Охрана предприятия

№ 5 (98) 2025

Оглавление

Управление рисками в финансовой сфере. Какие компетенции и навыки востребованы сегодня?

Сфера корпоративных рисков развивается беспрецедентными темпами благодаря стремительному технологическому прогрессу, глобализации и ужесточению нормативных требований. Цифровая трансформация экономики и бизнеса сопровождается появлением огромного числа новых уязвимостей. Многие компании оказались не готовыми к встрече с новыми угрозами.

Согласно проведенному в конце 2024 года исследованию «2024 Global State of Risk Oversight: Managing the Rapidly Evolving Landscape**»** (организаторы: компания Enterprise Risk Management Initiative и Центр управления корпоративными рисками при Университете штата Северная Каролина) *48% руководителей компании по всему миру сталкиваются с неожиданными и серьезными рисками* **(**https://erm.ncsu.edu).

Опрос показал, что факторы неопределенности способствуют возникновению неожиданных рисков, чреватых иногда катастрофическими последствиями. Компании недостаточно инвестируют в систему управления рисками. Во многих организациях отсутствуют базовые компоненты управления рисками, поскольку их руководители считают это направление «отвлекающим фактором» от более важных стратегических задач. Только 32% опрошенных считают, что практика контроля рисков в их организациях является зрелой или надежной. И всего 17 % участников исследования отметили, что процесс управления рисками позволяет им получать информацию, обеспечивающую конкурентное преимущество.

В эпоху беспрецедентных перемен и неопределённости специалисты в сфере финансов приобретают ключевую роль в укреплении системы контроля и управления рисками в своих организациях. Согласно другому опросу, проведенному консультативной группой Future of Finance

Leadership Advisory Group (https://blionline.org/future-of-finance), 43% респондентов отметили, что финансовый директор и финансовый отдел контролируют внедрение ERM (Enterprise risk management) в их организациях.

Чтобы успешно участвовать в процессе контроля и управления рисками в своих компаниях , специалистам в области бухгалтерского учёта и финансов недостаточно узко профессиональных компетенций. Им необходимо развивать различные навыки. О них пишет на сайте Chief Financial Officer Том Худ, исполнительный вице-президент консалтинговой финансовой организации AICPA & CIMA (https://www.cfo.com):

Аналитические навыки

Способность анализировать сложные массивы данных и выявлять тенденции имеет решающее значение для эффективного контроля и управления рисками. Это подразумевает не только понимание финансовой отчетности, но и знание экономических показателей, а также отраслевых и рыночных тенденций, чтобы прогнозировать риски, их вероятность, причины и влияние на организацию.

Стратегическое мышление

Специалисты в области бухгалтерского учета и финансов должны развивать и демонстрировать способность видеть не только цифры, но и понимать более широкий контекст бизнеса. В частности, это подразумевает согласование стратегии управления рисками с общими целями и задачами организации, а также понимание ее текущего положения и будущего направления развития.

Коммуникативные навыки

Необходимы как для сбора информации о рисках в организации, так и для предоставления высококачественных рекомендаций руководителям высшего звена, а также внутренним и внешним аудиторским комитетам. Это включает представление сложных данных в понятной форме и приведение убедительных аргументов в пользу стратегии по снижению рисков.

Технологические навыки

Чтобы лучше справляться со своей работой, специалисты в области финансов должны быть знакомы с программным обеспечением для управления рисками и инструментами анализа данных. Сюда входят такие технологии, как Большие Данные, машинное обучение и искусственный интеллект, которые помогают экономить время, сокращать количество ошибок и поддерживать стратегическое мышление.

Знания в сфере регулирования

Понимание нормативно-правовой среды и требований к соблюдению законодательства – важный компонент контроля и управления рисками, помогающий выявлять юридические риски и обеспечивать соблюдение организацией всех соответствующих законов и нормативных актов. Специалистам в области бухгалтерского учета и финансов необходимо уделять время изучению последних изменений в нормативно-правовой сфере и понимать, как они влияют на их организацию.

Адаптивность

Поскольку ситуация с рисками постоянно меняется, специалистам в области бухгалтерского учета и финансов необходимо уметь быстро перестраиваться и соответствующим образом корректировать стратегии, чтобы эффективно снижать текущие риски и опережать возникающие.

Специалисты по финансам должны брать на себя инициативу по преобразованию системы контроля и управления рисками из реактивного процесса в проактивную стратегию, чтобы подготовить организации к преодолению сложностей современного бизнес-ландшафта.

Мультифакторная аутентификация для финансовой безопасности

Глоссарий терминов Familiarize Team (https://docs.familiarize.com/ru/glossary) дает такое определение многофакторной аутентификации:

«Многофакторная аутентификация (MFA) — это протокол безопасности, который требует от пользователей предоставления нескольких форм проверки для доступа к конфиденциальным данным или системам. Используя MFA, организации могут значительно снизить риск несанкционированного доступа к финансовым счетам и конфиденциальной информации».

Эксперты отмечают, что по мере эволюции киберугроз меняются стратегии и методы внедрения MFA. В числе последних способов:

- *Аутентификация без пароля*: некоторые организации исключают пароли, полагаясь исключительно на биометрию или аутентификацию на основе специального устройства безопасности.
- *Адаптивная аутентификация:* этот метод оценивает факторы риска в реальном времени, корректируя уровень требуемой аутентификации в зависимости от поведения пользователя и его местоположения.
- *Интеграция с блокчейном:* новые технологии, такие как блокчейн, все чаще используются для проверки личности, что помогает снижать зависимость от традиционных способов многофакторной аутентификации.

Специалисты крупной финансовой организации First Western Trust (6 миллиардов долларов аффилированных активов) не сомневаются, что MFA имеет решающее значение для финансовой безопасности по следующим основаниям:

1. *Снижает риск кражи учётных данных*

Даже если хакер получит пароль, он не сможет войти в учетную запись без второго фактора аутентификации.

2. *Предотвращает фишинговые атаки и атаки с использованием методов социальной инженерии*

Киберпреступники часто используют тактику фишинга, чтобы обманом заставить людей раскрыть свои пароли. Многофакторная аутентификация предотвращает такие атаки, требуя дополнительного подтверждения.

3. *Усиливает защиту банковских и инвестиционных счетов*

Финансовые учреждения поощряют использование MFA для транзакций с высокой стоимостью, чтобы гарантировать, что неавторизованные пользователи не смогут переводить средства или получать доступ к конфиденциальным данным.

4. *Повышает безопасность при подмене SIM-карты*

Вместо аутентификации по SMS использование многофакторной аутентификации на основе приложений значительно снижает риск мошенничества с подменой SIM-карты, когда киберпреступники перехватывают телефонные номера.

Эксперты First Western Trust Bank советуют:

- Избегайте многофакторной аутентификации на основе SMS; вместо этого используйте такие приложения, как Google Authenticator или Microsoft Authenticator, для дополнительной безопасности.
- Включите многофакторную аутентификацию на всех финансовых и инвестиционных счетах. Это касается онлайн-банкинга, платформ для торговли акциями и криптовалютных кошельков.
- Регулярно проверяйте и обновляйте настройки безопасности — периодически проверяйте настройки многофакторной аутентификации и параметры безопасности учетной записи, чтобы обеспечить максимальную защиту.
- Используйте аппаратные ключи безопасности для дополнительной защиты. Такие устройства, как YubiKey (аппаратные ключи безопасности) обеспечивают дополнительный уровень безопасности помимо паролей и приложений для аутентификации (https://myfw.com/articles/why-multi-factor-authentication-mfa-is-a-must-for-financial-security)

Многие эксперты и практики в области корпоративной безопасности предупреждают против использования МФА как *единственной защитной меры*. Они указывают, что злоумышленники адаптируются, совершенствуют приемы обхода и добиваются неплохих результатов. Поэтому, считают специалисты, MFA должна быть не более чем частью более крупной программы безопасности, одним из уровней глубокой защиты.

Комплексный подход глубокой защиты включает в себя множественные, пересекающиеся меры безопасности. Вот как аналитики корпорации Касперского (https://www.securitylab.ru) рекомендуют укрепить защиту от обхода MFA:

— Усиление защиты конечных точек.

— Инвестиции в защиту от фишинга.

—Использование более защищённых методов MFA, таких как аппаратные ключи безопасности (FIDO2) или биометрия, которые менее уязвимы к фишингу.

—Использование специальных инструментов для обнаружения, расследования и автоматического реагирования на захваты учётных записей в облаке.

—Обучение сотрудников навыкам распознавания попыток фишинга и других методов социальной инженерии, направленных на учетные данные MFA.

— Подготовка к инцидентам и восстановлению.

Бэкграундные проверки при найме: границы возможного

Проверка кандидатов на вакансии является общепринятой практикой и составляет важную часть практически любого процесса найма.

Автор ряда статей в журнале «Совкомблог» Артур Сафин называет стандартный набор проверок:

- Сведения о предыдущей работе.
- Долги по исполнительным производствам.
- Судебные дела.
- Банкротство.
- Кредитная история.

Сафин включает в перечень также информацию от соседей, оговариваясь, что эта проверка скорее исключение, чем правило. Подробнее см.: **https://journal.sovcombank.ru/rabota/chto-proveryaet-sluzhba-bezopasnosti-pri-prieme-na-rabotu?ysclid=mclnsbgies551634433).**

Далеко не все организации осознают, что существует множество юридических ограничений, накладываемых на обработку персональных данных. То, что разрешено или требуется, варьируется в зависимости от страны. В Европе, к примеру, различные законы (не только о конфиденциальности, но и о реабилитации правонарушителей, трудовом законодательстве, нормативных актах и других отраслевых правилах) накладывают существенные ограничения на разрешенные виды проверок биографических данных в зависимости от конкретной ситуации.

В России, как и в Европе, рискованно требовать от кандидатов на должность заполнение анкеты при трудоустройстве. За это можно получить до 700 тысяч рублей штрафа, читаем на сайте https://www.rnk.ru. Эксперты утверждают, что анкета не входит в перечень документов, которые работник обязан предоставлять при трудоустройстве (ст. 65 ТК). Поэтому требовать ее заполнить работодатель не может. Отказать в приеме на работу из-за незаполненной анкеты тоже нельзя. За это ГИТ (Трудовая инспекция) может оштрафовать на 50 тыс. руб.

Кроме того, лишнюю информацию нельзя требовать по Закону от 27.07.2006 № 152-ФЗ "О персональных данных". Он запрещает заставлять кандидатов предоставлять сведения о родственниках. Чтобы обезопасить работодателя, в документе надо прописать, что кандидаты предоставляют анкету *по желанию*. В анкете не должно быть сведений, которые не относятся к деловым качествам будущего работника, а также информации о третьих лицах, например о родственниках (подробнее: https://www.rnk.ru/news/224250-za-anketu-pri-prieme-na-rabotu-mojno-poluchit-do-700-tysyach-rubley-shtrafa?ysclid=mclo545gbx719774387).

Относительно кадровых проверок Роскомнадзор выпустил документ "Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве", с которым можно ознакомиться детально по ссылке
https://legalacts.ru/doc/razjasnenija-roskomnadzora-voprosy-kasaiushchiesja-obrabotki-personalnykh-dannykh/?ysclid=mcloc0owqv50502047

В Европе все намного суровее.

В 2022 году испанское ведомство по защите данных (DPA) оштрафовало компанию, занимавшуюся сбором справок об отсутствии судимостей, на 2 миллиона евро за отсутствие законных оснований. DPA обнаружило, что такие справки о благонадёжности (т. е. документы, подтверждающие отсутствие судимостей) содержат персональные данные, связанные с судимостями и правонарушениями в значении статьи 10 Общего регламента ЕС по защите данных

(GDPR). Соответственно, информация не должна была обрабатываться без соответствующего разрешения, а в испанском законодательстве такого разрешения нет. В сентябре 2022 года французское DPA оштрафовало компанию за чрезмерный сбор данных в процессе найма и проверку криминального прошлого сотрудников без законных на то оснований. Несколькими месяцами ранее итальянское DPA оштрафовало компанию за незаконную проверку криминального прошлого сотрудников.

Предлагаем читателям рекомендации западных экспертов на это счет. Они не бесполезны и для российских компаний.

Прежде чем проводить какие-либо проверки анкетных данных, организация должна в каждом конкретном случае определить, какие проверки *требуются по закону и какие разрешены* в данной юрисдикции. В каждом конкретном случае следует тщательно учитывать специфику должности, любые отраслевые особенности и предполагаемую цель проведения таких проверок. Организации должны быть особенно внимательны, если они намерены проводить следующие виды проверок анкетных данных:

- *Проверка наличия опыта работы:* организация должна быть в состоянии обосновать, почему проверка наличия опыта работы (включая запросы на предоставление подтверждающих документов) необходима для оценки соответствия кандидата предполагаемой должности. Существует риск того, что такие проверки могут быть сочтены чрезмерными и навязчивыми.
- *Проверка кредитоспособности:* тип финансовой/кредитной проверки зависит от отрасли предполагаемой работы. В большинстве случаев проверка финансового прошлого должна ограничиваться кандидатами на должность или сотрудниками, чья должность требует высокого уровня честности, или в тех случаях, когда такая проверка требуется по закону.
- *Проверка в социальных сетях:* в большинстве случаев сложно обосновать необходимость проверки в социальных сетях для всех кандидатов на должность. При поиске общедоступной информации, содержащейся в социальных сетях (включая веб-сайты кандидатов, блоги, видеоблоги и т. д.), организациям следует ограничиться проверкой информации, содержащейся на общедоступных профессиональных веб-сайтах, а не в личных аккаунтах в социальных сетях. Организации также должны соблюдать условия предоставления услуг поставщиками социальных сетей, которые часто запрещают несанкционированный сбор информации из социальных сетей автоматизированными средствами.

Правила, касающиеся законности и масштабов проверки анкетных данных, различаются в зависимости от юрисдикции. В некоторых странах (например, в США) организации могут проводить более тщательную проверку, чем в других (например, в большинстве стран — членов ЕС). В Великобритании некоторые финансовые учреждения обязаны проводить дополнительные проверки кандидатов, например, тех, кто предположительно должен консультировать или оформлять ипотечные кредиты или инвестиции, работать со страховыми контрактами, предоставлять финансовые консультации.

Если работа сопряжена с потенциальным риском для безопасности других людей, например, при работе с тяжелой техникой, вождении транспортных средств или обращении с опасными продуктами, от кандидатов могут потребовать пройти тестирование на наркотики, чтобы убедиться, что они по состоянию здоровья способны безопасно выполнять свою работу. Однако для большинства должностей, например, для сотрудников службы поддержки клиентов и основных административных должностей, такие проверки вряд ли оправданны.

Организации должны тщательно продумывать, какая информация требуется для оценки соответствия кандидата, и не забрасывать сеть слишком широко. Такой подход позволяет снизить риск последующих исков о дискриминации со стороны кандидатов, которые могут быть поданы,

если организация слишком глубоко копает в жизни кандидата и получает информацию, не имеющую отношения к работе.

По мнению А. П. Де Цварт, Партнера Morrison & Foerster (транснациональная юридическая корпорация), прежде чем проводить какие-либо новые или существующие проверки, организация должна:

- Определить характер и соответствующий масштаб проверок.
- Выяснить, разрешены ли проверки анкетных данных действующим местным законодательством.
- Зафиксировать основания для сбора информации.
- Обосновать правовой аспект обработки персональных данных. Определить, существует ли какой-либо соответствующий закон, разрешающий обработку данных о судимостях и правонарушениях, учитывая контекст и цели обработки.
- Перед проведением проверок предоставить кандидатам отдельное уведомление о конфиденциальности, в котором будет четко разъяснено, 1) почему организация проводит проверки; 2) правовая основа для обработки собранной личной информации, 3) где организация получает личную информацию и 4) будет ли организация делиться личной информацией и с кем.
- Проводить проверку анкетных данных на последних этапах процесса.
- Удалить персональные данные**,** собранные после того, как станет ясно, что предложение о работе отклонено или кандидат не прошел проверку.
- Регулярно пересматривать правила и процедуры проверки анкетных данных, чтобы убедиться, что они соответствуют текущей практике организации и меняющимся законодательным требованиям.

Весь это набор мер может показаться обременительным занятием, указывает Де Цварт. «Но если вы хотите снизить риск возможных жалоб в регулирующие органы, привлечь внимание регулирующих органов и все, что с этим связано, было бы разумно заранее наладить процесс проверки анкетных данных в соответствии с местными требованиями в тех юрисдикциях, где у вашей организации есть сотрудники. Этот процесс можно внедрять поэтапно, с учетом различных приоритетов, но в конечном итоге это поможет избавиться от множества проблем в будущем» (https://www.mofo.com).

Мошенничество ради эффективности?

В бесчисленных публикациях о фроде авторам представляется неоспоримым казалось бы очевидный и банальный тезис: мошенничество приносит вред бизнесу/экономике.

В подтверждение этой «азбучной истины» приводится убедительная статистика. Так, одно из последних исследований в России, проведенное в 2025 году компанией edna (решения в сфере цифровых коммуникаций - https://edna.ru), показало, что с прямыми финансовыми убытками сталкиваются 25% компаний, подвергавшихся фрод-атакам. Еще 18% отметили, что из-за мошенничества увеличились операционные расходы. Также фрод искажает данные аналитики, что мешает принимать правильные маркетинговые решения. В ходе опроса 1 328 предпринимателей, владельцев бизнесов, топ-менеджеров крупных и средних компаний каждый пятый респондент отметил, что после фрод-атаки на компанию случились перебои в работе -

клиенты, которые получили фрод-рассылку, звонили в компанию и увеличивали нагрузку на колл-центры. Кроме того, 12% участников опроса сталкивались с кадровыми потерями после инцидентов, а еще 14% - с репутационным ущербом.

На этом фоне несколько неожиданными звучат голоса тех предпринимателей, которые оправдывают мошенничество «во благо эффективности бизнеса». Подобные суждения необычны и редки, но они есть, и редакция журнала «Охрана предприятия» не смогла пройти мимо публикации на сайте Ассоциации сертифицированных экспертов по борьбе с мошенничеством (https://www.acfe.com) «Как лидеры бизнеса во имя эффективности оправдывают мошенничество».

Автор этой статьи, доктор философии Принсли Дибиа, пишет, что мошенничество не всегда совершается со злым умыслом. Иногда оно оправдывается руководством компаний как необходимый компромисс для выживания на конкурентном рынке. Когда усиливается конкуренция и давление рынка, моральные постулаты, лежащие в основе борьбы с мошенничеством, могут ослабевать. В результате формируется культура, в которой допускаются мелкие нарушения, контроль отходит на второй план, а этические проблемы увязываются с неэффективностью бизнеса.

Более того, некоторые руководители организаций преподносят неэтичное поведение как стратегически или коммерчески оправданное. В этом случае мошенничество перестает восприниматься как нарушение. Оно становится приемлемой операционной реальностью.

Принсли Дибиа обращается к «теории нейтрализации», разработанной Дэвидом Матцей и Грешемом Сайксом в 1950-х и 1960-х годах. Эта теория исследует, как люди, совершающие преступления, оправдывают свои действия, чтобы смягчить чувство вины и избежать ответственности. Матца и Сайкс выделили пять конкретных тезисов: отрицание ответственности, отрицание ущерба, отрицание жертвы, осуждение осуждающих и апелляция к высшим ценностям. Каждое из этих оправданий, как представляется правонарушителям, «позволяет рационализировать» свое поведение, перекладывая вину на других или преуменьшая предполагаемый вред от своих действий..

Отрицание ответственности. «У нас не было выбора. Из-за ограниченного штата и бюджета пришлось пойти на компромисс».

Преступник утверждает, что обстоятельства вынудили его совершить данное преступление. По этой причине он/она не чувствует личной ответственности за преступление или его последствия. Распространенным аргументом в этой категории является заявление о том, что «другие люди вынудили совершить неприемлемое действие», даже если это не соответствует действительности.

Отрицание ущерба. «Это мелочь. Она едва ли повлияет на ситуацию в финансовом плане».

Преступник настаивает на том, что его действия не причинили вреда и, следовательно, не являются преступлением. Такой аргумент часто используется в случаях, когда жертва не очевидна, например, человек может незаконно скачивать фильмы или музыку и не чувствовать себя виноватым, потому что вред от его действий не очевиден. Люди также могут утверждать, что злонамеренные розыгрыши или оскорбительные высказывания были шуткой, даже если они причинили вред.

Отрицание жертвы. «На самом деле никто не пострадал. Это просто формальности».

Осуждение осуждающих. «Аудиторы не понимают, как устроен бизнес».

Апелляция к более высоким чувствам. «Мы сделали это для команды, чтобы поддержать компанию на плаву».

В последнем случае преступник может заявить, что негативные или незаконные действия были оправданными, поскольку способствовали достижению положительного результата. Например, человек, укравший товар или деньги, может заявить, что сделал это, чтобы помочь больному ребенку. По такому раскладу преступление «не является таковым», поскольку де оно было совершено ради высшей цели.

Каждая из перечисленных «рационализаций» помогает менеджерам и бизнесменам поддерживать имидж честного человека, когда они допускают или игнорируют неэтичное поведение. В результате формируется корпоративная культура, в которой мошенничество — это не то, что нужно предотвращать, а то, чем нужно управлять и что нужно терпеть.

Изучая эти модели мышления, криминологи стремятся выявить глубинные убеждения, способствующие совершению преступлений, чтобы предупреждать и сокращать мотивированные правонарушения в будущем.

Искусственный интеллект в охранной индустрии: преимущества и «подводные камни»

Искусственный интеллект и машинное обучение выводят охранную индустрию на качественно новый уровень.

Эксперты российской частной охранной компании Hanston (https://hanston.ru) выделяют как приоритетные следующие сферы применения ИИ в сфере охраны и безопасности:

- Мониторинг видеонаблюдения. Использование алгоритмов распознавания лиц и поведения для автоматического выявления подозрительной активности.
- Прогнозирование инцидентов безопасности. Анализ исторических данных для определения потенциальных рисков и угроз.
- Управление доступом на охраняемые объекты.
- Автоматизация рутинных процессов.

Наиболее активно элементы ИИ используются сегодня в системах видеонаблюдения, отмечают специалисты из Группы компаний «Сигма-Профи» (https://sigma-profi.com/). “Умные” комплексы на основе нейронных сетей превращают видеокамеру в аналитический центр: считывание движений тела, мимики лица, сетчатки глаза и других внешних данных делает возможным пресечение преступных намерений еще до совершения преступления.

В системе управления охраной сложных объектов ИИ позволяет решить важную задачу сбора информации о текущем состоянии безопасности, определения ее уязвимых мест, прогнозирования рисков и возможных угроз.

Охранная система с применением ИИ становится мультирубежной: она делится на отдельные независимые кластеры, которые объединяются одним управляющим центром. Еще одним значимым преимуществом охранных систем с применением ИИ стала их способность к трансформации, что позволяет в любой момент настраивать их фактически под любые требования заказчика.

О преимуществах ИИ можно говорить много и долго. Но не менее важно знать и понимать ***потенциальные опасности и подводные камни***, которые могут возникнуть в процессе

внедрения технологий ИИ в сферу охраны и безопасности. А именно об этом пишет Матс Тулин, директор по основным технологиям в компании Axis Communications, в журнале Security Management (https://www.asisonline.org/security-management-magazine).

По его мнению, в современном мире ответственность означает не только то, что технология не должна использоваться незаконным или ненадлежащим образом, но и то, что приоритет должен отдаваться открытости и прозрачности, чтобы пользователи понимали, как работает технология и как ее применять наиболее эффективно.

Поставщики услуг в сфере безопасности, считает Тулин, используют ИИ для достижения двух основных целей: автоматизации задач и получения полезной информации.

Возможность автоматизировать некоторые элементы обнаружения и реагирования произвела революцию в видеоаналитике в том виде, в каком мы ее знаем. Теперь компаниям не нужно полагаться на сотрудников службы безопасности, которые следят за настольными или настенными мониторами, — их решения по обеспечению безопасности способны автоматически оповещать о потенциальном инциденте.

Но у автоматизации есть недостатки. Например, аналитика на основе ИИ хорошо справляется с ложными срабатываниями, проверяя потенциальные инциденты, связанные с безопасностью, перед отправкой оповещений. Но каковы могут быть последствия, если ИИ примет неправильное решение? Важно знать, в каких случаях необходимо участие человека.

При оценке рисков прозрачность крайне важна. Компаниям необходимо точно знать, на что способны их решения на основе ИИ и на что не способны. Если поставщики технологий предоставляют неполную информацию, преувеличивают возможности, то могут подорвать доверие клиентов к их решениям. А поскольку инструменты на основе ИИ становятся все более популярными, распространение дезинформации может нанести серьезный ущерб.

Современные решения для обеспечения безопасности на основе ИИ генерируют значительные объемы данных, которые организации используют для лучшего понимания, что происходит в том или ином месте, и принятия решений. Крайне важно, чтобы организации понимали границы возможностей как модели ИИ, так и массива данных, которые она анализирует, а также были осведомлены о потенциальных предубеждениях.

Если аналитические системы постоянно испытывают трудности при работе в условиях разного освещения или погоды, об этом важно знать приобретателю технологии. Знание того, как решения работают в разных условиях, неизбежно влияет на эффективность их применения.

Генеративный ИИ быстро развивается, а это значит, что влияние этих новых инструментов — как положительное, так и отрицательное — еще недостаточно изучено. Инновационные решения не обладают таким же уровнем зрелости, как прежние аналитические решения, и производителям, поставщикам необходимо оценить, как алгоритмы работают в средах, где клиенты будут их использовать. Важно с осторожностью относиться к новым технологиям, и чем больше информации поставщики могут предоставить клиентам, тем лучше. Ни одно решение не является идеальным, но выявление потенциальных проблем — важный первый шаг к их ответственному решению.

Пожалуй, самый важный шаг, заключает Матс Тулин, это выстраивание тесного взаимодействия производителей, поставщиков, интеграторов и пользователей на протяжении всего цикла продаж и жизненного цикла продукта.

Учитывая темпы развития технологий, трудно предсказать, как будет выглядеть ИИ через год, не говоря уже о пяти или десяти годах. Такая неопределенность создает трудности, но одновременно это время идеально для того, чтобы сделать ИИ открытым и прозрачным.

Охранное видеонаблюдение: основные тенденции в 2025 году

Компания Eagle Eye Networks, Inc. (системы видеонаблюдения для физической охраны) опубликовала исследование об основных тенденциях в сфере видеонаблюдения в текущем году (https://www.een.com/video-surveillance-trends).

Авторы выделили следующие главные направления:

Удаленный мониторинг

Благодаря искусственному интеллекту и облачным технологиям удаленный мониторинг объектов охраны стал сегодня самым практичным и экономичным решением. Компании получили возможности централизации охранных операций, организации прямых трансляций и одновременной аналитики с любого места. Эффективность выражается в сокращении штата охранников, уменьшении расходов на охрану крупных объектов.

Расширение зоны наблюдения

Службы безопасности теперь могут размещать видеокамеры с искусственным интеллектом в любом месте на открытом воздухе, даже там, где это было невозможно из-за отсутствия источника питания и интернета, например, на сельскохозяйственных полях, удаленных строительных площадках, в труднодоступной горной местности. «Умные» камеры могут анализировать видеопотоки на месте, обнаруживать объекты, распознавать лица и выявлять аномалии, не полагаясь на внешние системы обработки данных.

Мультисенсорные камеры

Мультисенсорные камеры становятся одним из краеугольных камней современного видеонаблюдения. Они охватывают намного б***о***льшие территории меньшим числом устройств. В отличие от камер с одним объективом, эти системы обеспечивают широкоугольный или панорамный обзор, сводя к минимуму слепые зоны и сокращая потребность в установке нескольких камер. Они наиболее эффективны для использования в аэропортах, на стадионах, в крупных торговых центрах.

Обнаружение оружия

Обнаружение оружия с помощью ИИ становится ключевой мерой безопасности в школах, торговых центрах и общественных местах, пишет Ханс Калер, главный операционный директор Eagle Eye Networks на веб-сайте https://facilitiesmanagementadvisor.com. Однако у этой технологии есть и ограничения относительно обнаружения скрытого оружия. В дальнейшем эти ограничения можно преодолеть с помощью более совершенной поведенческой аналитики.

Использование в условиях недостаточной освещенности.

Усовершенствованные датчики изображения позволяют камерам снимать четкое видео даже в практически полной темноте. Они существенно расширяют возможности ИИ распознавать лица и считывать номерные знаки автомобилей.

Информационно-аналитический журнал «Rubеж» (https://ru-bezh.ru) весной 2025 года провел опрос группы российских экспертов относительно состояния и тенденций развития видеонаблюдения. Полученные результаты позволили сформулировать следующие актуальные направления развития видеонаблюдения в России:

- ИИ и видеоаналитика
- ИИ с предиктивной аналитикой
- Edge-вычисления (обработка данных на камерах для автономных систем на удаленных объектах)
- Экосистемы (углубленная интеграция видеонаблюдения с другими системами безопасности)
- Цветное изображение в темноте: переход на светодиодную подсветку
- Рост доли российских производителей
- Мультисенсорные камеры
- Создание полностью автономных систем

В то же время отмечаются и проблемы:

- Низкий спрос на ИИ в B2C-сегменте (business to consumer — бизнес для потребителя). Востребованы только базовые функции (распознавание номеров, контроль доступа)
- Дефицит кадров. Нехватка специалистов по «embedded-разработке» (разработке встроенного ПО) и ИИ
- Риски «псевдолокализации» — даже сертифицированное оборудование может остаться сборкой китайских компонентов.
- Дефицит кастомизации**.** Практически отсутствуют решения для узких задач, например, камеры с видеоаналитикой для контроля этажности в строительстве. (подробнее см. https://ru-bezh.ru/infografika/videonablyudenie-smotrit-vglub-novyh-napravleniy-osnovnye-trendy?ysclid=mckdkzoyem162775248).

Современные аудиотехнологии для охраны и безопасности

Аудиоаналитика с развитием цифровых технологий становится одним из еще малоизученных, но весьма перспективных направлений в сфере корпоративной безопасности.

Специалисты охранной компании Гольфстрим (https://gulfstream.ru/) указывают на огромный, но пока слабо реализуемый потенциал программной аудиоаналитики, которая способна:

- задавать параметры автоматического оповещения о возникших угрозах;
- предотвращать возможные инциденты;
- сводить к минимуму последствия негативных происшествий.

Звуковой фон несет в себе информацию, которую порой невозможно выделить при обычном «глухом» режиме видеонаблюдения. Когда в базу аналитической программы уже заложены типичные для определенной территории звуки, включение ее в работу позволяет вычленить из общего шума признаки подозрительной активности.

Другой вариант применения аудиоаналитики – установка микрофонов в «слепых» зонах, не просматривающихся видеокамерами. Когда фиксируемый звуковой поток превышает задаваемый в программе порог громкости, микропроцессор видеокамеры может активировать выполнение пакета действий по запрограммированному алгоритму:

- включить видеозапись, световую сигнализацию, индикацию надписи «Не шуметь!»;
- выполнить рассылку сообщений заданным адресатам;

- подать активирующий сигнал на различные устройства и оборудование.

И это далеко не полный перечень возможных системных решений, подчеркивают эксперты Гольфстрима.

Современные технологии обработки аудио-визуальной информации позволяют выявлять скрытые закономерности и тенденции, которые указывают на потенциальные угрозы. На сайте юридической компании d-pravo (https://d-pravo.ru) данный процесс именуется «звуковой разведкой», работа которой включает в себя следующие этапы:

1. Сбор звуковых данных может быть осуществлен с помощью специальных микрофонов, установленных на приборах или непосредственно на объекте охраны.

2. Фильтрация сигналов необходима для отделения ложных, шумовых сигналов от полезных.

3. Анализ спектра звука с целью определения характеристик и параметров звуковых сигналов. Может включать определение частот сигнала, его амплитуды, длительности и других характеристик.

4. Идентификация и классификация позволяют определить принадлежность сигналов к конкретным реальным источникам или событиям.

И по мере того, как аудиоустройства становятся все более интегрируемыми, они со временем становятся и более мощными. Аудиопродукты, которые в прошлом приходилось использовать по отдельности, теперь все чаще работают согласованно, пишет Лаура Степанек на сайте **https://www.sdmmag.com.** Это значительно расширяет возможности аудио, особенно в приложениях для удаленного мониторинга в реальном времени.

«Аудио добавляет ещё один уровень безопасности, обеспечивая ситуационную осведомленность, которую не может дать одно только видео», — говорит Тодд Келлер, президент американской компании Speco Technologies. «Независимо от того, используются ли аудиотехнологии для отпугивания злоумышленников или для подтверждения инцидентов с помощью звуковых оповещений, наличие звукового и визуального наблюдения позволяет получить полную картину. Такой подход усиливает меры безопасности и сокращает время реагирования» (там же).

По словам Криса Уайлдферстера, менеджера по работе с клиентами Axis Communications (штат Массачусетс, США), аудиотехнологии улучшают динамику работы системы безопасности. «Допустим, кто-то собирается перепрыгнуть через забор. На заборе установлена камера, и в нее загружена аналитика. Когда человек пересекает эту периметр, воспроизводится голосовое сообщение: «Вы вошли на охраняемую территорию; пожалуйста, покиньте ее тем же путем, которым пришли. Власти уведомлены». Аудиокомпонент подтверждает, что видеокамера действительно работает и злоумышленник находится под наблюдением. По словам Келлера, исследования показывают, что аудиопредупреждения реально снижают уровень преступности.

Аудиодинамики устанавливаются в разных местах на охраняемой территории, чаще всего по периметру безопасности. Сообщения могут зачитываться оператором в режиме реального времени или воспроизводиться в виде предварительно записанных сообщений. По словам экспертов, возможность транслировать заранее записанные сообщения, особенно на несколько динамиков, помогает сократить время обучения операторов и время, необходимое для объявления, а также устранить любые несоответствия в сообщениях.

Еще одно важное направление развития аудиотехнологий – акустическое нелетальное оружие для охраны объектов (как гражданских, так и военных). Это системы, воздействующие на цель направленными звуковыми сигналами.

Тема нелетального акустического оружия регулярно поднимается в различных публикациях российских СМИ. Так, в январском номере журнала «Военная мысль» за 2022 год была опубликована статья «Применение оружия нелетального действия в интересах охраны объектов от несанкционированного проникновения». В ней рассматриваются различные способы воздействия на живую силу в контексте защиты периметра, в том числе и акустический.

Авторы статьи считают, что акустическое оружие является одним из самых эффективных средств нелетального действия в контексте охраны объектов. Наилучшие рабочие и «боевые» характеристики демонстрируют акустические системы, использующие верхнюю часть слышимого диапазона – от 16 до 20 кГц. Громкий звук на таких частотах чрезмерно воздействует на барабанную перепонку, что приводит к смещению элементов среднего уха и возникновению болевых ощущений. Сильные болевые ощущения возникают у здорового человека при шуме интенсивностью 130-140 дБ. Эксперименты показывают, что звук до 130 дБ при длительности до 10 секунд не приводит к необратимым повреждениям органов слуха и в целом безопасен.

Образцы акустического оружия, пригодные для практического применения, создаются в ряде стран, включая Россию. В нашей стране в 2017 г. была представлена «звуковая пушка» под названием «Сирин». Сообщалось, что сигналы изделия «Сирин» в режиме громкоговорителя слышны на расстоянии до 5 км. Акустическое нелетальное подавление обеспечивается в радиусе 560 м; звуковое давление – до 152 дБ.

В дальнейшем были разработаны новые образцы с разными характеристиками, и теперь речь идет о целом семействе «Сирин». Подробнее см. https://topwar.ru/192191-akusticheskoe-neletalnoe-oruzhie-dlja-ohrany-obektov-i-dlja-drugih-zadach.html?ysclid=mclqizeb3w311346078.

Можно ли надежно защитить электронную почту от фишинга?

Ежедневно в мире отправляют и получают 300+ млрд электронных писем (https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/).

По прогнозам, число электронных писем превысит в 2027 году отметку в 400 млрд. Из-за популярности мессенджеров наблюдается снижение личных писем, но общий рост обеспечивает корпоративный сегмент.

Деловая почта для многих организаций и их сотрудников — самый популярный инструмент коммуникаций. Она позволяет быстро обмениваться информацией, документами и файлами с коллегами, руководством и клиентами. Однако 68% атак на компании начинаются именно с электронных писем. Хакеры взламывают электронную почту с целью хищения конфиденциальных данных и организации атак на финансовые и бухгалтерские подразделения компании.

Можно ли надежно защитить электронную почту от фишинга?

Нельзя, утверждает Кит Лоусон, специалист с 25-летним опытом в области кибербезопасности, в статье на сайте интернет издания Chief Security Officer (https://www.csoonline.com). Большинство взломов сетей происходит из-за фишинга. Компании используют несколько уровней зашиты от спама и фишинга, но ни одно из них не является идеальным, и злоумышленники, совершенствуя свой боевой арсенал, раз за разом пролезают со своими вредоносными письмами в почтовые ящики работников компаний. Не помогают и кампании по повышению осведомленности о

киберугрозах. Статистика свидетельствует: значительное число участников тренингов по-прежнему покупается на вредоносные ссылки.

Борьба с фишинговыми письмами — заведомо проигрышная битва, пишет Кит Лоусон. «Для обхода всех ваших средств защиты достаточно одного клика. Мы должны кардинально переосмыслить и изменить способы электронного общения».

Сквозное шифрование, к чему призывают многие эксперты, малоэффективно. Для обеспечения безопасности данных можно использовать строгие настройки сервера и сторонние инструменты, но зачастую их легко обойти: например, добавить в список рассылки всего одного небезопасного получателя и конфиденциальность будет нарушена. Принудительное шифрование приводит к ухудшению качества почты и вынуждает сотрудников искать обходные пути. Не существует надежной конфигурации, которая гарантировала бы шифрование данных, из-за растущей популярности SMTP-серверов, работающих в незашифрованном виде (SMTP — коммуникационный протокол, который позволяет отправлять и получать электронные письма в больших количествах). Протокол SMTP появился в эпоху, когда еще не было масштабной киберпреступности и массовой глобальной слежки за онлайн-коммуникациями, и шифрование в него не встроено.

Компания Google недавно объявила о внедрении «сквозного шифрования электронной почты» в Gmail с помощью расширений безопасной многоцелевой интернет-почты (S/MIME) (https://workspace.google.com/blog/identity-and-security/gmail-easy-end-to-end-encryption-all-businesses). Однако в своих комментариях Google признает определенные сложности и недостатки этого решения, которое сталкивается с теми же проблемами, что и SMTP, поскольку S/MIME сложно настроить и гарантировать его работу при отправке на удаленные системы.

Еще одна проигранная битва – электронная почта в качестве механизма аутентификации. Широкое распространение отправки уникальных ссылок на адреса электронной почты открывает возможности для атак на критически важные сервисы через личные аккаунты. Как только злоумышленник получает доступ к личной электронной почте, ему не составляет труда выйти на системы, которые используют эту почту для аутентификации или сброса пароля, отправить запрос на сброс пароля через сторонний сервис и получить доступ к этому сервису. Если этот сервис является корпоративной системой, значит, злоумышленники получили доступ к вашему бизнесу через личную электронную почту сотрудника. Это может быть первым шагом к масштабному нарушению корпоративной безопасности.

Продолжать использовать электронную почту для критически важных бизнес-функций, таких как крупные финансовые операции или обмен конфиденциальной информацией, значит играть в заведомо проигрышную игру, заключает Лоусон. Компаниям следует внедрять политику, которая поощряет использование более безопасных альтернатив.

Помимо электронной почты преступники давно освоили и другие каналы фишинга: мессенджеры, социальные сети, рекламу и SMS-сообщения, которые часто комбинируют для проведения атаки, пишет автор (или авторы) статьи «Мы боремся с фишингом неправильно» на сайте https://www.securitylab.ru (1 июня 2025 г.).

К примеру, в Telegram приходит «безопасный» PDF-документ. Внутри документа содержится ссылка на Google Drive. Google Drive перенаправляет на скомпрометированный веб-сайт. Сайт загружает поддельную страницу входа в систему. Ни одна система фильтрации не способна отследить всю эту цепочку целиком.

Если фишинг нельзя полностью победить, то это не означает, что против него невозможно успешно бороться. Эксперты российской корпорации Positive Technologies формулируют пять основных шагов для минимизации рисков:

1. *Сместите фокус на браузер.* Именно там, где пользователь вводит свои учетные данные, и происходит атака. Мониторинг с помощью расширения для браузера позволяет видеть реальную страницу, а не ее копию в системе проверки.
2. *Переходите от отслеживания индикаторов к анализу тактик.* Фиксируйте характерные признаки атак: наличие формы входа + несоответствие домена + попытка повторного использования пароля. Такие характеристики злоумышленникам изменить сложнее, чем адрес сайта.
3. *Внедряйте проверку в реальном времени.* Система должна блокировать ввод учетных данных немедленно, а не через час после обновления базы угроз.
4. *Анализируйте сессии, а не только ссылки.* Современные атаки часто направлены на перехват сессионных токенов (уникальных идентификаторов, создаваемых сервером при входе пользователя в приложение или на сайт), а не паролей. Отслеживайте подозрительный экспорт файлов cookie или автоматическую авторизацию через API (программный интерфейс приложений).
5. *Автоматизируйте обратную связь.* Любая блокировка должна сразу отправлять уведомление в центр операционной безопасности (SOC), чтобы аналитики не тратили время на ручную проверку. Подробнее https://www.securitylab.ru/analytics/559764.php

Как минимизировать ущерб от программы-вымогателя сразу после атаки?

Чтобы свести к минимуму потери от атаки хакеров-шантажистов, эксперты рекомендуют следующие шаги, которые необходимо предпринять в первые 72 часа.

Изолируйте зараженное устройство

Чтобы обеспечить безопасность сети, важно как можно быстрее отключить пострадавшее устройство от сети, Интернета и других устройств, советуют эксперты российской компании Mainton (программное обеспечение. IT-консалтинг). Чем раньше вы это сделаете, тем меньше вероятность заражения других устройств.

Остановите распространение и обезопасьте свом коммуникации

Будет разумно немедленно создать новые защищенные адреса электронной почты и не входить в учетные записи, которые могут быть также скомпрометированы, рекомендуют специалисты консалтинговой юридической компании Lawrence Stephens. Возможно, потребуется уведомить свой банк и/или поставщиков услуг о новом адресе. Крайне важно, чтобы пароли были немедленно изменены и усилены по всей организации. Необходимо отключить от сети все устройства, которые ведут себя подозрительно, в том числе те, которые работают за пределами предприятия — если они подключены к сети, они представляют опасность, где бы они ни находились. Отключение беспроводной связи (Wi-Fi, Bluetooth и т. д.) на этом этапе тоже хорошая идея.

Сохраните доказательства

Сохранение улик – в числе первоочередных задач. При отсутствии собственных специалистов по цифровой криминалистике, пригласите внешних экспертов. Консультанты Lawrence Stephens рекомендуют на начальном этапе не сбрасывать настройки до заводских. На основе сохраненных данных криминалистическая экспертиза получит информацию, необходимую для отслеживания и

возврата украденных активов. Возможно, что потребуется приобрести новые устройства, чтобы сохранить пострадавшие устройства в качестве улик.

Сообщите в правоохранительные органы и регулятору

Даже если полиция не может оказать немедленную практическую помощь, заявление в нее будет служить официальным документом для последующих юридических действий и мер по восстановлению, а также поможет расследователям выявить закономерности в действиях преступных группировок. Нельзя забывать о последствиях, связанных с соблюдением требований законодательства. Если вы не уведомите о взломе данных, ваш бизнес может быть оштрафован.

Оцените ущерб

Это совет от компании Mainton. Ваша цель — создать полный список всех затронутых систем, включая сетевые устройства хранения данных, облачные хранилища, внешние жесткие диски (включая флэш-накопители USB), ноутбуки, смартфоны и любые другие возможные устройства.

Выкуп: платить или не платить?

Это ключевой вопрос. Подавляющее большинство экспертов советуют не платить. В их числе и Евгений Касперский. Он называет три причины в пользу такого подхода. Во-первых, вы спонсируете разработку зловредов. Во-вторых, заблокированные данные могут и не вернуть. В-третьих, шантажировать вас могут повторно и неоднократно (https://www.kaspersky.ru/blog/to-pay-or-not-to-pay/30191/?ysclid=mcuazrixj791292248).

Хотя достоверной статистики нет (многие компании скрывают факты атаки), примерно четверть атакованных организаций предпочитают сторговаться и заплатить шифровальщикам. В процессе переговоров важно держать хакеров в неведении относительно принимаемых вами мер. Ведите подробный документальный учет всех контактов, включая запросы на оплату, электронные письма, телефонные звонки, текстовые сообщения, общение в социальных сетях. Если выкуп выплачивается в криптовалюте, запишите данные о транзакции, адреса кошельков, хэши (идентификаторы) транзакций. Если в ходе общения вас отправили на веб-страницу, обязательно сделайте скриншоты этих страниц на случай, если они исчезнут.

Точная документация имеет решающее значение для возможных последующих разбирательств и расследований со стороны регуляторов, полиции, судебных органов.

Тщательное предварительное планирование, быстрые и последовательные действия в первые 72 часа после атаки могут значительно ограничить, а при удаче и избежать ущерба.

(по материалам интернет ресурсов https://www.lawrencestephens.com, https://www.ebsco.com, https://www.bailry.com/ru, https://www.kaspersky.ru, https://www.cnews.ru)

Оружие для телохранителя

В современной системе личной охраны огнестрельное оружие рассматривается не как повседневное средство, а как необходимое только в ситуации «прямой, непосредственной и

неизбежной угрозы», пишет директор по стратегическому развитию в охранном предприятии Cooke & Associates Гаррет Людке в издании Security Management, June 2025.

Решение о вооружении группы быстрого реагирования никогда не принимается легкомысленно. Оно начинается с оценки угрозы:

- Профиль рисков
- Условия работы (городские или сельские, международные или внутренние)
- Общественное восприятие и соображения, касающиеся бренда
- Юридическая ответственность и пороговые значения применения силы

В штате Калифорния, США, известном строгими правилами обращения с огнестрельным оружием, вооруженные телохранители должны иметь соответствующую лицензию, выдаваемую Бюро безопасности и следственных служб (BSIS) после прохождения 40-часового курса и 14-часовой сертифицированной BSIS подготовки по обращению с огнестрельным оружием.

Курс обучения охранника предусматривает следующие дисциплины: право и ограничения на арест, необходимые условия для применения силы, связи с общественностью, составление отчетов, коммуникативные навыки. В качестве факультатива добавляются занятия о терроризме.

Обучение должно включать:

- Обращение с огнестрельным оружием и навыки стрельбы в стрессовых ситуациях
- Распознавание угроз и индикаторы возможной атаки
- Передвижение, укрытие и тактическое расположение
- Методы деэскалации ситуации
- Протоколы применения силы в зависимости от юрисдикции
- Методы преодоления физического и психологического стресса
- Медицина и оказание первой помощи

Телохранители с оружием помимо обучения должны заполнить анкету, пройти дактилоскопическую идентификацию в режиме реального времени, психологическое тестирование и предоставить подтверждение гражданства США или легального статуса в Соединённых Штатах.

Для ношения скрытого оружия требуется отдельное разрешение, выдаваемое местными властями, в зависимости от должности и юрисдикции.

На территории Российской Федерации действует целый ряд законодательных актов, указов, постановлений и других официальных документов, регулирующих деятельность охранных служб в отношении оружия.

Для официального приобретения, хранения, ношения и применения служебного оружия в работе сотрудников частного охранного предприятия необходима лицензия на оружие ЧОП. Этот документ выдается по месту регистрации охранной службы отделом лицензионно-разрешительной работы МВД. Срок действия лицензии на оружие составляет 6 месяцев, после чего возможно продление. Для получения лицензии на оружие необходимо подготовить пакет документов, состоящий из более десятка позиций (подробнее см. https://www.legis-s.ru/company/articles/razreshenie-na-oruzhie-dlya-chop).

В России только охранники 5 и 6 разрядов могут приобрести оружие. Срок обучения на максимальный 6-й разряд составляет 266 часов.

Охранник 6-го разряда может пойти учиться дальше непосредственно на телохранителя в частном охранном предприятии или другом специализированном учреждении. Для этого кандидат проходит психологическую подготовку и тестирование, сдает экзамен по обращению с оружием в рамках прицельной стрельбы по неподвижной мишени и прицельной стрельбы по движущейся цели. Учитывая особенности профессии, дополнительно проверяются знания иностранного языка, опыт в экстремальном вождении транспортного средства.

В числе обязательных требований – коммуникативные навыки. Для охраны клиента допускается применять огнестрельное оружие только в крайнем случае, когда конфликт нельзя предотвратить путем переговоров. Телохранитель должен уметь убеждать, быть дипломатом и готовым к регулярному общению с окружением клиента (https://dzen.ru/a/Xfeb4b1jlgC0ej4v?ysclid=mcsrv42lnn473806090).

Эффективные программы защиты руководителей, отмечает Гаррет Людке, опираются на детальное планирование перед операцией и юридическую координацию. Команды должны оценивать законодательство конкретной юрисдикции, выявлять ограничения и определять наиболее эффективный и законный план действий. Это часто включает в себя работу с юрисконсультом для получения разрешений на транспортировку, координацию с местными властями или привлечение проверенных местных сотрудников, если закон запрещает перевозку оружия (https://www.asisonline.org/security-management-magazine).

Рецензия

«Personal Threat Management: The Practitioner’s Guide»

By Philip Grindell

Книга Филипа Гриндэлла «Управление персональными угрозами: практическое руководство» предлагает комплексный подход к вопросам обеспечения личной безопасности и защиты.

Заявленная цель автора — «рассеять туман вокруг этой темы, прояснить некоторые термины и объяснить, как и почему кто-то может представлять для вас угрозу». Он делится своими знаниями — результатом многолетнего опыта работы в этой сфере в сочетании с изучением современных исследований в области оценки угроз и стандартов профессионализма.

В книге два основных раздела: «Понимание угроз» и «Управление угрозами».

Ключевой раздел посвящен управлению поведенческими угрозами. В нем подчеркивается, что «действия говорят лучше слов». Гринделл представляет концепцию «выявляй, сообщай, действуй». Автор рассказывает о том, как отличить реальные угрозы от тех, которыми можно пренебречь.

Книга охватывает критически важные области рисков, содержит практические советы по планированию мер безопасности, а также обсуждение различных сценариев, от террористических угроз до внутренних атак и действий одиночек.

Способность Гринделла разъяснять непонятные термины и давать практические советы делает эту книгу ценной для специалистов по безопасности, стремящихся улучшить свое понимание управления персональными угрозами.