла к выводу, что каждый зафиксированный взлом стоит компаниям в среднем $145, причем в Германии урон достигает $201, в США $195, в Индии $51.

Ликвидация последствий успешной кибератаки занимает в среднем 46 дней, больше, чем в 2014 году и стоит дороже на 22%.

Наибольший материальный ущерб наносят кражи корпоративной информации. Их последствия для бизнеса подчас разрушительны. Потери в производительности от хакерских атак в 2015 году на 5% больше средней цифры за предшествующие несколько лет.

Особенно страдает малый бизнес, который либо не имеет достаточных ресурсов для защиты, либо пребывает в уверенности, что «не представляет интереса» для киберпреступников.

Перед лицом растущих киберугроз компании увеличивают расходы на информационную защиту, а также на страхование от потенциального ущерба. Все больше организаций обращаются к новейшим технологиям, к продвинутым средствам аутентификации, показывает исследование, проведенное PwC.

Исследования также демонстрируют возрастающую роль топ-менеджмента в организации защиты от хакерских атак. 45% крупных компаний имеют сегодня штатную единицу Главного офицера по информационной безопасности (Chief Information Security Officer). Согласно последним опросам, во многих компаниях отмечается активное вовлечение совета директоров в обсуждение и решение вопросов финансирования и кадрового укрепления службы информационной защиты.

Борьба с хищениями

Согласно последнему исследованию 2015 Hiscox Embezzlement Watchlist: a Snapshot of Employee Theft in USA, американские компании с числом занятых менее 500 человек за последний год понесли потери от хищений, измеряемые средней цифрой $280 000. Хищения, осуществляемые главным образом собственным персоналом, отнюдь не проблема одних только крупных корпораций и финансовых институтов. 80% жертв таких преступлений – компании численностью менее 100 человек. Причем кражи характерны практически для всех отраслей экономики и бизнеса. В большей или меньшей мере.

Как показывают экспертные оценки, хищения чаще совершаются сотрудниками, имеющими солидный стаж работы в компании. Более 60% злоумышленников - женщины. Более 50% преступников не имеют прямого отношения к финансам и бухгалтерии. 21% преступлений совершается теми, кто по работе связан с денежными потоками, работает в банках, кредитных союзах, страховых компаниях.

Усредненный размер ущерба от воровства в финансовых организациях составляет $271 000. Наиболее серьезный урон наносится торговле и системе здравоохранения – в среднем $606 000 и $446 000 соответственно. Далее следуют некоммерческие организации ($201 775), муниципалитеты ($293 717), профсоюзы ($41 599).

Если брать только розничную торговлю, то убытки от хищений в 2015 году превышают 60 миллиардов долларов в год только в США. На три миллиарда больше, чем в 2014 году. При этом размер хищений собственными работниками в 6 раз превышает ущерб от магазинных воришек.

Чтобы сократить гигантские убытки, законодатели на федеральном и региональном уровнях идут навстречу пожеланиям бизнесменов по ряду вопросов. Например, в штате Техас принят закон, разрешающий предпринимателям сканировать и хранить определенное время персональную информацию клиентов, направлять ее в организации, призванные бороться с мошенничеством.

Технологии безопасности

Главная тенденция в этой области – интеграция технологий на основе сбора и анализа множества данных, которые на выходе превращаются в практически полезную информацию.

Главные на сегодняшний день технологические инструменты – «облачные» исчисления, цифровое видеонаблюдение, средства опознания по лицу, PSIM (решения, предназначенные для «управления обменом данными в системах физической безопасности» - physical security information management), системы датчиков, фиксирующие несанкционированные вторжения по периметру безопасности.

Все эти системы интегрируются в единый сложный комплекс управления охраной и безопасностью организации.

Крупная страховая компания Aflac инвестировала немалые средства в создание такого интегрированного комплекса (цифровое видеонаблюдение + тревожная сигнализация + средства контроля доступа), который позволяет осуществлять мониторинг безопасности в офисах, расположенных в разных штатах, из одного центра. Вложения окупаются за счет радикального сокращения численности охранников, в частности, отпала необходимость патрулирования периметра безопасности. Кроме того, сочетание цифровых камер слежения и видеоаналитики с детекторами обнаружения обеспечивает оператору мониторинга одномоментный доступ к информации в режиме реального времени, когда происходит инцидент безопасности.

Таких интегрированных систем становится все больше. Обладание ими уже не исключительная прерогатива крупных, богатых корпораций. Массовый выпуск содействует их удешевлению. И к ним все более внимательно присматривается средний и малый бизнес.

Стандарты и требования к бизнесу в сфере управления рисками

В результате финансового кризиса, последствия которого дают о себе знать в мировой экономике и по настоящее время, бизнесмены стали больше внимания уделять вопросам анализа и управления рисками. Как отмечается в докладе компании Ernst&Young 2015 Governance, Risk and Compliance, «руководители корпоративной безопасности и менеджеры по управлению рисками играют возрастающую роль в осмыслении внутренней и внешней среды, генерирующей риски для бизнеса, в разработке и реализации соответствующих политик и процедур, нацеленных на минимизацию рисков. Более, чем когда либо этими вопросами занимаются не только специалисты, но и советы директоров, первые лица компаний».

Этому способствует наблюдаемое во многих странах ужесточение контроля и мер регулирования частного бизнеса. Оно касается в первую очередь вопросов, связанных с обнаружением и минимизацией рисков. Так, в частности, в США и ряде других стран от организаций требуют внедрения более строгих стандартов ведения бухгалтерии и финансовой отчетности. Нарушения стандартов наказываются штрафами и разнообразными санкциями. Одним из обоснований жесткого подхода к бизнесу со стороны госорганов и отраслевых объединений в развитых странах служит продолжающаяся тенденция вывода производства и услуг в регионы с развивающимися экономиками, что, по мнению экономистов и экспертов, чревато новыми рисками.

В США Комитет организаций–спонсоров Комиссии Тредвея (COSO – добровольная частная организация, разрабатывающая рекомендации для корпоративного руководства по важнейшим аспектам организационного управления, деловой этики, финансовой отчетности, внутреннего контроля, управления рисками) сформулировал и внедряет 187 принципов ведения бизнеса.

На лондонской Stock Exchange корпорации, вошедшие в премиальный список, должны отчитываться, как они соблюдают ключевой для бизнеса документ – UK Corporate Governance Code. Аналогичное правило принято в ЕС, Гонконге, в некоторых других

регионах.

Но ситуация не такая безоблачная, как она выглядит в официальных документах. Говорит Рик Мейзон (компания Honeywell - разработки в области аэрокосмического оборудования, технологий для эксплуатации зданий и промышленных сооружений, автомобильного оборудования, турбокомпрессоров и специализированных товаров): «Мне кажется, что многие компании попадают в собственную ловушку, будучи уверенными, что у них все в порядке с выполнением требований регуляторов по управлению рисками. При этом они ссылаются на сертификаты, выданные регуляторами. Но это минимум, что надо делать на самом деле. Одно дело – бумаги. Другое – реальное следование установленным стандартам, позволяющее минимизировать угрозы и риски, быстро на них реагировать, повышать уровень защиты и безопасности бизнеса. Это вполне осуществимо, если вопросы корпоративной безопасности интегрированы в ткань бизнеса, а не являются вывеской для отвода глаз» (Security Management, November 2015).

Насилие на рабочих местах

Несмотря на внимание бизнеса, государственных органов, общественных организаций к корпоративным инструкциям и правилам поведения служащих, рабочих, учащихся, несмотря на внедрение продвинутых программ контроля за доступом и новейших средств идентификации, уровень насилия на рабочих местах (workplace violence) возрастает, отмечают западные эксперты.

Такой рост особенно характерен на примере США, где в 2015 году отмечены полторы сотни кровавых инцидентов с применением огнестрельного оружия, в результате которых десятки убитых и сотни раненых.

Согласно американскому институту National Institute for the Prevention of Workplace Violence, каждый инцидент насилия, в результате которого имеются жертвы, обходится организации в немалую сумму от $250 000 до одного миллиона долларов с учетом всех последующих расходов. Средняя стоимость судебного процесса приближается к $500 000, а решения судей о штрафах и компенсациях выливаются в среднюю цифру порядка $3 миллионов (в некоторых случаях цифра возрастает до более, чем $5 миллионов). Это только потери материальные. Здесь не учитывается репутационный ущерб, который трудно измерить точной суммой.

Следует отметить, что фактами насилия на рабочих местах охвачены практически все отрасли экономики, бизнеса и общественной жизни. Говорит Барри Никсон из упомянутого выше института: «Большинство специалистов сходятся во мнении, что крупные инциденты насилия вполне можно предотвращать с помощью четко сформулированных и внедренных программ. Но даже если компания предпринимает все мыслимые и немыслимые усилия по недопущению насилия, мы все же не можем точно предсказать, где, кто и когда взорвет ситуацию. Тем не менее, службы безопасности обязаны готовиться к чрезвычайным происшествиям, заблаговременно разрабатывать планы мер, которые бы учитывали всевозможные варианты развития ситуации. Такая работа сравнима с игрой в кости: известно, какие цифры могут выпасть, но неизвестно, какие именно» (Security Magazine, November Issue).

Никсон советует иметь в наличии план действий, охватывающий пять важнейших с

точки зрения защиты объектов: помещения и имущество, технологии, информация, корпоративные сети, люди. Разработку плана надо начинать с анализа потенциальных угроз для всех этих объектов и потенциального воздействия реализованных угроз на процессы бизнеса. То есть речь идет об оценке рисков и осмыслении, что можно и следует делать для предотвращения и минимизации ущерба. На финальной стадии работы важно подключить финансовых аналитиков, которые бы просчитали потенциальный урон для компании.

Важнейшую роль в предотвращении фактов насилия (включая учебные заведения) играют СКУД. «Мы используем электронную систему контроля доступа, которая фиксирует и регистрирует каждого, кто приходит в школу, - говорит Крис Уинн, директор по безопасности окружного управления школ Val Verde. - Система держит под замком все входные и внутренние двери в часы, когда идут занятия, управляет ими на протяжении всего учебного времени» (там же).

Серьезно проблемой насилия занимаются в компании Schneider National. «Насилие на рабочих местах представляет собой растущую угрозу для бизнеса - отмечает директор службы безопасности компании Уолт Фонтейн. - Мы почти ежедневно занимаемся этими вещами. В результате удалось сформировать в компании такой климат, когда работники чувствуют себя комфортабельно на своих рабочих местах, зная, куда и к кому надо обращаться при первых признаках возможного инцидента. Мы постоянно проводим встречи с коллегами, персоналом, совместно обсуждаем обстановку, рабочие процессы, происходящие в компании» (там же).

Бюджет и финансы

Решение проблемы предупреждения насилия во многом обусловлено финансовой политикой в компаниях. К примеру, недавний опрос, проведенный экспертами по безопасности, показал, что кампусы американских учебных заведений в подавляющем большинстве не защищены надлежащим образом от потенциальных киллеров. И вопрос упирается главным образом в бюджетные ограничения.

По результатам опроса, проведенного Margolis Healy (американская компания, предлагающая услуги в сфере обеспечения безопасности высших учебных заведений), обнаружилось, что 25% руководителей из 513 вузов вообще не задумывались о мерах предотвращения убийств на территории кампуса. Причина? Отсутствие средств. Нехватка денег остается проблемой для всех корпоративных служб безопасности, в каких бы отраслях экономики и бизнеса они не находились. Она проще решается для крупных корпораций. Например, более половины компаний, входящих в список Security 500 members, увеличили за последний год расходы на безопасность. Еще 30% оставили прежнюю цифру в данной статье бюджета. А 13% вынуждены пойти на финансовое сокращение.

Отношение к расходам на безопасность определяется тем, насколько первые лица, от которых зависят решения, понимают значение работы по анализу и снижению рисков для бизнеса. А важность такой работы вполне возможно проиллюстрировать в реальных цифрах, характеризующих потенциальные потери от недооценки рисков и угроз при помощи различных метрик и методологий.

Крупный бизнес осознает грозящие ему опасности и идет на увеличение расходов.

Службы безопасности в корпорациях привлекаются к управлению бизнес рисками, к подготовке предложений по их минимизации, к работе с клиентами, партнерами и поставщиками. Особенно важно для работников СБ налаживание прямых связей с бизнес клиентами своих компаний для выяснении их потребностей и опасений, связанных с безопасностью предлагаемых им услуг/продуктов. Полученные в результате контактов данные и сведения затем трансформируются в конкретные планы и проекты по безопасности, представляемые на утверждение и финансирование топ-менеджменту. Это один из самых эффективных путей укрепления материального фундамента СБ в корпорациях, полагают эксперты.

Приглашенный несколько лет назад для проведения всеобъемлющего аудита, разработки и руководства программой безопасности в университете High Point University специалист Джефф Карпович, столкнулся с серьезной дилеммой: «Все просто: если университет хочет иметь программу, которой можно гордиться, которая действительно эффективно обеспечивает безопасность и защиту, то надо вкладывать дополнительные средства. Но если в этом вопросе нет надлежащей поддержки со стороны университетской администрации, со стороны президента вуза, то сделать нечто реальное просто невозможно» (Security Magazine, November Issue).

К счастью Карпович получил все, на что он надеялся. Университет изыскал требуемые средства. Ему удалось увеличить штат СБ в десять раз – с 12 до 120, и на протяжении последних лет кардинально уменьшить статистику инцидентов безопасности на территории университета.

Обеспечение непрерывности ведения бизнеса в условиях стихийных бедствий

От стихийных бедствий особенно страдает бизнес американского континента. Но при этом многие компании в США и других странах Северной и Южной Америки, составляя планы непрерывности ведения бизнеса (business continuity), не ограничиваются мерами снижения ущерба от природных катаклизмов, но включают в эти планы все потенциальные риски, чреватые прекращением либо серьезными нарушениями бизнес процессов.

Придание работе компании устойчивости даже в форс-мажорных обстоятельствах уже не является больше просто хорошей практикой. Это нечто большее, охватывающее отношения организации со своими работниками, клиентами и партнерами. Семь лет назад в США насчитывалось 77% компаний, которые имели документированные планы непрерывности ведения бизнеса. В 2015 году число таких компаний достигло 93%.

Сегодня органы регулирования в США требуют от организаций быть готовыми встретить чрезвычайные ситуации, иметь соответствующие планы действий. Все чаще такие требования выдвигаются и самими организациями к клиентам, партнерам и партнерам партнеров.

Компании нередко предусматривают множество технических и технологических мер, таких, например, как перевод интернет систем на альтернативные сайты в случае

вынужденной необходимости. Однако, зачастую игнорируют или недооценивают человеческий фактор и проблему коммуникации в условиях форс-мажорных.

Сегодня большинство компаний широко практикуют удаленный доступ в корпоративные сети. Многие организации автоматизировали этот процесс. Но немало и тех, кто по старинке пользуется для внутренних связей электронной почтой, а то и социальными сетями. А это чревато утечками и потерей коммуникации со своими сотрудниками при чрезвычайных обстоятельствах, когда организации могут остаться на время без интернета.

Важнейший фактор гибкости и выживаемости бизнеса заключается в обучении персонала, в программах тренинга. Директор по безопасности ADP (услуги облачного аутсорсинга, включая финансы и работу с кадрами) Рональд Клаутиер замечает, что всегда может что-то произойти, влияющее на бизнес - будь то изменчивая погода, политические или иные события. Поэтому так важно фокусировать внимание на готовности встретить любую напасть во всеоружии, не дав бизнесу развалиться или понести серьезные потери. С активным участием службы безопасности в ADP сформирована команда кризисного управления, которая осуществляет планирование действий в условиях кризиса, готова взять на себя управление в чрезвычайной ситуации и в дальнейшем восстановление бизнес процессов.

Работа с кадрами

В последнее время набирает силу тенденция формирования корпоративных служб безопасности такими офицерами, которые бы отличались не столько менталитетом силовика, сколько умением анализировать риски для бизнеса компании и соответственно реагировать на них.

Такая же тенденция характерна и для учебных центров. Там наряду с обычными курсами охранного дела (СКУД, охрана помещений и имущества, аудиты безопасности и пр.) внедряются программы по подготовке специалистов, способных также разбираться в бизнесе, в сферах маркетинга, материального снабжения, инженерного дела…Но, конечно, не за счет, а в дополнение к традиционным дисциплинам.

Тренинги особенно важны для тех сотрудников СБ, которые наделены правом носить и применять служебное оружие. Этому вопросу уделяется первостепенное внимание в компании Nationwide Insurance (одна из крупнейших в США страховых и финансовых корпораций). Регулярно проводимые с охранниками и офицерами занятия включают имитационные игры, в ходе которых надо принимать нетривиальные решения, проработку ролевых сценариев, учебную стрельбу по мишеням, использование нелетальных средств защиты от злоумышленников.

Важную роль играет регулярное тестирование квалификации сотрудников СБ. Практикующий специалист по корпоративной безопасности Дональд Пейзант отмечает, что «грандиозные планы выглядят такими зачастую лишь на бумаге». А как они работают, можно выяснить только тестированием систем охраны и тех, кто их обслуживает. В ходе учений с охранниками, в основном из гостиничной отрасли, представители учебного центра, которым руководит Пейзант, организуют попытки несанкционированного проникновения в те помещения отелей, куда посторонним вход воспрещен, а также незаконного проноса ножей и огнестрельного оружия.

Еще одна характерная тенденция - обучение сотрудников СБ помимо прямых их профессиональных обязанностей работе с клиентами компании, взаимодействию с ними. Так обстоит дело, например, в детском госпитале города Сиэтл. На тренингах охранникам внушают, что они должны проявлять особое внимание к родителям и родственникам, посещающим больных детей, помогать, успокаивать и утешать их, если в этом есть необходимость. Охранников учат вежливости, предупредительности, учтивости, этикету, умению сохранять спокойствие и выдержку в трудных ситуациях, связанных с поведением посетителей.

Глобализация бизнеса и охрана персонала транснациональных корпораций

2015 год отмечен продолжением процессов глобализации бизнеса, охватывающих практически все континенты. Операции компаний западных стран расширились в Азии на 8%, в Южной Америке – на 6%.

Особенно активно распространяют по миру свои услуги и продукты финансовые организации. По некоторым прогнозам, к 2030 году сектор финансовых услуг в Китае, Нигерии и Индии создаст больше рабочих мест, чем в Великобритании, признанном финансовом центре мира.

По последнему опросу, проведенному Chubb Multinational Risk Syrvey, более половины крупных компаний планируют и осуществляют экспансию в другие страны и регионы, 26% увеличивают свой зарубежный персонал, 27% увеличивают количество командировок своих работников.

С другой стороны, ряд важных для бизнеса регионов подвергаются политической турбулентности. Это в первую очередь касается Ближнего Востока и Северно-Западной Африки. Именно отсюда исходит главная угроза международного терроризма. Но парадокс: авторитетные экспертные сообщества, среди них МВФ, прогнозируют, что этот нестабильный регион в течение ближайших пяти лет будет занимать третье место в мире по темпам экономического развития, по привлекательности потребительского рынка, самого молодого и быстро растущего.

Все эти обстоятельства требуют от корпоративных служб безопасности повышенного внимания к защите здоровья и жизни персонала, работающего или выезжающего в командировки в нестабильные регионы. Естественно, адекватный ответ на новые вызовы требует дополнительных, и немалых, средств. Однако, эксперты подсчитали, что производительные и репутационные потери от инцидентов с работниками, выезжающими за рубеж, намного превосходят вложения в их безопасность.

Компании обязаны заранее продумывать и разрабатывать программы защиты людей, охватывающие не только сотрудников центральных подразделений, находящихся в разъездах, но и местных работников в зарубежных отделениях и филиалах, и экспатриантов. Эти программы должны учитывать многие обстоятельства, связанные с работой людей вдали от центральных офисов. Ключевой момент – предусмотренная заранее возможность немедленно определить местонахождение и связаться с

сотрудником в минуту опасности.

Если инцидент случается и печально заканчивается по вине самой организации, то она несет судебную ответственность. Так обстоит дело во многих странах, включая США. Журнал Security Magazine (ноябрьский выпуск) приводит свежий пример. Суд штата Коннектикут присудил $41 миллион школьнику, подвергнувшемуся жестокому избиению с нанесением тяжких травм во время поездки в Китай, которую организовала и спонсировала школа, где он учился. Правда, администрация школы подала апелляцию, которая сейчас рассматривается.

Эксперты советуют службам безопасности при планировании командировок, особенно в неспокойные регионы, привлекать к этой работе самих командированных, обговаривая с ними все необходимые детали. При этом важно, чтобы все стороны проявляли здравый смысл, избегая по возможности ненужного риска.