Охрана предприятия

№ 2 (95) 2025

Оглавление

Специалист по борьбе с отмыванием денег: задачи и функции

Эксперты Financial Crime Academy, одной из ведущих на Западе научно-исследовательских организаций в области борьбы с финансовыми преступлениями, так формулируют специальность AML (Anti-Money Laundering): «Специалисты AML это профессионалы, отвечающие за соблюдение компанией нормативно-правового соответствия в сфере противодействия отмыванию денег. Они играют критически важную роль в обнаружении, предотвращении и информировании подозрительной активности, которая может указывать на отмывание денег, финансирование терроризма, другие незаконные финансовые операции» (financialcrimeacademy.org/aml-officer-job/).

Основные обязанности специалиста AML

Разработка и контроль программы AML комплаенс

Мониторинг и информирование о подозрительной активности в финансовых транзакциях

Организация и проведение финансовых расследований и внутренних аудитов

Квалификация и компетенции, требуемые для специалиста AML

Высшее образование (минимум диплом бакалавра) в сфере финансов, бухгалтерского дела или смежной области

Опыт работы по этой специальности, как минимум, в течение нескольких лет

Знание нормативно-правовой базы AML, основ управления рисками, способов и приемов отмывания денег, методологии и стратегий анализа рисков

Аналитические способности и внимание к деталям финансовых документов, данным о транзакциях, профилям клиентов, что крайне необходимо для анализа сложных финансовых транзакций, фиксации аномалий, изучения признаков («красных флажков») преступления.

Роль специалиста AML постоянно эволюционирует соответственно тем изменениям, которые происходят в криминальном ландшафте. Эксперты называют главные аспекты этой эволюции:

Углубление компетенций в области технологий работы с данными. Речь идет в первую очередь о приобретении навыков использования искусственного интеллекта, машинного обучения для обработки и анализа массивов данных

Смещение фокуса на управление рисками в масштабах всей организации. Традиционной AML экспертизы сегодня уже недостаточно. От специалиста AML требуют более широкого подхода к анализу рисков

От них также требуется сосредоточить внимание на предотвращении финансовых преступлений (помимо реагирования).

Качественная, эффективная корпоративная программа борьбы с финансовыми преступлениями включает следующие элементы:

Внутренние политики, инструкции, процедуры

Регулярные занятия с персоналом организации по ознакомлению с рисками и угрозами

Комплексная проверка клиентов и партнеров, предусматривающая, в частности, идентификацию личности, сбор и анализ информации, в том числе транзакций

Мониторинг и оповещение о подозрительной активности

Внутренние аудиты и проверки

Ключевое значение приобретает тесное взаимодействие с другими подразделениями организации, включая службу IT, отдел информации, менеджера по вопросам комплаенс. Кроме того, постоянные контакты с регуляторами, органами правопорядка, коллегами по профессии дают хорошие возможности обмениваться информацией и лучшими практиками, быть в курсе последних тенденций, изменений в законодательстве и регулировании.

Занимая проактивную позицию в своей работе, непрерывно наращивая знания и умения, профессионалы по борьбе с отмыванием нелегальных денег способны принести огромную пользу

бизнесу, своевременно выявляя и предотвращая финансовые преступления, минимизируя риски и угрозы.

Отмывание «грязных» денег: какие тренды превалируют сегодня?

Согласно данным Управления ООН по наркотикам и преступности ежегодно отмывается от 2% до 5% мирового ВВП. Отмывочный ландшафт сегодня претерпевает заметные изменения, обусловленные геополитическими сдвигами, технологическим инновациями, повсеместным ужесточением законодательного регулирования.

Эксперты обращают внимание на тенденцию к увеличению числа таких преступлений. Несмотря на предпринимаемые государственными структурами и бизнесом попытки противодействовать, криминал довольно успешно находит и эксплуатирует лазейки, применяя все более изощренные способы отмывания.

Особо значимый рост инцидентов отмечается в области электронных денег, в первую очередь, криптовалюты, что объяснимо процессами ускоренной цифровизации финансовой сферы.

С другой стороны, в ряде стран наблюдается существенное усиление наказаний для организаций, замешанных в отмывочном процессе.

Базельский Институт управления (Basel Institute on Governance - швейцарская международная неправительственная организация, входящая в сеть «Программы Организации Объединённых Наций в области предупреждения преступности и уголовного правосудия»), опубликовал список стран с высокими рисками легализации грязных денег. Список возглавляет следующая десятка: Гаити, Чад, Мьянма, Демократическая Республика Конго, Республика Конго, Мозамбик, Габон, Гвинея-Бисау, Венесуэла.

Компания KYC Hub (управление рисками в финансовой сфере) дает любопытную статистику по ряду ведущих западных стран.

США

Министерство финансов выпустило объемистый документ под названием “2024 National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing». Он подтвердил статус США как страны с самым высоким показателем числа инцидентов на душу населения: три с половиной на 100 000 жителей. Каждый год отмывается примерно 300 миллиардов долларов или около четверти общемировой цифры. А налагаемые на правонарушителей штрафы составляют порядка 15 миллиардов долларов. Самый большой корпоративный штраф за всю историю заплатил в 2024 году TD Bank – 3 миллиарда (о скандале вокруг этого банка смотри статью «Впервые в истории США крупный банк признал участие в отмывании грязных денег» в выпуске журнала «Охрана предприятия» № 93).

Великобритания

В этой стране статистика дает цифру 2.5 инцидента на 100 тысяч поданных. На протяжении ряда последних лет правительство пытается сдержать рост финансовых преступлений. Последний по времени шаг в этом направлении был сделан осенью 2024 года, когда МИД объявил об очередной новой инициативе - усилении мер по выявлению незаконных финансовых потоков и борьбе с отмыванием иностранных денег. Для демонстрации «серьезных» намерений ввели санкции против украинского предпринимателя Фирташа.

Австралия

Здесь наркоторговля превратилась в основную прачечную с долей 40.9% от всех зафиксированных случаев отмывания грязных средств.

Канада

И Канада заняла «достойное» место в списке стран, где прачечные с каждым годом становятся всё активнее, невзирая на предпринимаемые государством меры противодействия с акцентом на верификацию UBO (действия, направленные на установление личности и законности конечных владельцев бизнеса, включая проверку личных данных). Рост случаев легализации особенно характерен для криптовалютных транзакций и сферы недвижимости.

Германия

Еще 10 лет назад журналисты называли Германию «раем для отмывания нелегальных денег». С тех пор мало что изменилось, несмотря на принятые законы, направленные на ужесточение контроля. Последний законопроект, внесенный на рассмотрение Бундестага летом 2024 года, предусматривает создание нового органа - «Центра расследования случаев отмывания денег», который бы занимался выявлением подозрительных финансовых потоков по методу «следуй за деньгами», напрямую приводящему к профессиональным организаторам и сетям. Но рассмотрение законопроекта было отложено из-за кризиса в правящей коалиции, до выборов, которые выиграл, как известно, блок ХДС/ХСС, и формирования нового правительства.

Чем обернулось нарушение антиотмывочного законодательства для американского банка Patriot National Bank?

Ответ: многомиллиоными убытками и принуждением к исправительным, восстановительным мерам.

Предоставляющий розничные и коммерческие банковские услуги Patriot National Bank (штат Коннектикут) был уличен Управлением валютного контроля Минфина США в осуществлении «опасной и порочной» практики, в частности, в нарушении антиотмывочного законодательства.

Банк и Управление валютного контроля подписали в начале 2025 года Соглашение, в соответствии с которым:

- Банк создает Compliance Committee (Комитет по соблюдению требований регуляторов) в составе трех членов, два из которых не работают в банке. Комитет должен разработать и внести в правление банка документ, содержащий перечень действий, необходимых для реализации каждого из пунктов Соглашения.

- Правлению банка поручено составить стратегический план исправительных мер на трехлетний период. В плане должны быть отражены задачи банка в отношении управления рисками, балансовых отчетов, забалансовых операций, структуры процентных ставок, финансовой устойчивости (capital and liquidity adequacy), разработки линеек продуктов, а также сегментов рынка, где банк планирует развиваться. Правление ежегодно будет рассматривать его реализацию и вносить по необходимости соответствующие коррективы.

- Правление разработает эффективную концепцию стратегического управления финансами. Банк должен достичь и поддерживать установленный властями минимальный уровень коэффициента достаточности капитала.

- Банк обязуется подготовить и представить в двухмесячный срок письменную программу управления рисками для новых и модифицированных продуктов и услуг, включающую политики и процедуры, связанные с анализом и оценкой рисков (risk assessment).

- Банк должен представить в письменной форме план действий по соблюдению свода законов и правил, принятых в США в целях борьбы с отмыванием денег и финансированием терроризма (BSA/AML Action Plan).

- Банк должен обеспечить идентификацию, управление и контроль рисков по операциям с предоплаченными банковскими картами.

- План мониторинга и Due Diligence (процесса, в рамках которого осуществляется тщательный анализ бизнеса или инвестиционной сделки, с целью получения достоверной информации о ее состоянии и возможных рисках) предполагает, что менеджеры программ будут зарегистрированы в Агентстве по борьбе с финансовыми преступлениями Минфина США, а их действия должны соответствовать требованиям местных лицензионных агентств.

- Постоянный мониторинг и тестирование рисков должно быть документировано надлежащим образом и покрывать все аспекты работы банка, включая предупреждение и предотвращение отмывания денег и других финансовых преступлений.

- Отдел по борьбе с отмыванием необходимо укомплектовать профессионально подготовленными операторами мониторинга в соответствии с политиками банка.

- Банк обязуется осуществлять строгий контроль политики Due Diligence в отношении программных менеджеров, предусмотрев, в частности, периодические проверки их работы на местах, ежегодный анализ выполнения программ и аудитов по борьбе с отмыванием денег и финансированием терроризма.

- Предусмотрена ежегодная проверка личных счетов программных менеджеров на предмет их сегрегированности (недопустимости смешивания личных счетов с капиталом банка) и прозрачности. Банку вменяется в обязанность иметь надлежащие процедуры и инструкции, предусматривающие закрытие счетов программного менеджера при появлении очевидных признаков риска, таких, к примеру, как отказ предоставить аудиторам требуемую финансовую информацию.

- Банк должен подготовить и представить Оверсайт платежных систем (Payment Activities Oversight Program) – программу мониторинга денежных переводов между банковскими счетами с целью идентификации и документирования сопряженной с высокими рисками и/или подозрительной, аномальной, необоснованной активности. Подобающая программа управления рисками должна включать отслеживание рисков, проистекающих от платежной активности, и обладать ключевыми индикаторами рисков. Кроме того, программа должна предусмотреть использование соответствующих метрик для ее измерения, управления, корректирования и оптимизации.

(по материалам веб-сайтов https://www.bankingdive.com, https://www.consumerfinancialserviceslawmonitor.com и ряда других ресурсов)

Как обмануть мошенников с помощью технологий Deception

Технологии обмана мошенников, получившие название Deception (обман, уловка, надувательство), появились сравнительно недавно и получают все большую популярность как инструмент обнаружения и предупреждения киберугроз.

Хакеров вычисляют по ловушкам, целям-приманкам или так называемым «горшочкам с медом» (honeypots). Ханипот это сетевой объект, единственная цель которого — привлекать злоумышленника и провоцировать его на атаку. Кроме этой задачи ханипот не имеет иной ценности в сети, в которой установлен; с ним не ведется никаких легитимных сетевых взаимодействий. Подвергаясь атаке, ханипот фиксирует ее и сохраняет характерные действия атакующего. В дальнейшем эти данные помогают проанализировать путь злоумышленника. Побочная цель — задержать продвижение атакующего по сети, заставив его потратить время на изучение ложного ресурса (подробнее см. https://habr.com/ru/companies/bastion/articles/680820/).

Чтобы поймать хакера, ловушки должны быть неотличимы от настоящих сервисов. Современные обманные технологии представляют сложные цифровые записи в форме соблазнительных приманок. У крупных организаций такие ловушки могут являть собой реальный, сложный по архитектуре продукт, содержащий липовые профили социальных сетей, фальшивую конфигурацию офиса, даже реальных людей, играющих роль менеджеров.

По мнению Синтии Брумфельд, аналитика в области коммуникационных технологий, инструментарий Deception не ограничивается созданием ловушек. Конечная цель - формирование целой среды, отвлекающей внимание и действия злоумышленников от действительных ценных активов, прежде всего, цифровых ресурсов организации.

Брумфельд цитирует экспертов американской компании Rapid7 (https://www.rapid7.com), характеризующих технологию Deception как «технологию обнаружения и реагирования на инциденты безопасности, призванную помогать службе безопасности выявлять, анализировать и выстраивать прочную защиту против изощренных киберугроз путем отвлечения хакеров на фальшивые IT ресурсы, которые размещаются внутри корпоративных сетей».

Сегодня цифровые обманные ловушки продаются в немалом ассортименте. Однако их производители и поставщики, полагает специалист по информатике Рассел Хэндорф, «возможно,

не задумываются о том, как в действительности готовится, запускается и реализуется операция Deception. Для ее успеха необходимо хорошо знать инфраструктуру компании, обладать компетенцией анализа данных. Но, главное, понимать, что Deception не просто ловушка. Это стратегия, требующая вдумчивого подхода, смелого и точного исполнения» (Chief Security Officer, January, 24, 2025).

Дипин Десаи, директор по исследованиям в компании Zscaler (решения облачной безопасности), сравнивает Deception с детекторами движения, неприметно размещенными в доме для предупреждения о несанкционированном проникновении.

Критически важный компонент Deception – внешнее правдоподобие. Даже если преступник, попавшийся на приманку, быстро распознает обман и покидает ресурс, он все равно оставляет за собой след, небольшой красный флажок. Том Ленгфорд из Rapid7 считает, что серьезных хакеров трудно обмануть. Они быстро соображают, что что-то не так и выходят из игры.

Хуже всего, если раскрытый обман разозлит хакера до такой степени, что он начнет мстить. Например, удалит или заблокирует все доступные данные, затем сотрет все следы своего пребывания и уйдет. Эксперты советуют начинать с создания архитектуры «нулевого доверия», в платформу которой надо интегрировать технологию Deception. Предусмотреть, чтобы попавший в ловушку был бы автоматически изолирован от реальной среды.

Операция Deception помогает собирать самые разнообразные данные о хакерах. К примеру, о его присутствии в социальных медиа, в средствах коммуникации, обо всём, что может быть полезно как для службы кибербезопасности компании, так и для правоохранительных органов.

Инструментарий Deception с успехом может применяться и для внутренних расследований. Если инсайдер окажется в одной из ловушек, то, естественно, у службы безопасности появится к нему/ней вопрос, что там делает, почему интересуется ресурсом, не имеющим отношения к прямым служебным обязанностям.

Немаловажно, что наличие Deception как компонента архитектуры безопасности положительно отмечается внешними аудиторами, в частности, от страховых компаний.

Конечно, чем крупнее организация, тем больше возможностей для воспроизводства правдоподобной картины. Некоторые американские компании создают фальшивые департаменты, возглавляемые реальными участниками игры. Даже нанимаются профессиональные актеры. Они приходят в псевдо офисы и разыгрывают роли менеджеров. Сидят за компьютером, пьют кофе, просматривают обманку - электронную почту…

Для подавляющего большинства компаний в этом спектакле нет необходимости, отмечает Синтия Брумфельд. Достаточно выстроить систему кибербезопасности, надежно защищающую корпоративные данные и интеллектуальную собственность как от внешних атак, так от инсайдеров. Нужно ли встраивать туда технологию Deception, зависит от поставленных задач. И не надо забывать, что плохо продуманная, слабо выстроенная операция Deception не снизит, а, напротив, может только усилить риски успешной хакерской атаки.

Сергей Шеметов

Кибербезопасность организации в условиях ограниченного бюджета. Статья первая

Киберугрозы становятся все более сложными и разнообразными, и защита от них требует значительных затрат. Но что делать компаниям с ограниченными ресурсами, которые не могут позволить себе дорогие решения? В этой статье мы рассмотрим, как обеспечить кибербезопасность в организации с ограниченным бюджетом, добиваясь приемлемого уровня защиты от возможных угроз.

Последние годы многие компании сталкиваются с беспрецедентно высоким числом кибератак на свои информационные активы. При этом заметно, что фокус внимания преступников перемещается на предприятия малого и среднего бизнеса в расчете на ограниченность финансовых ресурсов для кибербезопасности.

Если малое предприятие полагает, что не является прибыльной целью для киберпреступников, то это заблуждение. Именно малый и средний бизнес наиболее уязвим в виду ограниченности финансовых ресурсов для кибербезопасности, недостатка осведомленности и отсутствии штатных специалистов по кибербезопасности. Между тем, последствия кибератак, такие как утечка данных, денежный и репутационный ущерб, могут быть для них катастрофическими.

Выход в данной ситуации один - принимать оптимальные решения по расходам на кибербезопасность.

Первым шагом необходимо проанализировать ландшафт киберрисков и угроз. Одновременно провести проверку надежности вашей системы кибербезопасности. Делать это можно разными способами. Один из самых надежных – пентест, то есть тестирование системы на возможность несанкционированного проникновения.

Об этом расскажем подробнее.

Пентест (тестирование на проникновение) представляет собой контролируемую имитацию хакерской атаки на информационные системы, сети и веб-приложения с целью выявления уязвимостей, которые могут быть использованы злоумышленниками для несанкционированного доступа или нанесения ущерба компании. Основная цель тестирования: выявить проблемные места в системе безопасности, определить возможные векторы хакерской атаки, оценить тип и вероятный ущерб, который будет нанесен в случае реальной попытки проникновения злоумышленников в ИТ-инфраструктуру компании.

Тестирование на проникновение может служить отправной точкой для построения и модернизации системы кибербезопасности, поскольку позволяет объективно оценить уровень защищенности информационных систем с учетом всех применяемых решений и процессов в области информационной безопасности.

Вариантов пентеста несколько.

Анализ защищенности веб-приложений и сайтов

В современной цифровой экосистеме веб-приложения (сайты, веб-ресурсы, веб-службы) стали неотъемлемой частью бизнес-операций практически любой организации. Уязвимости в этих активах являются наиболее распространенной точкой получения первоначального несанкционированного доступа к системе. Злоумышленники постоянно совершенствуют свой инструментарий, улучшая как технические средства, так и методологию проникновения в веб-ресурсы.

Пентест веб-приложений предполагает имитацию реальных атак с использованием различных инструментов и техник для идентификации слабых мест в системе. В процессе тестирования выявляются проблемы безопасности в веб-приложениях или веб-службах, которые могут быть использованы злоумышленниками.

Тестирование на проникновение извне

Моделируя различные типы кибератак извне, пентест дает представление о потенциальных внешних киберугрозах, позволяет обнаружить уязвимости в подключенных к Интернету системах периметра сети, которые злоумышленники могут использовать для несанкционированного доступа или компрометации систем.

Тестирование на проникновение внутри локальной сети

В данном варианте тестируется защищенность корпоративной сетевой инфраструктуры внутри организации. Он позволят оценить эффективность безопасности внутренней сети, получить представление о потенциальных внутренних киберугрозах и уязвимостях, которые могут быть использованы инсайдерами, уже обладающими доступом к внутренней сети компании, для несанкционированного проникновения в базы данных с чувствительной информацией и компрометации систем. Устранение выявленных уязвимостей и сегментация сети — лучший способ избежать распространения вредоносного по всей организации.

Тестирование на проникновение в беспроводные сети

Беспроводные сети работают в большинстве организаций. Они удобны, так как предоставляют сотрудникам легкий доступ к сетевым услугам. Однако также представляют значительный риск для безопасности. Хакеры неустанно прощупывают возможные векторы атак с минимальным риском обнаружения, а беспроводные сети отвечают этим требованиям. Преступник, находясь вдали от вашего здания, используя антенну с высоким коэффициентом усиления, может попытаться воспользоваться вашей беспроводной сетью, рассчитывая, что его/ее просто не заметят.

Анализ защищенности мобильных приложений

Это критически важная процедура, нацеленная на проверку безопасности мобильных приложений через имитацию реальных методов взлома. Поскольку мобильные приложения становятся все более сложными и разнообразными, риски соответственно растут с каждым годом. Анализ защищенности мобильных приложений играет важную роль в определении недостатков логистики и технических уязвимостей.

Моделирование фишинговых атак

Этот вариант заточен под проверку уровня осведомленности персонала компании о киберрисках и угрозах. Могут применяться различные сценарии, имитирующие реальные фишинговые кампании. При этом автоматически ведется статистика действий реагирования со стороны сотрудников организации, которые и не подозревают о проверке. Фиксируются такие опасные действия как загрузка подозрительного файла или ввод данных на вредоносном веб-сайте, копирующем добропорядочный ресурс, предназначенном для захвата корпоративных учетных данных с целью дальнейшего проникновения в ИТ-инфраструктуру компании, развертывания программ-вымогателей.

Результаты проведения пентеста выражаются:

- в детальной характеристике обнаруженных уязвимостей, которые сортируются по уровню риска;

- в подробных технических выводах;

- в описании наиболее вероятных сценариев атаки;

- в калькуляции потенциального ущерба для бизнес-процессов компании;

- в рекомендациях по устранению выявленных уязвимостей, повышения осведомлённости технической команды и персонала компании.

Об авторе: *Шеметов Сергей Сергеевич, Генеральный директор ООО "ПЕНТЕКТ", ведущей российской компании в области кибербезопасности ("Специализированные консалтинговые услуги для защиты современных предприятий и организации от угроз кибербезопасности")* https://pentect.ru/

Безопасники становятся ближе к совету директоров, но по-прежнему испытывают нехватку финансирования

На протяжении длительного времени руководители корпоративной безопасности в компаниях полагали, что первые лица, принимающие решения, не воспринимают их работу достаточно серьезно.

Так, результаты опроса 365 специалистов по кибербезопасности в средних и крупных компаниях США, Канады и Западной Европы, проведённого исследовательской фирмой Enterprise Strategy Group (ESG) по заказу Trend Micro, принесли неутешительные выводы: кибербезопасность в большинстве организаций остаётся на вторых ролях.

Главные проблемы, которые выявил опрос:

- Во многих компаниях кибербезопасность считается технологической областью, не связанной с бизнесом и не приносящей прибыли.

- Кибербезопасность финансируется по минимуму, потому что бизнесменам достаточно «базовой», а не очень хорошей безопасности.

- Наблюдаются разногласия между безопасниками и акционерами в выборе моделей управления безопасностью .

- Отсутствует чёткое распределение ответственности и обязанностей между ИБ и ИТ.

(подробнее об этом см. https://habr.com/ru/companies/trendmicro/articles/542644/*).*

Это исследование проводилось несколько лет назад. А результаты опроса, организованного в прошлом году компанией Splunk (разработчик программного обеспечения для обработки и анализа машинно-генерируемых данных) среди американских компаний, выявил неожиданно

приятную тенденцию. Так, в 2024 году 82% директоров по кибербезопасности (CISO) напрямую докладывали главному исполнительному лицу в организации (CEO). А несколькими годами ранее таких было всего 47%.

Опросом Splunk было охвачено 500 директоров по безопасности плюс 100 акционеров и руководящих менеджеров.

Опрос показал, что начальники кибербезопасности, поддерживающие крепкие связи с первыми лицами, лучше взаимодействуют внутри компании с подразделением IT и инженерно-техническим коллективом по сравнению с теми, кто не пользуется привилегией близости к совету директоров. У них также заметно лучше идут дела с внедрением технологий искусственного интеллекта по таким направлениям кибербезопасности как обнаружение угроз, анализ данных, реагирование на инциденты, внутренние финансовые расследования.

В то же время только 29% респондентов из числа безопасников считают выделяемые на их нужды средства адекватными поставленным задачам, а 18% прямо говорят, что из-за скудости финансирования не могут надежно защитить организацию от злоумышленников. Для сравнения – более 40% членов правления верят, что имеющихся денег для кибербезопасности хватает. Но 64% представителей топ-менеджента признают, что просто не могут полностью удовлетворить потребности кибербезопасности из-за скудости бюджета.

Почти все опрошенные (94%) становились жертвами разрушительных кибератак.

Мэри Пратт, автор ряда статей в отраслевых изданиях по кибербезопасности, отмечая, что многие члены совета директоров не получают всю полезную информацию от безопасников, предлагает следующие рекомендации для последних (securitymedia.org):

1. *Проделайте серьезную подготовительную работу*

Следует приготовить и разослать письменный отчет для членов совета директоров загодя, за несколько дней и даже недель до личного представления. Эксперты по лидерству настаивают на тщательной, целенаправленной подготовительной к заседанию совета директоров работе, советуют при необходимости пройти специальное обучение, как готовиться и выступать.

2. *Доложите оценку состояния безопасности (кибербезопасности) и что конкретно следует улучшить*

Каждый раз, выступая перед первыми лицами компании, делитесь данными как о новых рисках, так и о перспективных возможностях улучшения безопасности.

3. *Будьте прозрачны*

Оценки не должны затушевывать риски для предприятия. О них надо говорить прямо и откровенно, в простой и доступной форме.

4*. Предупредите сложные вопросы*

В зале заседаний нет места для сюрпризов. Следует думать заранее о возможных вопросах и продумывать ответы на них.

5. *Будьте честны в отношении слабостей и уязвимостей систем безопасности*

Необходимо реалистично отвечать на вопросы о рисках и угрозах, о действительном состоянии корпоративной безопасности.

6. *Не пугайте аудиторию*

Атмосфера неуверенности и сомнений не работает для совета директоров, который определенно хочет правдивую информацию, исключительно для того, чтобы принимать обоснованные решения, куда и в каком объеме направлять инвестиции для минимизации рисков и угроз.

7. *Найдите чемпиона*

Налаживайте индивидуальные отношения с членами совета директоров, в первую очередь с теми, кто имеет технический опыт и мог бы помочь подготовиться к собраниям, просмотреть материалы для совета директоров, выступить в поддержку ваших предложений.

8. *Ближе к делу*

Переходите к делу с самого начала. Правление должно знать, зачем вы здесь.

9. *Пропустите технические моменты*

Не надо подробностей о последних эксплойтах, новейших технологиях. Вместо этого разговор сфокусируйте на высокоуровневых вопросах безопасности, но представляйте информацию в простых деловых терминах.

10. *Раскройте рентабельность безопасности*

Не все директора по безопасности могут рассчитать рентабельность инвестиций. Но это то, к чему надо стремиться. К примеру, сосредоточить внимание совета директоров не на стоимости новых технологий, а на выгодах инвестиций за счет снижения затрат на исправление ситуации после атаки, в частности, сокращения времени простоя.

11. *Определите критерии успеха*

К примеру, оценивайте свой успех по тому, как члены совета директоров реагируют на ваше выступление, насколько разумные вопросы задают или вообще молчат. Их реакция свидетельствует о степени доверия.

12. *Воспользуйтесь возможностями*

Безопасникам желательно выступать перед советом директоров, а не в комитетах. Проявите инициативу, чтобы регулярно включаться в повестку собраний и совещаний. Более того, рассматривайте свое выступление как возможность обосновать значение для бизнеса сильной программы безопасности, продемонстрировать компетентность не только в своей специальности, но и в бизнесе компании, стремление корректировать программу безопасности с учетом задач и стратегии бизнеса.

Как контролировать «операционный стресс»

Кризисы, частые инциденты безопасности, просто физические, нервные рабочие перегрузки, как правило, сопровождаются стрессом, который получил у ряда западных экспертов термин «операционный стресс» (не путать с медицинским термином).

Стив Гримандо, дипломированный специалист по изучению поведения людей в условиях форс-мажора, дает следующее определение: «Операционным стрессом следует называть ожидаемые и предсказуемые эмоциональные, физические или поведенческие реакции сотрудников организации, которые проявляются в процессе управления операциями в чрезвычайных, форс-мажорных ситуациях» (Security Management, January, 2025). В нормальных, не кризисных условиях чаще всего происходит перегорание на работе, когда для выполнения срочных и сложных задач не хватает ни времени, ни инструментов, ни ресурсов.

Помимо внешних раздражителей, причиной стресса нередко бывает искаженное, преувеличенно острое восприятие действительности, изменение личной самооценки.

Эксперты российской компании Business Relations, авторы книги «РБК Pro: практикум руководителя. Как поддержать настрой в команде и не перегореть самому» Иван Маурах, Владимир Герасичев, Арсен Рябуха выделяют наиболее характерные признаки стресса:

- беспричинные и частые приступы раздражительности, злобы, недовольства окружающими, обстановкой, миром;

- вялость, слабость, депрессия, пассивное отношение и нежелание общаться или что-либо делать, быстрая утомляемость;

- бессонница, беспокойный сон;

- невозможность расслабиться, постоянное напряжение тела и нервной системы;

- плохая концентрация внимания, заторможенность, сложность в понимании обычных вещей, снижение интеллектуальных возможностей, проблемы с памятью, заикание;

- недоверие к себе и окружающим людям, суетливость;

- подавленное настроение;

- повышенный интерес к алкоголю, наркотикам, курению, компьютерным играм и другим вещам/занятиям, которые ранее особо не интересовали.

Особенность «операционного стресса» заключается в том, что какие бы «черные лебеди» в виде внезапного кризиса, инцидента безопасности ни проявлялись, он (стресс) предсказуем, а, следовательно, им можно эффективно управлять. Гордон Грэхем, эксперт по кризисному управлению, один из учредителей консалтинговой компании Lexipol, известен таким изречением: «Что предсказуемо, то предотвратимо».

Хорошее планирование предполагает возможные психологические последствия форс-мажора и предусматривает соответствующие меры контроля. Правда, последние меры далеко не всегда срабатывают по многим причинам, чаще всего психологическим, когда, например, испытываемый работником стресс воспринимается им самим как слабость и тщательно скрывается.

Контролировать и управлять оперативным стрессом – задача не одного назначенного для этой функции менеджера. Каждый член команды должен хотя бы в общих чертах понимать причины и

последствия стресса, в частности, уметь идентифицировать тревожные сигналы эмоциональных реакций, знать, что в таких случаях делать.

Гримандо предлагает следующие базовые рекомендации для успешного противодействия:

- Изучать уникальные виды стресса, вызываемого быстрыми изменениями в ландшафте угроз.

- Превратить контроль и управление стрессом в интегральную составную часть культуры и практики организации.

- Обучать персонал умению замечать поведенческие признаки стресса и принимать меры реагирования.

- Поддерживать и культивировать способы и методы психологического, эмоционального самоконтроля и взаимного контроля, особенно в экстремальных ситуациях.

- Обеспечить активный мониторинг изменений, происходящих в бизнес процессах и операциях, заблаговременно предупреждая угрозу возникновения опасного для организации стресса у ее работников.

На пути модернизации системы управления посетителями

Программа управления посетителями (Visitor management system - VMS), занимает сегодня ключевое место в комплексе мер по контролю и управлению доступом (СКУД). Интеграция VMS с PIAM (Physical Identity and Access Management) позволяет организациям пользоваться одновременно физической и цифровой идентификацией, обеспечивать плотное отслеживание потоков посетителей.

Современные решения VMS и PIAM идут в направлении сокращения и даже отказа от охранников на входе и менеджеров в регистратуре взамен на мобильные цифровые процедуры идентификации, учета и регистрации, что облегчает работу организации и удобно гостям. В ходе предварительной регистрации посетитель получает цифровой пропуск прямо на свой мобильный дивайс. Тем самым отпадает необходимость физической выдачи электронного пропуска в виде карты или бейджа. Предварительная регистрация ускоряет процесс входа на объект, а мгновенные уведомления исключают ожидание, создавая гостеприимную атмосферу. Инновации формируют положительное первое впечатление, что важно для любых компаний, особенно ориентированных на VIP клиентов.

Система цифровой мобильной регистрации значительно улучшает качество обслуживания, а для компаний с несколькими объектами недвижимости появляется возможность централизованного управления с единого интерфейса.

В модернизированных системах VMS мобильные учетные данные глубоко индивидуализированы, адаптированы под конкретные цели визита, они содержат ограничения по времени и пространству нахождения гостя в организации.

Интеграция в VMS искусственного интеллекта открывает новые возможности, о которых 15 – 20 лет назад можно было только мечтать. К примеру, помогать гостям ориентироваться при первом

посещении, отвечая на их вопросы в автоматическом режиме, а корпоративной службе безопасности отслеживать и анализировать поведенческие характеристики посетителей, прогнозировать потенциальные риски и угрозы.

Уровень безопасности существенно повышается при интеграции VMS с системой управления зданием (умным офисом), контролирующей параметры окружающей среды, зону паркинга и прилегающие к зданию территории, а также управляющей «умными замками», которые защищают помещение от несанкционированного проникновения биометрическими датчиками, кодовыми комбинациями, иными технологиями.

Другой ценный аспект модернизированных систем VMS имеет отношение к готовности реагировать и предотвращать инциденты безопасности. Технология отслеживания в режиме реального времени местонахождения каждого посетителя в любой временный момент позволяет принимать быстрые и верные решения в случае возникновения чрезвычайной ситуации, к примеру, требующей немедленной эвакуации. Интеграция с программой массового оповещения повышает степень защищенности и безопасности для гостей, своевременно получающих предупреждение об угрозе, инструкцию к действиям на свой смартфон в виде текстового и/или голосового сообщения. В сообщении может содержаться информация о маршруте эвакуации, месте укрытия.

Интегрированная с решением VMS система СКУД позволяет автоматическое закрытие/открытие дверей в случае форс-мажора с учетом конкретного местонахождения как работающего в здании персонала, так и посетителей. Таким форс-мажором может быть пожар, стрельба, другой опасный для здоровья и жизни инцидент.

Упоминаемые здесь преимущества и характеристики современных решений управления посетителями важно иметь в виду, выбирая систему VMS для своей организации. Эта система, как минимум, должна отвечать следующим требованиям:

- возможность интеграции с системами безопасности и умного офиса;

- масштабируемость (способность справляться с ростом нагрузки);

- надежная защита персональной и конфиденциальной информации, в частности, путем шифрования;

- доступный и удобный для администраторов, службы безопасности и посетителей интерфейс.

Как мошеннические схемы влияют на доверие людей к бизнесу и государству

Интернет издание Journal of Financial Crime (январь 2025) опубликовал пространный отчет об исследовании, проведенном группой американских социологов относительно того, как широко распространившееся мошенничество в отношении простых людей влияет на их доверие к бизнесу, в том числе банкам, а также к правоохранительным органам. Одновременно исследователи поставили задачу выяснить, насколько эффективны попытки бизнеса и государства научить пользователей распознавать признаки мошенничества в электронных сообщениях и при посещении веб-сайтов.

В экспериментальном исследовании приняли участие 5 891 американец. Их разбили на две группы: тех, кто уже был объектом мошенничества (таких оказалось 91.2%), и тех, кто не был. Со всеми участниками проведены короткие интерактивные тренинги и контрольные тесты на усвояемость.

Знакомим читателей с некоторыми характерными результатами масштабного проекта.

Первоначально организаторы исходили из предположения, что жертвы мошенничества в сравнении с другими участниками продемонстрируют меньшую степень доверия к банкам, бизнесу в целом, государственным структурам, а также к ложным, обманным коммуникациям, представленным им в ходе эксперимента. К своему удивлению, исследователи не выявили существенных отличий между двумя группами. Генеральный вывод: размах мошенничества депрессивно воздействует на все население, включая и потерпевших от аферистов, и не потерпевших. Разница между теми и другими в смысле доверчивости практически не заметна.

Исследование подтвердило, что интерактивный тренинг по распознаванию признаков обмана дает ощутимый практический результат. Но при этом эффект обучения жертв преступлений нисколько не превосходит эффект обучения тех, кто лично еще не сталкивался с мошенниками.

Другое интересное заключение: короткое интерактивное обучение способам идентификации мошенничества в электронной почте оказалось более эффективным, чем тренинги по коммуникации с веб-сайтами. В первом случае применялись специально подготовленные сообщения, имитирующие мошенничество. Во втором случае такой возможности не было, и обучение свелось просто к набору рекомендаций.

Авторы проекта отмечают, что отсутствие интерактивности в процессе обучения снижает его эффективность. Письменные и устные советы, рекомендации имеют свойство улетучиваться из памяти по прошествии определенного времени.

Исследование также продемонстрировало, что эффективность тренингов по коммуникации с государственными учреждениями выше, чем тренингов, ориентированных на коммуникации с частными компаниями. Эксперты объясняют это нескольким причинами.

Во-первых, население в повседневной жизни контактирует преимущественно с частным сектором экономики. Соответственно подвергается большим рискам.

Во-вторых, общаясь с бизнес организациями, люди обращают внимание на вопросы, обычно выпадающими из учебной повестки (например, об обратной связи – отзывах клиентов на сайтах электронной коммерции и онлайн-покупок).

В-третьих, учебные материалы, подготовленные госорганизациями, как правило, качественнее тех, что предлагает бизнес.

Участники проекта продемонстрировали относительно слабый уровень распознавания признаков подделки в электронной почте. Это обстоятельство, подчеркивается в отчете, следует принять во внимание тем организациям, которые занимаются рассылкой email сообщений своим пользователям.

Навыки обнаружения мошенничества со временем ослабевают. Так, например, полученные на тренинге знания о фишинговых атаках выветриваются уже через пару недель. Эффект обучения признакам видео и текстового мошенничества в сфере инвестиций держится не более полугода. Наилучшие результаты продемонстрировали те участники, которые повторяли тренинги каждые три месяца.

Авторы проекта признаются, что вынуждены были использовать ограниченное число (12) форм коммуникаций, составляющих весьма малую долю разнообразного и постоянно совершенствующегося инструментария на вооружении криминала. Что, возможно, сказалось на точности результатов.

Подробнее см. **https://www.emerald.com/insight/content/doi/10.1108/jfc-12-2023-0314/full/html**

Безопасность на парковках: угрозы прежние, решения новые

Согласно американской статистике, автомобильные парковки занимают третье место по числу преступлений после домашних насилий и инцидентов на транспорте: почти 240 тысяч за последние пять лет в США. По России подобной статистики обнаружить в открытых источниках не удалось. Но, скорее всего, цифра тоже не маленькая.

Никто не будет спорить, что владельцы торговых центров и других объектов с парковочной зоной заинтересованы в безопасности парковок, осознают, что это их ответственность. Однако, как отмечает М. Хаггард, владелец юридической фирмы Haggard, бизнес предпочитает инвестировать непосредственно в охрану офисов и коммерческих площадей, считая парковки объектами второстепенной важности. И это обстоятельство оборачивается серьезной проблемой, так как парковки относительно безлюдны и, как показывает практика, бывает невозможно найти свидетеля совершенного там преступления. Чем охотно и пользуется криминал.

Один из важнейших аспектов – слабая освещенность подземных парковок. Данное обстоятельство привлекает воров, насильников, наркоторговцев, убийц, считает М. Уилленбринк, эксперт по безопасности парковок в компании Genetec (разработка решений для физической охраны). По его мнению, на парковки необходимо распространить такие же требования безопасности, как и на офисы, и на жилые помещения. Установка дополнительных источников освещения поубавит наглости у многих злоумышленников.

Среди других мер – установка в изолированных помещениях (например, на лестницах, ведущих в подземную парковку), камер видеонаблюдения и коммуникационных устройств.

Для больших парковочных зон Хаггард рекомендует использовать беспилотные летательные аппараты как средство мониторинга. Дроны стоят сравнительно недорого, во всяком случае, много дешевле, чем возможные судебные издержки по следам совершенного преступления.

Герб Уббенс, президент Paratus Consultants Group, в течение 30 лет наблюдал эволюцию охраны парковок. Когда он только начинал карьеру, то, по его словам, не было ни аварийных станций с синим фонарем (комбинированный узел телефона экстренной связи и аварийного выключателя, распространенный в США и Канаде), ни мобильных дивайсов, ни дистанционно регулируемых источников освещения, ни видеонаблюдения с встроенной аналитикой, позволяющей отслеживать автомобили по госномерам и предупреждать охрану о появлении на парковке во внеурочное время незнакомца.

Риски и угрозы в принципе остались прежними, но возможности им противостоять радикально улучшились.

Уббенс обращает внимание на то, как безопасность парковок воспринимается пользователями. Если люди чувствуют, что здесь небезопасно, что владелец не слишком озабочен охраной, то организация рискует терять как своих работников, так и клиентов. А восприятие во многом зависит от вида внушительной системы видеонаблюдения, многочисленных средств коммуникации, дюжих охранников.

Эксперты рекомендуют не оставлять голыми бетонные стены и перекрытия, а покрывать их приятными для глаза яркими красками.

Другой совет - постоянно совершенствовать систему информационных указателей, снижающую риски столкновения, помогающую посетителям лучше ориентироваться, запоминать место, где оставили автомобиль. Такие рекомендации имеют отношение к безопасности, поэтому не стоит ими пренебрегать, в первую очередь, тем, кто проектирует новые здания с парковочной зоной.

Конечно, владельцы объекта несут полную ответственность за безопасность парковок. Но чтобы точно рассчитать, сколько и куда вкладывать деньги, необходимо серьезно проанализировать криминальную обстановку в районе объекта, внимательнейшим образом изучить историю преступлений на парковках объектов, находящихся рядом.

При этом иметь в виду, что там, где оплата парковки производится наличными, риски криминала существенно выше по сравнению с парковками, где внедрена оплата с помощью системы распознавания госномеров и мобильного приложения.

Криминальная активность – не единственная угроза безопасности. Споры за парковочное место и другие возможные конфликты, тем более переходящие в насилие, также должны приниматься во внимание при подготовке инструкций по реагированию на инциденты. При этом особые требования предъявляются к компетенциям охранников деэскалировать и предотвращать споры и стычки, которые отрабатываются на специальных тренингах.

Парковки представляют собой первое и последнее место, где пользователь получает представление о компании, в которую приехал. Если он раздражен неудобствами парковки, не чувствует себя в достаточной безопасности, то в следующий раз, возможно, выберет другую организацию.

(по материалам журнала Security Management - https://www.asisonline.org/security-management-magazine)

Рецензия: «Corporate Security - In the Digital Age Paperback», by Ron Kornblum

В современном взаимосвязанном мире компании сталкиваются с множеством угроз и вызовов, представляющих опасность для бизнеса. Никогда ранее надежная охрана и всеобъемлющая безопасность не играли такой важной роли как сегодня.

Монография о корпоративной безопасности Рона Корнблюма представляет собой исчерпывающее руководство, которое погружает читателя в премудрости защиты бизнеса от внешних и внутренних рисков. Книга позволяет получить полное представление о сфере корпоративной безопасности, вооружает читателя познаниями стратегии, необходимыми для эффективной защиты.

Автор фокусирует внимание на практических аспектах охраны, используя сценарии, взятые из реальной жизни.

Книга отражает комплексный подход к методологии управления рисками. Читатель в ней найдет подробную характеристику разнообразных направлений – от изучения слабостей и уязвимостей систем охраны до конкретных операций по обеспечению безопасности организации.

Каждый раздел содержит полезные рекомендации и лучшие практики.

Автор адресует свой труд широкому кругу читателей – профессионалам корпоративной безопасности, топ-менеджменту, акционерам. Книга служит важным информационным ресурсом, практическим помощником для анализа, планирования и осуществления надежной и успешной программы корпоративной безопасности.