Охрана предприятия

№ 4 (97) 2025

Оглавление

Как бизнес может и должен бороться с кардингом

С момента появления первых банковских карт попытки мошенничества с ними остаются в числе наиболее острых и дорогостоящих рисков. Ассоциация финансовых специалистов (**https://www.afponline.org**) провела в прошлом году опрос «2024 AFP Payments Fraud and Control Survey Report», в ходе которого выяснилось, что 30% компаний не смогли вернуть украденные мошенниками деньги.

Многие бизнесмены и коммерсанты предпочитают переводить и получать деньги через карты – быстро и удобно. Но при этом рискуют их лишиться из-за похищенных учетных данных, слабой верификации, других потенциальных уязвимостей.

Наиболее распространенные виды мошенничества с банковскими картами (кардинга):

- несанкционированный доступ к онлайн-аккаунту пользователя;

- операции без присутствия карты (тип транзакций по банковским платёжным картам, при которых держатель карты физически не присутствует во время и в месте проведения оплаты);

- инсайдерские риски;

- поддельные счета;

- поддельные профили банковских клиентов.

Специалисты по борьбе с платежным мошенничеством в компании Mineraltree (финансовый аудит) предлагают 8 наилучших, по их мнению, практик предотвращения кардинга (https://www.mineraltree.com):

Мониторинг транзакций в режиме реального времени

Такой мониторинг необходим для идентификации и реагирования на подозрительную активность в транзакциях. Продвинутые аналитические системы используют исторические данные и алгоритмы машинного обучения в целях обнаружения аномальных явлений, таких, например, как неожиданные скачки в платежах или транзакциях, осуществляемых с незнакомой ранее локации.

Тщательная верификация каждого счета

Уделяя внимание таким подробностям как адрес вендора, условия оплаты, детали счета, вы можете обнаружить нестыковки до момента оплаты. Помогают системы автоматизированной сверки счетов-фактур.

Инвестируйте в технологии APA (Accounts Payable Automation)

Они позволяют компаниям оптимизировать и автоматизировать процесс расчета по оплате. Что в свою очередь снижает риск человеческой ошибки, на что обычно и рассчитывают мошенники. Технологии APA нередко используются в процессе финансового аудита, что помогает вовремя заметить и проследить признаки подозрительной активности.

Не пренебрегайте инструментами для выявления и предотвращения мошеннических действий (fraud detection tools)

В первую очередь, системами с использованием искусственного интеллекта и машинного обучения при анализе транзакций и поиска аномалий.

Отдавайте предпочтение виртуальным картам

Виртуальные карты работают так же, как и традиционные кредитные карты. Но в отличие от последних обладают функцией «токенизации». Вместо привычных номеров, срока действия и кода безопасности банковских карт используются уникальные и непредсказуемые значения, безличные идентификаторы, называемые токенами.

Проводите регулярные тренинги с персоналом компании

Сотрудники организации независимо от ее профиля представляют собой переднюю линию защиты от мошенников. Знание ими хотя бы основных способов предотвращения мошенничества имеет для компании критическое значение. Темы занятий должны покрывать такие вопросы как распознавание фишинговых сообщений в электронной почте, работа с платежными данными, признаки мошеннических схем и другие важные моменты. Эксперты советуют использовать разнообразные методы обучения, включая симуляцию фишинговых атак.

Берите на вооружение мультифакторную аутентификацию

Учетные данные при мультифакторной аутентификации могут включать одновременно пароль, смс с кодом, биометрический идентификатор, как вариант дополнительного уровня безопасности – контрольный (личный, секретный) вопрос, правильный ответ на который санкционирует физический или виртуальный доступ.

Предусмотрите сегрегацию обязанностей работников финансовой службы

Сегрегация (разделение) обязанностей препятствует наделению одного сотрудника слишком большим контролем над платежными процессами. Компании уменьшают риски мошенничества (и, добавим, ошибок), возлагая обязанности по платежам на разных работников бухгалтерии.

Как криминал пытается обойти биометрическую защиту

Биометрические системы стали одним из важнейших способов физической и цифровой безопасности. Еще в 2018 году в России был принят закон о Единой биометрической системе.

Эксперт по биометрической защите Алексей Лукацкий замечает, что о применении таких систем в сфере безопасности говорят мало. Возможно, чтобы не обозначать их слабые зоны и уязвимости. «Однако принцип «безопасность через незнание» в данном случае не работает, - пишет эксперт на сайте forbes.ru, - Необходимо широкое обсуждение механизмов защиты такой базы».

Называя более полутора десятков способов взлома системы биометрической идентификации (см. его блог lukatsky.blogspot.com), Лукацкий отмечает, что выбор наиболее удобного из них зависит от конкретных задач. «Если нужно заставить систему принять «правильное» решение, то эффективнее всего атаковать систему верификации. Когда действия злоумышленников направлены на конкретного человека, то логичнее синтезировать его голос и видео. Существующие технологии уже позволяют, имея запись голоса или видео любого человека, синтезировать его речь или наложить его лицо на другую видеозапись».

Один из авторов статей в издании Forbes наглядно показал неудовлетворительную надежность ряда систем биометрической защиты в устройствах потребительского класса. Для теста он заказал гипсовую 3D-копию своей головы, после чего попытался с ее помощью разблокировать смартфоны пяти моделей: LG G7 ThinQ, Samsung S9, Samsung Note 8, OnePlus 6 и iPhone X. Гипсовой копии оказалось достаточно для снятия блокировки четырёх из пяти протестированных моделей. Эксперимент показал, что распознавание лиц — не самый надёжный метод защиты конфиденциальной информации. Комментируя этот эксперимент, представители «пострадавших» компаний сказали, что распознавание лиц делает разблокировку телефонов «удобной», но для «самого высокого уровня биометрической аутентификации» предпочтительны сканеры отпечатка пальца или радужной оболочки глаза (habr.com).

Ни одна система не демонстрирует точность с нулевым показателем ложноположительных и ложноотрицательных срабатываний даже в оптимальных лабораторных условиях. За счёт настроек системы можно, к примеру, увеличить точность распознавания до 100%, но тогда увеличится и количество ложноположительных срабатываний. И наоборот, можно уменьшить количество ложноположительных срабатываний до нуля — но тогда пострадает точность.

Скотт Бриско, директор по развитию контента в организации профессионалов охранной индустрии ASIS International, опубликовал в издании этой организации, журнале Security Management (апрель 2025 г), статью «Искусство и наука обхода биометрического скрининга». В ней он ссылается на 60-страничный Отчет Европола «Биометрические уязвимости» (https://www.europol.europa.eu/). Отчет раскрывает, как преступники, террористы и другие злоумышленники разрабатывают способы обмануть биометрические методы проверки, в том числе наиболее надежные и проверенные.

«Следует понимать, что большинство уязвимостей все еще находятся на стадии лабораторных испытаний, - поясняется в Отчете. – Таким образом, возможность взломов, описанных в Отчете, следует воспринимать не как признак слабости систем, но скорее как продолжение усилий по предотвращению таких уязвимостей и повышению осведомленности для их выявления на ранней стадии».

В Отчете рассматриваются конкретные уязвимости, присущие четырем видам биометрической защиты – распознаванию отпечатков пальцев, лиц, радужной оболочки глаза и голоса.

Отпечатки пальцев

Новые, усовершенствованные технологии 3D-печати позволяют создавать картинку с характеристиками, схожими с характеристиками настоящих отпечатков пальцев. Кража отпечатков 3D-модели может позволить злоумышленникам путешествовать, пересекать границу под именем и биографическими данными другого человека. Иной способ манипулирования – уничтожение или изменение отпечатков, чтобы избежать идентификации.

Распознавание лиц

96% персональных устройств, для разблокировки которых требуется распознавание лица, взламываются с помощью простой распечатки фотографии. При повторных атаках часто используется видео. Существуют и более продвинутые технологии обмана, например, 3D-печать масок. Такие маски на 57% эффективнее обманывают системы распознавания лиц в двухмерных измерениях. Еще один способ – морфинг, когда берутся два внешне похожих человека и с помощью ПО для обработки фотографий создается т.н. «составное лицо». Морфинг, к примеру, позволяет преступникам путешествовать с паспортом, в котором есть составное изображение их лица и лица владельца паспорта. Наконец, есть и старомодный грим.

Распознавание по радужной оболочке глаза

Жестокий метод предполагает использование радужной оболочки глаза только что умерших людей, так как их текстура остается неизменной в течение нескольких часов после смерти. Менее жестокие, но и менее эффективные способы основаны на распечатанных 2D и 3D фотографиях размером в глазное яблоко.

Распознавание речи

Голосовые биометрические системы идентификации получают широкое распространение – от онлайн-банкинга до электронной коммерции. Они могут быть уязвимыми для подмены с использованием синтетических медиа, включая технологии дипфейков. В то же время имитация голоса вряд ли обманет продвинутые системы аутентификации, основанные на физиологических характеристиках голоса. Основными векторами атак являются повторные атаки (прямые записи речи людей, синтетическая речь, голосовые конверторы, преобразующие слова одного говорящего в голос другого человека). Синтез и преобразование – наиболее опасны.

В Отчете Европола рекомендуется повышать осведомленность о рисках и угрозах для аутентификации, совершенствовать технологический инструментарий и методологию обнаружения атак, брать на вооружение комплексный подход к биометрическому распознаванию (сбор и хранение данных, передачу, идентификацию и верификацию), стандартизацию отчетности и агрегирование данных.

Многие эксперты указывают, что уязвимости биометрических систем безопасности во многом обусловлены тем, что производители в первую очередь думают об удобстве использования, а не о надежности.

Инновационные сдвиги в сфере физической идентификации и управления доступом (PIAM)

Рынок PIAM (Physical Identity and Access Management) охватывает решения и технологии, предназначенные для оптимизации управления физическим доступом к средствам, активам и информационным системам. Сегодня он претерпевает значительные изменения, обусловленные передовыми технологиями, развитием угроз безопасности и изменением нормативно-правовой базы.

Рынок решений PIAM подвержен быстрому росту и динамичным изменениям. В 2024 году он оценивался примерно в 2,6 миллиарда долларов США. Ожидается, что к 2033 году достигнет примерно 5,7 миллиарда долларов, что соответствует среднегодовому темпу роста в 13,6% с 2025 по 2033 год.

Системы управления физической идентификацией и доступом уже давно не ограничиваются традиционными замками с ключами и бейджами. Современные решения включают в себя биометрическую верификацию, технологии RFID (радиочастотной идентификации), интеллектуальные датчики, искусственный интеллект, машинное обучение, интернет вещей (IoT).

Ускоренному росту рынка PIAM способствуют несколько ключевых факторов:

1. *Повышенные требования к безопасности*. Физические взломы могут служить точками входа в цифровые системы, что вынуждает компании внедрять более строгие комплексные меры контроля доступа, охватывающие как физическую, так и цифровую сферы.

2. *Соблюдение нормативных требований*. Правительства и регулирующие органы по всему миру ввели (или собираются вводить) более строгие правила в отношении защиты данных и физической безопасности. Такие отрасли как финансы и критически важная инфраструктура особенно остро нуждаются в соблюдении этих правил, что стимулирует инвестиции в передовые решения PIAM.

3. *Технологические достижения*: интеграция с биометрической верификацией, устройствами IoT и облачными системами управления делает эти решения более привлекательными для предприятий.

4. *Экономическая эффективность и преимущества в работе*. Помимо обеспечения безопасности, современные решения PIAM способствуют повышению операционной эффективности. Автоматизированные системы сокращают необходимость в ручных проверках и могут быстро адаптироваться к изменениям в организационной структуре или персонале, снижая административные издержки и обеспечивая быстрое управление доступом.

Аналитики рынка отмечают, что интеграция PIAM с передовыми системами кибербезопасности ведёт к созданию единой стратегии безопасности, устраняющей разрыв между физической и цифровой безопасностью. Новые тенденции, такие как управление идентификацией на основе

блокчейна, использование систем автоматической аналитики больших данных для обнаружения угроз, также способны изменить рыночную ситуацию. Эти инновации обещают улучшенную отслеживаемость, снижение уровня мошенничества и более активный подход к управлению рисками.

Несмотря на то, что рынок давно созрел, остается ряд нерешенных проблем.

Одной из наиболее значительных проблем эксперты исследовательской, консалтинговой компании Verified Market Reports называют сложность и стоимость внедрения и поддержания решений PIAM.

Другая проблема – трудности интеграции этих систем с существующей инфраструктурой, что приводит к увеличению времени развертывания и росту затрат. В первую очередь, эта проблема затрагивает компании с ограниченными бюджетами и ресурсами.

Третья проблема – нехватка специалистов в данной области. Спрос на квалифицированный персонал, способный внедрить и эффективно управлять Piam Systems, опережает предложение. Опрос ISC (комплексные услуги в области управленческого консалтинга) показал, что 64% организаций стремятся, но пока безуспешно, найти для функции кибербезопасности экспертов по PIAM.

Четвертая проблема - конфиденциальность и потенциально неправомерное использование персональных данных. Дэррил Джонс, вице-президент компании CIAM, указывает на опросы, согласно которым 89% потребителей обеспокоены тем, как ИИ влияет на безопасность их личности, а 97% обеспокоены тем, что их личные данные находятся в сети.

Рынок управления физической идентификацией и доступом находится на переломном этапе, характеризующемся стремительным развитием технологий, растущими требованиями регулирующих органов и повышением осведомлённости о комплексных потребностях в сфере безопасности. Поскольку лидеры отрасли продолжают внедрять инновации и адаптироваться, рынок готов предложить безопасные, масштабируемые и экономичные решения для управления доступом. Эта тенденция не только обещает повысить эффективность работы, но и создаёт основу для более безопасного глобального ландшафта, в котором физическая и цифровая безопасность работают рука об руку.

(по материалам публикаций на веб-сайтах www.verifiedmarketreports.com, www.openpr.com, www.openpr.com, www.datahorizzonresearch.com, www.solutionsreview.com)

Рекомендуемые вопросы финансовой службы (бухгалтерии) к службе кибербезопасности

Киберкриминал стал главной угрозой для бизнеса. В центре внимания злоумышленников – работники бухгалтерии, финансовых служб в компаниях, обладающие привилегированным доступом к финансовой информации, конфиденциальным данным клиентов. По мнению экспертов, «утечка 20% коммерческой тайны организации может привести к банкротству, компрометация даже 5% конфиденциальных данных может обернуться для организации потерей статуса лидера рынка» (https://vaael.ru).

С другой стороны, бухгалтерский учет все более зависит от электронных систем и цифровых данных, подчеркивает магистр Римского университета La Sapienza Ж. Абдылдаева. На сегодняшний день существует множество угроз и уязвимостей, с которыми сталкиваются бухгалтерские системы, пишет она на сайте журнала «Актуальные исследования» (https://apni.ru/journal).

В числе *внешних угроз* Абдылдаева называет:

- Атаки с использованием вредоносных программ.
- Фишинг и социальная инженерия.
- Атаки на облачные сервисы, используемые современными бухгалтерскими системами.

Среди *внутренних угроз*, по мнению магистра, превалирует человеческий фактор. Внутренние угрозы связаны с неконтролируемым доступом к бухгалтерским данным. «Это может включать как умышленное манипулирование данными со стороны недобросовестных сотрудников, так и несанкционированный доступ к конфиденциальной информации из-за неправильной настройки прав доступа» (там же).

Кроме того, автор публикации упоминает и кратко характеризует угрозы, связанные с уязвимостями программного обеспечения, уязвимостями протоколов безопасности, слабой информационной защитой.

Рекомендации специалистов по защите бухгалтерии от кибератак в принципе не оригинальны. Предлагается:

- Использовать встроенные системы защиты.
- Делать резервные копии.
- Перевести бухгалтерию на удаленные сервера.
- Обучать персонал базовым навыкам безопасности: не открывать подозрительные письма, не кликать непроверенные ссылки, не запускать странные программы и вводить личные данные только на надёжных сайтах. (https://vk.com/wall-211708210_121)

Между тем, ключевое значение приобретает тесное взаимодействие между бухгалтерией и службой безопасности внутри одной организации.

Консультант по кибербезопасности и владелец компании Reisender Филипп Ли сформулировал восемь вопросов, которые финансовые директора (главные бухгалтеры) должны задать руководителю СБ, чтобы «лучше понимать состояние безопасности в организации и помогать в повышении ее эффективности» (https://www.cfo.com).

1. Как мы проверяем свои возможности по реагированию на инциденты и что улучшаем в результате?

В ответах ищите конкретные примеры тренингов по реагированию на инциденты, результаты и уроки тестирования готовности организации, своевременное корректирование планов реагирования на инциденты.

2. Как мы управляем рисками в сфере кибербезопасности и кто участвует в программе управления рисками?

В ответах должны быть описаны такие процессы и процедуры как регулярная оценка рисков, моделирование угроз, планирование стратегии по их минимизации. Важно знать, кто получает

уведомления об этих рисках (акционеры, совет директоров или иные заинтересованные стороны).

3. Интегрирована ли функция кибербезопасности в общую программу управления рисками организации?

Интеграция является ключевым фактором для комплексного подхода к управлению рисками, включая согласование мер по кибербезопасности с бизнес-задачами, синхронизацию методов управления рисками по всей организации.

4. Соответствуют ли имеющиеся у организации системы требуемому уровню безопасности, почему были выбраны именно эти системы?

Система должна быть отобрана с учётом отрасли, потребностей бизнеса и организационных рисков.

5. Как мы справляемся с управлением рисками сторонних организаций?

Речь идет о комплексной проверке, регулярных аудитах зафиксированных в договорах требованиях к стандартам безопасности.

6. Какие исключения из программы безопасности сделаны для какого-либо отдела, системы или процесса в организации?

Этот вопрос направлен на выявление пробелов или исключений в программе безопасности. В ответах должно содержаться весомое обоснование таких решений, например, сравнительный анализ затрат и выгод, определение приоритетности рисков.

7. Каковы ключевые показатели эффективности в области кибербезопасности и как они отслеживаются?

Ключевые показатели охватывают: количество выявленных инцидентов, время реагирования и результаты мероприятий по обеспечению безопасности.

8. Каков наш подход к анализу угроз и как мы используем его для повышения уровня безопасности?

Как компания собирает, анализирует и использует информацию об угрозах, включая партнерство финансовых служб с поставщиками информации об угрозах, участие в обмене информацией между разными подразделениями, взаимодействие в работе по обеспечению безопасности.

Точные и ясные ответы на перечисленные вопросы необходимы руководителям финансовой службы (бухгалтерии), чтобы принимать обоснованные решения, положительно влияющие на формирование и развитие корпоративной программы безопасности.

Красные флажки AML в криптовалюте

По данным крупного агрегатора данных о криптовалютах CoinMarketCap, на сегодняшний день существует более 5000 видов криптовалют. Технология, лежащая в их основе, нашла применение в различных отраслях, ее будущее обладает огромным потенциалом.

Новый цифровой мир с момента его возникновения неизменно в фокусе внимания отмывателей грязных денег. Криптовалюты анонимны. Пользователей редко связывают с реальными именами. Именно этим и пользуются преступники, чтобы скрыть деньги, полученные нечестным путем. Процесс отмывания строится на том, чтобы максимально запутать следы и сделать невозможным выяснение, откуда взялись деньги.

Выявление красных флажков AML (Anti-Money Laundering) – важнейшая мера защиты от финансовых злоупотреблений. Предупреждающие сигналы необходимы для поддержания целостности и безопасности цифровых финансовых систем.

Эксперты межправительственной организации FATF (Financial Action Task Force on Money Laundering - группа разработки финансовых мер борьбы с отмыванием денег) сформулировали основные признаки отмывания денег с помощью криптовалют и виртуальных активов. Так, чаще всего мошенническими являются следующие типы транзакций:

- Платежи небольшими суммами, чтобы не привлекать внимания.
- Высокодоходные транзакции с криптовалютой за короткий период.
- Мгновенный перевод виртуальных средств из зон с жёстким контролем в страны с низким уровнем регулирования.
- Мгновенный вывод виртуальных средств без каких-либо промежуточных транзакций.
- Внесение ранее идентифицированных украденных средств на криптокошельки.

Выявленные закономерности включают:

- Новые счета, которые несовместимы с определенным состоянием открывателя.
- Новые счета финансируются за счет солидного предварительного платежа, который вскоре после этого обменивается.
- Транзакции с нелогичными наборами криптовалют или счетами без привязок.
- Крупные суммы криптовалют регулярно переводятся в течение определенного периода на один счёт с множества других.
- Небольшие суммы с нескольких виртуальных кошельков мгновенно перемещаются или удаляются.
- Периодические обмены фиатных денег (цифровых валют центральных банков) на криптовалюту без видимого обоснования.

Анонимность транзакций затрудняет получение властями информации о подозрительной активности с использованием виртуальных средств. Отмывание денег с использованием анонимности криптовалют может иметь следующие признаки:

- Транзакции с использованием более одного типа криптовалюты, особенно высокоанонимных валют с «неоправданно» высокими показателями.
- Перевод средств с прозрачного блокчейн-счета на централизованную платформу криптовалютной биржи, а затем на частный или анонимный кошелёк или валюту.
- Компании, работающие в качестве нелицензированных провайдеров, взимают более высокие комиссии за обработку виртуальных средств от имени своих клиентов, чем лицензированные компании.
- Значительный объём одноранговых транзакций (обмена данными или активами между двумя сторонами, без участия третьей стороны) с использованием микширующих сервисов (миксеров криптовалют) без должного обоснования.

- Средства из подозрительного источника, переведенные на криптовалютный кошелек, например, с сайтов азартных игр.
- Средства, поступающие на криптовалютные кошельки с подозрительных IP-адресов или управляемые с помощью программного обеспечения для шифрования.
- Средства, переводимые через международные границы с использованием децентрализованной системы.
- Пользователи, использующие прокси-серверы или DNS (системы доменных имен), чтобы скрывать доменные имена при регистрации криптовалютного кошелька.
- Несколько виртуальных кошельков – все с одного IP-адреса.
- Средства, отправленные с явно недостаточным уровнем проверки клиентов или процедуры «знай своего клиента».
- Использование банкоматов с виртуальной валютой для многочисленных мелких транзакций в юрисдикциях с высоким уровнем риска.

Незаконные источники криптовалютных средств могут быть связаны со следующим поведением:

- Средства, поступающие от инвестиций в криптовалюту, или от первоначальных предложений монет, или от платформ ICO (Initial Coin Offering — способ привлечения инвестиций для стартап-проекта, основанного на технологии блокчейн) с недостаточным контролем.
- Один виртуальный кошелёк, привязанный ко многим кредитным или дебетовым картам, используется для вывода крупных сумм фиатных денег.
- Обширные депозиты на виртуальные кошельки, которые мгновенно выводятся в виде фиатных денег.
- Прозрачность клиентов практически отсутствует, персональная идентификация недоступна поставщикам криптовалют.

Преступники, перемещающие средства через границы и по всему миру, часто злоупотребляют регионами, где слабо контролируются правила использования криптовалют. К общим признакам такого поведения относятся:

- Средства в криптовалюте, которые поступают или отправляются в страну, не являющуюся страной проживания клиента.
- Клиенты, использующие криптовалютные сервисы в зонах повышенного риска, где, как известно, действуют ограниченные процедуры по борьбе с отмыванием денег.
- Клиенты размещают свои рабочие места в зонах с небольшим количеством криптовалютных протоколов или вообще без них, не имея на то никаких оснований.

(по материалам интернет ресурсов binance.com, financialcrimeacademy.org, fatf-gafi.org, securitylab.ru, habr.com, woolypooly.com).

Коррупция в банке HSBC: когда “красные флажки» игнорируются

Весной 2025 года швейцарская неправительственная организация Public Eye предала гласности результаты проведенного ею расследовании «серьезных нарушений» со стороны банка HSBC, одного из крупнейших финансовых конгломератов в мире, относительно борьбы с отмыванием грязных денег.

Речь идет о скандальном «деле Forry», о брокерской фирме, тесно связанной с HSBC, через которую отмывались сотни миллионов долларов. По версии швейцарских следователей, в период с 2002 по 2015 год со счёта Центрального банка Ливана на счёт HSBC в Швейцарии на имя Forry Associates были переведены средства на сумму более 330 миллионов долларов. Платежи производились в соответствии с брокерским контрактом между Центральным банком и Forry за услуги, связанные с еврооблигациями и казначейскими векселями. Следователи утверждают, что компания Forry контролировалась братом тогдашнего председателя ЦБ Ливана Раджой Саламе. Из этих средств 248 миллионов долларов были переведены на личный счёт Раджи Саламе в HSBC. По меньшей мере, шесть европейских стран начали расследование этого дела.

The National, англоязычная ежедневная газета Объединённых Арабских Эмиратов, опираясь на материалы, собранные Public Eye, подробно рассказала, как чрезмерное влияние высокопоставленного менеджера HSBC, «стремившегося сохранить деловые отношения», подорвало систему внутренних проверок и контроля банка.

На протяжении многих лет менеджер HSBC по работе с клиентами Собхи Таббара, давний знакомый Раджи Салами, утверждал, что Forry была законным брокером, хотя, позднее судебные преследования доказали, что Forry была подставной компанией – без сотрудников и реальных услуг.

HSBC поддерживал деловые отношения с Раджой Саламе, в основном, на основании документа 2009 года, отправленного ЦБ Ливана в адрес Таббаре, однако следователи выяснили, что правление никогда не одобряло этот контракт. По данным Financial Times, четыре бывших члена центрального совета ЦБ Ливана, которые работали в соответствующий период, на условиях анонимности заявили, что не помнят, чтобы одобряли транзакции с Форри. Глава ЦБ Риад Саламе отказался предоставить записи, подтверждающие решения центрального совета, сославшись на банковскую тайну.

The Nation пишет, что банк HSBC уже был замешан в целой серии скандалов, связанных с отмыванием денег, в частности, отмыванием почти 900 миллионов долларов для наркокартелей. В рамках урегулирования в 2012 году HSBC Holdings выплатил рекордный штраф в размере 1,25 миллиарда долларов федеральным регулирующим органам США, признал серьёзные нарушения и пообещал провести реформы. Взамен судебная система США отложила судебное преследование, согласившись закрыть дело, если HSBC выполнит свои обязательства в течение пяти лет. В течение этого испытательного срока HSBC продолжал обрабатывать подозрительные транзакции Форри, несмотря на почти двадцать запросов разъяснить ситуацию, отправленных отделом комплаенса менеджеру по работе с клиентами Forry Associates в период с 2006 по 2013 год, согласно расследованию Public Eye.

Еще в 2015 году подразделение финансовой разведки HSBC отследило движение средств и обнаружило, что основная часть денег была переведена со счета Форри на личные счета Раджи Саламе в Ливане через HSBC.

Из-за этих тревожных сигналов HSBC решил закрыть счёт Форри в 2016 году. Однако банк сообщил об этом в отдел по борьбе с отмыванием денег только четыре года спустя, на фоне финансового краха Ливана.

Расследователи обнаружили сложный денежный след, тянущийся по всему миру со счёта Форри, который, по их словам, типичен для схем отмывания денег. Большая часть средств сначала была переведена на счета Раджи Саламе в Ливане, а затем возвращена Риаду Саламе. Некоторые комиссионные также были переведены напрямую из Форри на два офшорных счёта Риада Саламе, которые HSBC не смог отследить, а также на счёт, принадлежащий Анне Косаковой, любовнице Риада.

Мистер Дебс, адвокат, рассказал The National, что крупные транзакции также приносили банкам прибыль, что отчасти объясняет, почему подозрения игнорировались, как и бонусы для менеджеров по работе с клиентами, которые вели этот счёт.

Ливан подал иск против HSBC в Швейцарии, впервые обратившись в суд с иском против иностранного банка в связи с делом о коррупции, обвинив его в том, что он не провёл надлежащую проверку происхождения средств.

Досмотровые системы и современные требования безопасности

Ряд экспертов обращают внимание на растущий разрыв между современными требованиями к безопасности и широко используемым досмотровым оборудованием, главенствующую роль в котором по-прежнему играют устаревшие модели металлодетекторов.

Последние давно доказали свою эффективность в обнаружении потенциально опасных предметов при охране объектов и на публичных мероприятиях. В то же время им свойственны серьезные недостатки: ложные срабатывания, ограниченная чувствительность, необходимость в тщательной настройке в зависимости от конкретных условий эксплуатации, воздействие окружающей среды (атмосферные, электромагнитные помехи), дефицит обученных операторов, способных адекватно интерпретировать результаты сканирования и принимать соответствующие меры (подробнее см. https://1cpbo.ru/stati/plus-menus-metalodetector.html?ysclid=maw55w37bp407211156).

В то время как современные предприятия используют все более сложные системы управления бизнес процессами, охраной и безопасностью, традиционные металлодетекторы выглядят безнадежным анахронизмом, пишет Виктория Хэнскомб в журнале Security Journal Americas (digital.securityjournalamericas.com). Сегодняшние посетители приходят на предприятия и стадионы, в офисы, торговые центры и концертные залы с персональными электронными устройствами. Старые модели скрининга любой металлический предмет считают подозрительным.

Когда устаревшее оборудование не отличает реальные угрозы от ложных, службам безопасности приходится тратить время на дополнительный досмотр, возможно, отвлекая внимание от действительных рисков, удлиняя очереди, создавая нервозность и недовольство гостей, которые в массе своей сегодня более нетерпеливы и требовательны, чем двадцать лет назад. Не говоря уже о том, что длинные очереди чреваты потерей рабочего времени, нарушением спланированного хода массовых мероприятий.

Современная проверка, отмечает В. Хэнскомб, предполагает более детальную оценку и должна отвечать следующим требованиям:

- Быстрое и точное устранение потенциальной угрозы.
- Оптимизация времени ожидания в очередях в пиковые периоды.
- Минимизация ложных срабатываний.
- Согласование системы безопасности с другими операциями на объекте.
- Сочетание эффективности скрининга с соблюдением неприкосновенности частной жизни.
- Обеспечение ненавязчивого и уважительного подхода к людям.

Достижения в области биометрической идентификации, искусственного интеллекта (ИИ) и машинного обучения делают скрининг безопасности более эффективными. В отличие от традиционных систем, просто реагирующих на металлические предметы, решения на основе ИИ способны одновременно анализировать несколько характеристик: размер, форму, плотность и другие параметры. Аналитика в режиме реального времени позволяет выявлять структуру трафика, частоту посещений, соответственно корректировать протоколы.

Эксперты отмечают ряд тенденций, формирующих будущее систем досмотра.

Директор по специальным технологиям безопасности Группы компаний Систематика (www.tadviser.ru) Андрей Прозоров отмечает постепенное распространение новых регламентов и процедур контроля и досмотра, высокоэффективных технологий оперативного выявления (детектирования), распознавания, локализации и подавления угроз безопасности. В том числе, технологии скрининга и визуализации предметов, скрытых в одежде и под ней, непосредственно на теле человека, с помощью электромагнитных волн обратного рентгеновского рассеяния, радиоволн миллиметрового диапазона, неионизирующих электромагнитных волн терагерцового диапазона (электромагнитного излучения, спектр частот которого расположен между инфракрасным и микроволновым диапазонами), а также – интеллектуальной видеоаналитики, системы оценки психоэмоционального состояния людей, включая профайлинг (анализ действий, слов и мимики человека), виброимиджинг (оценка эмоционального состояния) и т.д.

Одновременно совершенствуются и традиционные досмотровые средства: стационарные арочные и ручные металлодетекторы, рентгенотелевизионные интроскопы, детекторы взрывных веществ и наркотиков, радиационные мониторы и другие виды современной техники.

Определенный оптимизм внушает динамика рынка систем автоматического скрининга безопасности, имеющих ключевое значение в различных секторах, включая аэропорты, другие объекты критической инфраструктуры, общественные мероприятия. Этот рынок, по прогнозам экспертов, достигнет 7,2 миллиарда долларов США к 2030 году, прибавляя в среднем на 9,5% с 2025 по 2030 год. Расширение рынка отражает глобальную тенденцию, при этом значительный рост прогнозируется в регионах Европы и Азиатско-Тихоокеанского региона (www.verifiedmarketreports.com)

Этот рост подчеркивает срочную необходимость инноваций в технологиях безопасности, побуждая производителей инвестировать в передовые системы визуализации, биометрию и искусственный интеллект для расширения возможностей обнаружения систем скрининга.

Как правильно подходить к формированию бюджета безопасности компании

Безопасность организации представляет собой ресурс, по важности для бизнеса не уступающий таким факторам как технологии, финансы, кадры и прочие важнейшие условия успешного развития. Вместе с тем, многие российские (и не только) компании финансируются по остаточному принципу, исходя из средств, которые правление компании готово потратить на службу безопасности.

Структура СБ компании в зависимости от профиля деятельности, типологии угроз включает четыре фундаментальных аспекта:

1. Внешние, физические угрозы для предприятия.
2. Внутренняя безопасность.
3. Информационная безопасность.
4. Финансовая безопасность.

Олег Попов, руководитель сервиса проверки сотрудника и контрагента UNIRATE24, указывает, что крупные компании тратят на безопасность 1% своей годовой выручки (www.unirate24.ru). Для средних и малых предприятий эта цифра существенно выше.

Основатель и директор компании HiveWatch, занимающейся технологиями безопасности, Райан Шонфельд пишет, что «руководители служб безопасности по-прежнему сталкиваются с необходимостью оправдывать свои растущие бюджетные потребности, демонстрировать их очевидную ценность для бизнеса» (Security Management, April, 2025).

Шонфельд утверждает: «сегодня руководители СБ должны подходить к составлению бюджета как к стратегическому мероприятию, которое согласуется с целями бизнеса».

Хорошо структурированный бюджет СБ – это уже не просто наличие необходимых ресурсов, но демонстрация того, как инвестиции в безопасность защищают активы, обеспечивают безопасность предприятий, поддерживают долгосрочное стратегическое планирование.

Составление бюджета включает несколько последовательных этапов (шагов).

Шаг 1. *Оценка ресурсов и способов высокой окупаемости инвестиций*

Следует учитывать несколько бюджетных категорий:

- Операционные расходы на повседневную деятельность.
- Капитальные вложения в долгосрочную инфраструктуру.
- Ассигнования на конкретные проекты.
- Расходы на персонал, включая обучение и повышение квалификации.
- Инвестиции в технологии, исключая избыточные и ненужные.
- Расходы на аутсорсинг и резервные фонды.

Шаг 2. *Создание межфункционального взаимодействия*

Представление, что служба безопасности работает в вакууме, безнадежно устарело. Приступая к оценке технологических решений, необходимо учитывать возможности интеграции технологий безопасности с бизнес системами, а также удобство их использования.

Шаг 3. *Подготовка к разговору с первыми лицами, принимающими стратегические решения*

Успех зависит от правильной, выверенной коммуникации с акционерами и топ-менеджментом. Надо хорошо разобраться, как работает процесс обсуждения и утверждения заявок на финансирование, какие данные и показатели необходимо продемонстрировать. Обязательно заблаговременно проговорить свой план с кем-то из представителей верхнего звена, чтобы на заседании правления получить поддержку.

Шаг 4. *Встреча лицом к лицу с C-Suite*

Вот тут-то и начинается самое интересное, замечает Шонфельд. Основная трудность – донести технические аспекты заявки до высокой аудитории. Руководители должны убедиться в окупаемости инвестиций, в их соответствии приоритетам бизнеса, в той пользе, которую они

принесут разным направлениям (управлениям) компании. Важно заранее подготовить ответы на трудные вопросы, например:

Можно ли отложить инвестиции до лучших времен?

Имеются ли экономически обоснованные альтернативы?

Чем можно заменить предлагаемые инвестиции, чтобы удовлетворить потребности в краткосрочной перспективе?

Как согласуются предложения с ключевыми показателями эффективности организации?

Какую пользу извлекут для себя другие управления организации?

Итак, главное внимание уделять демонстрации, как инвестиции в безопасность защищают и расширяют возможности бизнеса, обеспечивают измеряемую отдачу. Четко формулировать: «при вложении в X мы достигнем Y».

Какие киберучения нужны компаниям

Интерес российских компаний к киберучениям постоянно растет.

В 2023 году Группа компаний «Солар» при поддержке нацпроекта «Цифровая экономика» провела опрос, который показал, что 75% российских организаций намерены проводить киберучения, 52% респондентов уже применяли такой инструмент повышения практических навыков.

В 2024 году спрос на киберучения в России вырос на 25%, как можно судить по результатам исследования компании «Инфосистемы Джет», которая провела опрос более 200 организаций бизнес-сегмента.

Спрос и намерения еще не позволяют создать ясную картину, какой процент российских компаний реально проводит со своим персоналом занятия по ознакомлению с киберрисками и угрозами.

А в США такая статистика есть. Она показывает, что 52% американских организаций регулярно устраивают антифишинговые тренинги. Четверть компаний организуют учебу по распознаванию схем социальной инженерии.

В то же время 40% наемных работников вообще никогда не привлекались к занятиям по кибербезопасности. Таким образом, многие работающие американцы, похоже, слабо представляют себе методы кибератак, уловки хакеров, а еще хуже – как на них реагировать.

Эксперты считают, что вина за это лежит на работодателях, которые не рассматривают кибербезопасность как неотъемлемую часть своей работы.

Журналист и редактор Дж. Фрулингер в статье онлайн издания Chief Security Officer перечисляет и характеризует наиболее важные темы и вопросы для тренингов.

Фишинг и социальная инженерия

Мошеннические схемы социальной инженерии это не только зловредные письма в электронную почту. Злоумышленники все чаще используют голосовые и видео имитации, чтобы получить доступ в корпоративные сети, базы данных, финансы. Необходимо обучать персонал компаний, в первую очередь тех, кто имеет прямое отношение к финансам, по каким подозрительным или очевидным признакам можно идентифицировать мошенничество и как реагировать в таких ситуациях. Кстати, неплохо зарекомендовал себя такой метод учебы, как рассылка фальшивых («фишинговых») email-писем сотрудникам компании с целью проверки, кто как реагирует.

Пароли

Утомительная для пользователей, но все еще стержневая для кибербезопасности процедура.

Правила безопасного пользования корпоративными и личными (в том числе мобильными) устройствами для дистанционной работы

Своевременное и верное по адресату информирование об инциденте

Если одному работнику попытка фишинга представляется бесспорной, то другому, возможно, она кажется неочевидной. Поскольку преступники нередко совершают рассылку фишинговых писем «веерным» способом, то информирование не только службы кибербезопасности, но и коллег – самое правильное решение.

К настоящему времени во многих странах накоплен полезный опыт тренингов по кибербезопасности. Формы и методы учебы разные: видео симуляции, блог посты, интерактивные сценарии, упомянутые выше псевдофишинговые письма и так далее. Выбор большой. Главное, подчеркивает Фрулингер, они должны быть максимально интересны, адаптированы под служебные функции и задачи разных групп: топ-менеджмента, менеджеров среднего звена, тех, кто непосредственно работает с клиентами. Особую группу, требующую повышенного внимания, составляют сотрудники бухгалтерии.

Важно, чтобы в учебном процессе участвовали все департаменты и службы организации, включая первых лиц.

Тренинг не должен быть разовым мероприятием. Социологи и психологи выяснили, что полученные на таких занятиях знания выветриваются через несколько месяцев, а у кого-то и через пару недель. Авторы исследования «An investigation of phishing awareness and education over time: When and how to best remind users», проведенного USENIX (Ассоциация передовых вычислительных систем), утверждают, что наилучшая периодичность для занятий - каждые четыре месяца.

Конечно, нельзя упускать из виду и стоимость тренингов. Поэтому немаловажное значение приобретает измерение эффективности таких занятий для бизнеса. Такое измерение в разных странах организовала, к примеру, международная маркетинговая аналитическая компания Aberdeen. Ее эксперты, проведя ряд исследований, пришли к выводу, что регулярное проведение занятий по ознакомлению с киберрисками снижает годовые показатели риска успешных атак на 50%, а негативное воздействие на бизнес – на 72%.

Мошенники в компании: мотивы и характерные черты

В мае месяце этого года в МВД России рассказали об особенностях и мотивах мошенников. Последние часто ничем не выделяются внешне и легко сливаются с толпой. Их основные мотивы – корысть и желание самоутвердиться за счет жертв. В МВД подчеркнули, что у мошенников есть слабые стороны: они опасаются уточняющих вопросов и проверки информации, а также теряют интерес, если понимают, что собеседник осведомлен и уверен в себе. (подробнее: https://vz.ru/news/2025/5/16/1332520.html?ysclid=marxvk683c324132465).

В книге В.А. Зверева «Как защититься от мошенничества на финансовом рынке», 2019 г., со ссылкой на исследования психологов, выделяются некоторые категории сотрудников банков, имеющие возможные мотивы для совершения мошенничества. Это в первую очередь люди, которые имеют большие личные долги или финансовые запросы, приверженные к высокорискованным операциям, сотрудники с неясным или уголовным прошлым.

Мотивацией для мошенничества, пишет автор, могут быть такие факторы, как недооценка своих успехов, чувство неудовлетворённости работой, боязнь ее потерять, невыдача премиальных, ощущение, что тебе платят меньше, чем того заслуживаешь. Мошенником может стать любой человек, если ситуация благоприятствует совершению преступления.

К мошенничеству подталкивают человеческие пороки: азарт (поймают или не поймают), просто желание украсть то, что плохо лежит (мания обогащения), нежелание работать, пагубные пристрастия к азартным играм, наркотикам, дорогим сексуальным удовольствиям, жизнь не по средствам, большие долги, большие финансовые потери, неожиданная потребность в деньгах, зависть к руководителю, игра и проигрыш в казино, женитьба и др.

Относительным оправданием мошенничества могут быть и условия, в которые попал человек. Например. если он поставлен перед выбором — быть уволенным в период кризиса, остаться без денег, превратиться в бомжа или пойти на мошенничество. В отдельных случаях выбирают второе. Давление внешних обстоятельств связано чаще всего с финансовым неблагополучием (https://kartaslov.ru).

На сайте организации Financial Crime Academy (financialcrimeacademy.org) встречаем попытку классификации мотивов внутрикорпоративных преступлений. Наиболее распространенные мотивы:

- Жадность
- Финансовые потребности
- Патологическое желание совершить преступление
- Желание бросить вызов системе — менталитет «поймай меня, если сможешь»
- Принуждение (людей могут заставлять что-то делать их коллеги, семья или начальство)
- Использование средств для приобретения незаконных товаров, таких как наркотики или огнестрельное оружие
- Идеология (ради «высшей цели», как в случае с террористическими организациями)

Следователи и аудиторы должны понимать, указывают эксперты, что побуждает людей совершать мошенничество, чтобы лучше оценивать риски и помогать работодателям или клиентам в реализации соответствующих превентивных и следственных мер. У большинства мошенников, от топ-менеджера до рядового сотрудника, есть одна общая черта: они почти никогда не устраивались на работу с намерением совершить мошенничество, но когда то совершают его впервые.

Мошенничество происходит на всех уровнях организации, но есть определённые тревожные сигналы, которые должны предупреждать о потенциальных угрозах на каждом уровне. Реальные случаи организационного мошенничества проанализированы в докладе Ассоциации сертифицированных специалистов по расследованию мошенничества «2014 ACFE Report to the Nations». Наиболее часто упоминались следующие факторы:

- Они живут не по средствам (самый распространённый тревожный сигнал, встречавшийся в 44% случаев.)
- Финансовые трудности составляют 33% всех случаев.
- Необычайно тесные отношения с поставщиком или клиентом (22% случаев).
- Проблемы с контролем, отказ от разделения обязанностей (21% случаев).

Среди экспертов популярен термин «треугольник мошенничества», разработанный криминологом Дональдом Кресси. Он описывает три элемента, которые повышают риск мошенничества: (1) возможность, (2) стимул и (3) рационализация. Треугольник мошенничества помогает понять, почему обычные люди совершают мошенничество при определенных обстоятельствах.

Зная, какие признаки указывают на мошенничество, принимая соответствующие превентивные меры, компании могут потенциально снизить распространенность таких злоупотреблений. Признание того, что каждый человек при определённых обстоятельствах может стать мошенником, подчёркивает необходимость постоянной бдительности и значение принципа «доверяй, но проверяй».

Рецензия
Physical Security Reimagined: A Masterclass for the Future: Next Generation Physical Security
by Prateek Prehar

В наше время, когда проблемы безопасности становятся все более динамичными и сложными, книга «Переосмысление физической безопасности: мастер-класс для будущего: следующее поколение физической охраны» по новому интерпретирует представления о безопасности. Она отражает новаторский комплексный подход, объединяющий человеческие ресурсы, передовые технологии и стратегические концепции для разработки и реализации современных решений в этой области.

Монография представляет собой мастер-класс, предназначенный для специалистов по безопасности, руководителей компаний и студентов, изучающих сферу охранных услуг, корпоративной безопасности. Она помогает если не устранить, то хотя бы сократить существующий разрыв между теоретическими концепциями и практическим применением знаний, предлагая действенные рекомендации по разработке, внедрению и управлению программами безопасности в различных экономических отраслях.

Благодаря подробному анализу, реальным примерам из практики и инновационным моделям оценки рисков автор показывает, как следует оптимизировать инвестиции в безопасность в зависимости от меняющихся угроз. Он предлагает читателям инструменты, помогающие выйти за

рамки традиционного представления о физической охране. Одновременно объясняет и подчёркивает значение интеграции, предвидения и адаптивности систем безопасности.

Независимо от того, является ли читатель опытным специалистом по безопасности, владельцем бизнеса, которому приходится нести значительные расходы на охрану и безопасность, или начинающим профессионалом, стремящимся заявить о себе в этой сфере, эта книга дает знания, необходимые для того, чтобы претендовать на лидерские позиции в охранной индустрии.