Охрана предприятия

3 (96) 2025

Оглавление

Дипфейки становятся рутиной

Старший бухгалтер финансового подразделения в гонконгском офисе британской транснациональной корпорации Arup (услуги в области дизайна, инжиниринга, архитектуры, 90 офисов в 35 странах) получил по электронной почте письмо от лондонского начальства с требованием секретной немедленной транзакции 25 млн долларов США. Письмо показалось ему подозрительным, фишинговым. Однако бухгалтер отбросил все сомнения, когда с ним связались по видеоканалу. На экране высветились лица его начальника и других коллег из штаб-квартиры в Лондоне. Деньги были отправлены по указанным счетам. Это произошло год назад, весной 2024 года.

Корпорация признала факт обмана. «Как и многие другие бизнесы во всем мире, мы подвергаемся регулярным атакам с использованием голосовых и визуальных дипфейков. Можем уверенно констатировать резкий рост числа и изощренности таких атак», - заявил Роб Грейг, главный информационный менеджер компании (https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html).

Дипфейки (другое название – синтетические медиа) согласно экспертам CISA (Агентство по кибербезопасности и защите инфраструктуры) представляют собой угрозы в трех направлениях: имперсонация руководящего лица для хищения денег, манипуляция брендом, овладение доступом в корпоративные базы данных.

Дипфейки становятся рутиной. Об этом говорят результаты опроса **Medus survey**: большинство (53%) респондентов - финансовых работников - подвергались в 2024 году атакам с применением дипфейковых схем. При этом более 43% атакованных стали жертвами злоумышленников.

Конечно, цифры таких опросов нельзя считать полностью корректными, если принять во внимание нежелание огромного числа компаний публично признавать, что «лопухнулись».

Люди в подавляющем большинстве уверены, что обмануть их с помощью приемов дипфейка невозможно. Исследования, проводимые в разных странах, выявляют колоссальный разрыв между подобным самомнением и реальностью. Что же заставляет людей, профессионально образованных, в том числе обученных способам распознания мошеннических схем, отбрасывать прочь сомнения, подозрения и верить, что картинка на экране их компьютера или смартфона идентична реальности, спрашивает журналистка Дженифер Грегори в блоге на сайте securityintelligence.com. Завораживающие цифры миллионных транзакций? Или нечто другое?

Академический журнал Sage попытался в этом разобраться и пришел к выводу, что жертвы дипфейка ничем не отличаются от других людей, ни возрастом, ни полом. Можно предполагать, что старшие поколения более уязвимы для изощренных схем обмана. В то же время проводимые в компаниях учебные занятия с персоналом по программе ознакомления с угрозами и рисками, хотя и являются важным фактором корпоративной безопасности, пишет журнал, их эффективность с точки зрения защиты от синтетических медиа весьма ограничена.

Нейрофизиолог Тижл Грутсводжер из Western Sydney University, занимающийся исследованиями мозга, похоже, попал в точку, провозгласив, что выявление дипфейков требует от нас абсолютно новых умений и компетенций, с которыми ранее мы не сталкивались. В интервью журналу Science Magazine он говорит: «Нам никогда в своей жизни не приходилось думать над тем, кто перед нами – реальный или подменный, имитированный человек. Наш мозг просто не тренирован на такое распознание».

Ученый также обнаружил, что человеческий мозг лучше справляется с задачей идентификации без сознательного вмешательства в этот процесс.

Когда люди получают по видео картинку, сформированную с помощью дипфейка, то в зрительный сегмент коры головного мозга приходит электрический сигнал, ***отличный*** от сигнала, которую генерирует реальная, идентичная картина на экране. Почему? На этот вопрос эксперт затрудняется ответить. Возможно по причине, что сигналы не затрагивают наше сознание из-за вмешательства в этот процесс других зон коры головного мозга. А может быть, из-за того, что человеческий мозг просто еще не научился, не натренировался безошибочно отличать изощренную имитацию от действительности.

Во всяком случае, очевидно, что пришло время тренировать наши мозги, настраивая их на безусловное предположение, что любое изображение, любая видео картина, наблюдаемая нами, может быть продуктом синтетических медиа. «Задавая себе такой вопрос постоянно и везде, сталкиваясь с тем или иным контентом, мы постепенно обретем способность распознавать поступающие в мозг сигналы как производные от синтетических медиа», - пишет Дженифер Грегори. И добавляет, что не менее важно немедленно сообщать «во все инстанции» о каждой атаке с использованием дипфейка.

Искусственный интеллект - смертельная угроза для банков и других финансовых организаций

Британская исследовательская группа «Say No To Disinfo» провела смелый эксперимент, подвергнув 500 клиентов одного из банков дезинформационной атаке с применением искусственного интеллекта. Синтетические сообщения, распространенные через социальную сеть X (в прошлом Твиттер), запугивали пользователей, что их сбережения «под угрозой».

Результаты последующего опроса участников эксперимента получились такими:

- 61% участников выразили желание забрать свои деньги из банка.

- Более 33% респондентов готовы были сделать это «очень вероятно», 27% - «возможно».

В переводе на язык финансов эксперимент показал, что мизерного вложения ($13)в генерацию ИИ контента достаточно, чтобы привести в движение миллион долларов США.

Исследование продемонстрировало высокую уязвимость финансовых институтов перед лицом изощренных атак злоумышленников с применением новейших цифровых технологий (подробнее об эксперименте см.
https://www.saynotodisinfo.com/_files/ugd/438ee6_d9f4506bfd2e43218b96f716bae91ce1.pdf

Другой опрос, проведенный образовательно-исследовательской организацией в области финансов Financial Education and Research Foundation's (FERF), выявил, что более трети финансовых директоров компаний (CFO) проявляют серьезную озабоченность в связи тем, что внедрение искусственного интеллекта может обернуться слишком высокими для бизнеса рисками, которые не оправдывают инвестиции в эти технологии. То есть когда реальные риски перекрывают ожидаемые экономические результаты.

Эксперты обращают внимание, что неясности и сомнения вокруг искусственного интеллекта вынуждают финансовых директоров помимо своих прямых обязанностей отвлекаться на ранее несвойственные им задачи, такие как мониторинг и анализ рисков и угроз, проверка качества и надежности данных (data quality assurance), формирование в команде «культуры безопасности», возвращение работающих на «удалёнке» сотрудников назад в офис (return to office initiatives).

Поэтому не удивляет распространенный среди финансовых профессионалов скептицизм относительно ИИ. Примерно 4 из 10 финансовых директоров (38%) – участников исследования «2025 Financial Executives Priorities Report» - выразили сомнение в отношении инвестиций в технологии искусственного интеллекта. Показательно, что только 4% опрошенных в ходе упомянутого исследования считают низкими риски от внедрения ИИ.

В то время как рынок ИИ остается в высокой степени непредсказуемым, многие финансовые руководители не находят удовлетворительного ответа на вопросы, какова реальная цена внедрения этих технологий, как выстраивать систему кибербезопасности и стратегию обучения персонала. Так, к примеру, треть респондентов при найме сотрудников в финансовую службу отдают предпочтение компетенциям, связанным с управлением данными и ознакомлением с новыми технологиями, перед знаниями и навыками в области финансового планирования и анализа, бухгалтерского учета.

Подавляющее большинство (78%) высказывают озабоченность киберрисками, которые возрастают многократно ввиду распространения дипфейков и других изобретательных приемов обмана на базе ИИ. При этом:

- в некоторой степени озабочены 50%;

- совсем не озабочены 3%;

- слегка озабочены 19%;

- очень озабочены 28%.

Подробнее результаты исследования см. https://www.cfo.com/news/38-of-cfos-remain-undecided-about-ais-cost-versus-risk-ferf-2025-financial-executives-priorities/738593/

Подводя итоги, авторы исследования отмечают, что в условиях все более активного использования искусственного интеллекта для вымогательских программ и иных мошеннических схем финансовым службам, их руководителям, чтобы обеспечить нормальное функционирование, необходимо особо пристальное внимание уделять в 2025 году вопросам защиты своей самой ценной интеллектуальной собственности – финансовой и персональной информации.

Как радикально улучшить выявление финансовых преступлений с помощью видеоаналитики

Ежегодно мошенничество стоит финансовым организациям сотни миллиардов долларов. Потери растут год от года по мере совершенствования криминалом своей тактики и технологического инструментария.

Банки и другие финансовые организации тоже не стоят на месте. Они берут на вооружение интегрированные технологии видеонаблюдения и аналитики – проверенное средство не только обнаружения, но и предотвращения хищений и прочих видов преступности.

Джеф Корралл, ведущий специалист компании March Networks (системы охраны и безопасности) рассказал в интервью журналу Security Management, February 2025, как видеоаналитика революционизирует программы банков по обнаружению и предупреждению мошенничества. Он выделяет следующие направления использования инновационных технологий:

1. Сигналы угрозы в реальном времени

Системы мониторинга рисков и угроз генерируют обширные массивы данных, но не каждый сигнал указывает на реальный риск. Видеоаналитика является одним из самых надежных средств отличать реальные угрозы от ложных. К примеру, когда транзакция характеризуется необычно большим объемом снятия наличных, система видеонаблюдения способна быстро зафиксировать и идентифицировать человека, снимающего кэш, его банковские счета.

2. Система распознавания автомобильных госзнаков

Автоматические кассовые устройства, позволяющие снимать деньги со счёта, не выходя из автомобиля, часто становятся объектами нападения, особенно в пригородах и сельской местности. Технология распознавания автомобильных госзнаков в системе продвинутого видеонаблюдения существенно минимизирует риски. Для банков она служит источником ценной информации о рецидивистах, специализирующихся на данном виде преступлений. К примеру, система посылает охране сигнал тревоги при приближении к банкомату автомобиля, чей владелец в «черном списке».

3. Поведенческая аналитика

Скимминг (установка на банкоматах скрытых устройств, позволяющих считывать информацию с платёжных карт в процессе транзакции) остается одной из серьезных угроз для банков. Технология поведенческого анализа в системе видеонаблюдения позволяет вовремя обнаружить необычные, аномальные действия человека вблизи банкомата, когда, к примеру, он/она слоняется рядом, но ничего не предпринимает, или использует несколько карт, быстро меняя одну за другой.

4. Интегрированное видеонаблюдение

Взлом банкомата – постоянно растущая угроза для банков. Комбинация видеонаблюдения с физическими сенсорами зарекомендовала себя как надежное средство защиты. Камеры наблюдения и сенсоры движения фиксируют аномальную активность (например, автомобиль, подозрительно близко припаркованный к терминалу, или машину без госзнака, или необычное поведение человека, подошедшего к банкомату) и сразу же сигнализируют охране.

5. Детекторы праздношатания (Loitering Detection)

Такие устройства особенно нужны во внерабочее время суток. Видеонаблюдение + аналитика помогают идентификации подозрительных личностей, слоняющихся вблизи банкомата длительное время.

6. Гибридные видеонакопители **(**Video Storage with Hybrid Solutions)

Гибридные решения сочетают ресурсы локальной инфраструктуры и облачного хранилища. Их преимущество в гибкости - банки могут хранить одни данные на локальной базе, другие в облаках. Это экономично, удобно, легко масштабируемо.

7. Решения Camera-to-Cloud

Технология Camera-to-Cloud предусматривает загрузку видеоданных непосредственно в облачные хранилища в реальном времени. Она особенно полезна для дистанционного мониторинга, поскольку устраняет необходимость ручной передачи данных в облака.

Криптовалютный криминал и способы борьбы с ним

Появление криптовалюты открыло новые широкие возможности для финансовых инноваций и инвестиций, но одновременно сопровождается быстрой экспансией отмывателей «грязных денег» в образовавшиеся лагуны цифровой среды. Почти 41 млрд в криптовалютах получили преступники в 2024 году, согласно отчету аналитической компании Chainalysis. Переводы на криптокошельки, связанные с преступной деятельностью, составили 0,14% от всех блокчейн-транзакций.

Меры противодействия затрудняются децентрализованной и наднациональной природой криптовалюты. В отличие от традиционных денег последняя не контролируется, либо слабо

контролируется регуляторами и государством. Транзакции осуществляются фактически в обход полномочий правительственных и финансовых институтов, которым нелегко по одним только криптографическим адресам связать транзакции с реальными игроками.

Преступники же постоянно совершенствуют методы отмывания полученных нелегальными способами денег. Большое распространение получили так называемые «тумблеры» - смесители криптовалюты, позволяющие повысить конфиденциальность транзакций путем их раздробления на более мелкие переводы, или объединением несколько транзакций, направлением их на случайно выбранные адреса, чтобы запутать и осложнить попытки идентификации пользователей. Услугами смесителей пользуются не только отмыватели. К «тумблерам» активно прибегают и наркоторговцы, и киберпреступники.

Другой популярный у криминала способ – использование одноранговых сетей (peer-to-peer networks) и внебиржевых брокеров (over-the-counter brokers). Эти площадки помогают злоумышленникам оперировать криптовалютой, скрывая свою идентичность, не оставляя заметных следов.

Нельзя не упомянуть в этой связи и систему децентрализованных финансов (DeFi) —экосистему финансовых приложений, построенных на базе сетей блокчейна. Цель DeFi — создать общедоступную и прозрачную экосистему финансовых услуг с открытым исходным кодом, работающую без какого-либо центрального органа. DeFi-системы делают финансовые продукты доступными в децентрализованных сетях типа блокчейн, позволяя пользоваться продуктами и совершать трансакции, минуя таких посредников, как банки, брокерские компании, кредиторы и т. д. Но, как отмечают эксперты, эта цель не достигнута в виду отсутствия надлежащего контроля и регулирования. Более того, децентрализованные финансы стали популярным объектом для хакерских атак. Эксплуатируя анонимность и децентрализованность DeFi платформ, преступники отправляют грязные деньги через сложную сеть транзакций, стараясь скрыть следы.

Эксперты образовательной и консалтинговой организации Financial Crime Academy (**https://financialcrimeacademy.org**) работают над методологией борьбы с криптовалютной преступностью. Важнейшим компонентом антиотмывочной стратегии они называют организацию системы мониторинга транзакций и идентификации красных флажков. Скрупулёзно анализируя транзакции на предмет выявления признаков подозрительной активности, можно выйти на схемы отмывания нелегальных денег и принять предупредительные меры. Последние могут включать информирование о подозрительных транзакциях соответствующих инстанций, замораживание средств, шаги по разрушению и ликвидации преступных схем.

Для достижения практических результатов необходимо выполнение, как минимум, следующих условий:

Инвестировать в продвинутые инструменты и технологии, обеспечивающие результативный анализ данных о транзакциях подозрительной активности

- Разработать четкие и понятные процедуры своевременного информирования о подозрительных транзакциях

- Установить тесное взаимодействие с другими компаниями в криптоиндустрии, а также с правоохранительными структурами для обмена важной информацией

В качестве инструментов предлагается максимально использовать такие методы и технологии как:

- Блокчейн анализ — совокупность методов получения и обработки данных из записей в распределённом реестре (блокчейне)

- Алгоритмы машинного обучения
- Аналитика данных (data analytics)
- Искусственный интеллект

Все эксперты указывают на важное значение учебы и тренингов для работников криптокомпаний. Занятия должны проводиться регулярно и охватывать широкий спектр проблем, включая нормативно-правовое регулирование, методы криминала по отмыванию криптовалюты, характерные риски, присущие криптоиндустрии.

Немалая роль в объединении усилий на международном уровне отводится организации ФАТФ, которая представила в 2024 году обновленную методологию взаимных оценок, сфокусированную на повышение эффективности мер борьбы с отмыванием нелегальных средств и финансированием терроризма. В документе, в частности, говорится, что криптовалютные компании могут осуществлять деятельность только при наличии лицензии или регистрации. Для юрлиц — в юрисдикции, где они созданы, для физлиц — в юрисдикции, где осуществляется их деятельность. Нарушители закона и их сообщники не допускаются к владению или управлению VASP (Virtual Asset Service Provider - поставщик услуг виртуальных активов). Также предусмотрены: беспрепятственный обмен сведений о бенефициарной собственности криптокомпаний с компетентными органами, предоставление финансовых данных для расследования случаев отмывания денег и финансирования терроризма. Разработка руководящих принципов для VASP закрепляется за локальными надзорными органами.

Отмывание криптовалют представляет собой серьезную угрозу для мира финансов. Бороться с ней эффективно возможно при условии тесного взаимодействия криптокомпаний, правоохранительных органов и регуляторов.

Андрей Меркулов

Проблемы использования Open Source решений для обеспечения ИБ в 2025 году

Решения Open Source (с открытым исходным кодом) сегодня применяются во многих сферах – эта тенденция усилилась многократно после ухода с рынка западных игроков. На базе этих инструментов создаются, в том числе, продукты для бизнеса и массового сектора (например, операционные системы Astra Linux). Проведенное Ассоциацией ФинТех исследование «Технологическая независимость российского финтех-рынка» показало, что 82% опрошенных российских компаний-разработчиков считают такой подход оптимальным с точки зрения сроков, функциональности и рисков.

Применение Open Source: pro et contra

Применение Open Source имеет множество преимуществ помимо отсутствия необходимости крупных финансовых затрат. Основные из них:

- гибкость и кастомизация – такие инструменты могут адаптироваться под любые задачи и функционировать в абсолютно разных условиях;

- доступность – после ухода иностранных компаний доступ ко многим продуктам ограничен, а решения с открытым исходным кодом всё еще свободно распространяются;
- прозрачность исходного продукта – специалисты могут проводить анализ используемых решений на предмет отсутствия в них скрытых уязвимостей или нежелательных функций;
- поддержка сообщества – ввиду популярности Open Source разработок, в интернете есть библиотеки знаний по внедрению и настройке, а также по решению часто встречаемых проблем.

Такой инструментарий дает свободу при решении задач, связанных с обеспечением информационной безопасности. Однако, имеет он и свои недостатки, ограничения. Перечислим их здесь:

- отсутствие поддержки – если организация решила применять Open Source решения, ей нужно быть готовой самостоятельно сопровождать системы защиты информации;
- необходимость квалифицированных специалистов – внедрение и сопровождение таких разработок предъявляют более высокие требования к знаниям и умениям сотрудников, ответственных за обеспечение ИБ;
- ограниченная документация – чтобы корректно использовать их, приходится вкладывать дополнительные ресурсы на сопровождение;
- сырые продукты – поскольку разработчики Open Source инструментов не обязаны на постоянной основе поддерживать их, никто не гарантирует отсутствие критических проблем;
- сложности интеграции – далеко не все продукты совместимы с разработками, представленными на рынке;
- несоответствие нормативным требованиям – имеются сферы, в которых применение Open Source решений не допускается регуляторами.

Вот наиболее популярные классы решений, для которых имеются аналоги с открытым исходным кодом:

- SIEM (Security Information and Event Management) — решение для централизованного сбора, анализа и оценки корреляции событий информационной безопасности (Wazuh, OSSEC -

прародитель Wazuh, обладающая меньшими требованиями к мощности вычислительной сети организации).

- IDS/IPS (Intrusion Detection System) — системы обнаружения и предотвращения вторжений (Snort, Suricata)

- WAF (Web Application Firewall) - инструмент для защиты веб-сайтов и веб-приложений (ModSecurity)

- Защита от DDoS (Honeypot)

- Сканирование уязвимостей (OpenVAS)

- Резервное копирование (Bacula, Duplicati)

- Межсетевое экранирование (pfSense)

- Удаленный доступ (OpenVPN)

- Управление инцидентами (TheHive)

- Инвентаризация активов (Zabbix, Lansweeper)

- Гарантированное стирание информации (KillDisk)

- Самостоятельное тестирование на проникновение (OWASP ZAP, Metasploit)

А что думают регуляторы?

Российское законодательство до недавних пор относилось к применению Open Source решений с осторожностью. Однако ситуация изменилась после утверждения Указа Президента № 250, который напрямую запрещает субъектам КИИ (критической информационной инфраструктуры) применение средств защиты информации из недружественных стран. Проблема в том, что большинство популярных Open Source инструментов производится именно там. Таким образом, в настоящий момент на объектах КИИ запрещено использовать решения с открытым исходным кодом для обеспечения информации безопасности.

В нашей стране сегодня по разным оценкам действует более 50 тыс. объектов КИИ, при этом лишь единицы из них обеспечивают применение исключительно отечественных сертифицированных средств защиты информации. Значительная же их часть для учета информационных активов, например, использует Zabbix и другие перечисленные выше инструменты – для иных задач. Импортозамещение проходит достаточно медленно, поэтому пока не получается исключить возможность применения иностранных средств защиты информации, включая решения с открытым исходным кодом. Нет сомнений, что рано или поздно российские вендоры оптимизируют производство и обеспечат адекватные ценники на свои продукты, позволяющие эффективно заниматься импортозамещением.

Также следует заметить, что штраф, который предусмотрен за использование несертифицированных средств защиты информации, составляет максимум 25 тыс. рублей. Поэтому 99% организаций проще платить штраф, нежели тратить на несколько порядков больше денег на приобретение сертифицированных средств защиты информации. Ведь, к примеру, приобретение и интеграция в инфраструктуру SIEM-системы, способной обрабатывать до 2 тысяч событий в секунду, обойдется в среднем от 2 до 2,5 млн руб., что в сто раз превышает максимальную сумму штрафа.

В финансовой сфере помимо требований по защите ПДн какие-либо санкции за использование Open Source инструментов вообще отсутствуют. Так, главный стандарт по защите финансовой информации ГОСТ 57580.1 имеет единственное требование по использованию сертифицированных средств защиты информации в рамках процесса реализации мер защиты информации. При этом невыполнение или частичное выполнение данной меры имеет некритичное влияние в рамках общей оценки соответствия требованиям. Аналогичная ситуация и для планируемой к утверждению обновленной версии данного документа. То есть в финансовой сфере пока не предвидится существенных изменений в применении Open Source.

Итак, использование инструментов на базе открытого исходного кода в 2025 году для обеспечения информационной безопасности допустимо для части сфер, однако несет дополнительные риски и требования для сотрудников организации. Open Source должен внедряться только тогда, когда у организации есть возможность самостоятельно поддерживать используемые средства защиты информации. Это означает обязательное наличие высококвалифицированных сотрудников, которые смогут всё корректно настроить и

задействовать полный функционал, предполагаемый разработчиком. Таких специалистов найти нелегко, не говоря уже о высоком уровне оплаты их труда.

Что же делать в таком случае? Выбирать более квалифицированных специалистов, способных самостоятельно развернуть систему защиты информации, построенную исключительно на Open Source, или закупать только отечественные средства защиты информации?

Этот выбор стоит особенно остро в условиях дефицита специалистов на рынке и учитывая растущие ценники на отечественные продукты. Хотя в любом случае оба варианта являются проигрышными, поскольку в долгосрочной перспективе не будут способствовать развитию рынка. Я бы рекомендовал отдавать приоритет квалифицированным кадрам. Ведь без грамотных специалистов не получится обеспечить в полном объеме применение даже самых многофункциональных и гибких сертифицированных средств защиты информации в будущем.

Андрей Меркулов, *консультант по информационной безопасности RTM Group*
Окончил ВГУИТ по специальности информационная безопасность автоматизированных систем, более трех лет работает в сфере ИБ, более года - в компании RTM Group (https://rtmtech.ru/)

Как измерить вероятность угрозы

В процессе исследования рисков, включая анализ возможных сценариев, бывает сложно определить, какие риски наиболее опасны, наиболее вероятны и на какие из них следует в первую очередь фокусировать внимание. Если сравнивать риски между собой по возможным последствиям, то определить, какие из них приоритетны, не составляет большого труда. Но что касается их вероятности, то здесь все не так просто.

Физическая охрана сегодня не имеет готовой формулы или методологии определения вероятности рисков и угроз. С другой стороны, потратив определенное время на мониторинг и анализ рисков с использованием математики, профессионал в сфере управления рисками может выработать достаточно точные индикаторы вероятности инцидентов безопасности.

Блогер Даниель Янг (https://www.circadianrisk.com), имеющий большой опыт аналитика и консультанта в области корпоративной безопасности, предлагает использовать следующие индикаторы:

1. Локация

Физическая локация представляет собой гигантский информационный ресурс. По ней вы определяете наиболее вероятные риски: уровень криминала в регионе, наличие и активность ОПГ, факторы городской или сельской среды. Все эти данные в совокупности показывают, как внешние угрозы могут влиять на ваш бизнес.

2. Время

Время года, сезона, дня также помогает в определении вероятности рисков. Несанкционированные проникновения в офисы зачастую происходят во внерабочее время, по ночам. В зависимости от календаря вы можете заблаговременно оценить потенциальные природные риски: наводнения, пожары и т.п. Плюс праздники, когда риски, как правило, повышаются.

3. Исторический контекст

С какими инцидентами безопасности вы уже сталкивались? Если фирма подвергалась грабежу, то это может повториться. Если хакеры уже взламывали вашу корпоративную сеть, то ждите повторения. Конечно, речь не о всех без исключения угрозах (землетрясения повторяются не часто), но важно иметь в виду, что если инцидент случился, то вероятность его повторения достаточно высока.

4. Активные внешние факторы

Кто-нибудь угрожал вашей организации в онлайне? Получали ли ваши партнеры и конкуренты по бизнесу угрозы? Анализ непосредственных угроз, равно как и угроз в адрес схожих организаций, дает важные ключи к оценке вероятности рисков. Вот почему так важно отслеживать социальные сети и иную онлайновую активность, быть в курсе того, что говорят в интернете о вашей компании.

5. Внутренние факторы

Многие компании концентрируют внимание на внешних рисках и угрозах, реже – на внутренних. И это большая ошибка. Именно угрозы, исходящие изнутри организации, могут оказаться наиболее разрушительными для бизнеса. Вы хорошо знаете своих коллег, подчиненных? Кого из них следует рассматривать как проблемных сотрудников? Держите в памяти все внутренние инциденты безопасности, случавшиеся в прошлом. Интересуйтесь у кадровиков относительно жалоб работников на своих коллег.

Вероятность и возможность.

Это не одно и то же, утверждает Янг. А в чем разница?

Прогноз возможности того или иного инцидента не означает его вероятности, пишет автор блога. Последняя определяется с помощью постановки правильных вопросов, разбора возможных сценариев, анализа ее потенциала. Необходимо поставить себя на место преступника и понять логику его действий. Что и как вы бы «хотели и могли украсть у компании». Или «взломать базу данных с конфиденциальной информацией». То есть важно смотреть на ситуацию со стороны.

Итак, наилучший путь попытаться определить вероятность инцидента, это провести глубокий анализ рисков, который охватывает как вероятность, так и уровень серьезности возможного инцидента. В результате вы будете иметь в руках список потенциальных инцидентов с высокой степенью вероятности как основу для эффективных контрмер.

Как изучение видеозаписей в ходе расследования воздействует на мозги

Повсеместное использование камер видеонаблюдения давно превратилось в базисный элемент обеспечения охраны, безопасности и проведения расследований. Но только недавно ученые стали обращать внимание на последствия, вызванные интенсивной, продолжительной работой операторов мониторинга на психику и мозги.

Процесс изучения криминала по видеозаписям представляет собой сложное сочетание трех последовательных этапов: 1) обнаружения признаков явления (угрозы), 2) распознавания его характеристик, 3) эмоционального реагирования, пишет психолог в сфере финансовых расследований Диана Конканнон, в публикации журнала Security Management.

В чисто физическом смысле наши глаза воспринимают свет как «электрические сигналы», обрабатываемые в зрительной зоне коры головного мозга. При их попадании в эту зону происходит процесс выявления первоначальных признаков, когда специальные нейроны идентифицируют текстуру, глубину, цвет, движение. Затем данные признаки накладываются на характеристики, известные нам по своему опыту, к примеру, поведенческие характеристики. На третьем, более высоком когнитивном уровне, происходит эмоциональное реагирование.

К примеру, человек сначала воспринимает физически видимые детали преступления: злоумышленника, жертву, место преступления. В зависимости от подготовки и опыта он фокусирует внимание на такие особенности как метод нападения, средства атаки, реакции жертвы. Возникает соответствующая эмоциональная реакция. Все эти три фактора, отмечает психолог, формируют умозаключение, на основании которого принимаются меры реагирования.

Автор упомянутой статьи разбирает вызовы и проблемы, связанные с происходящими в коре головного мозга процессами.

Усталость

Усталость, вызванная продолжительным и многократным просматриванием одних и тех же видеозаписей, ослабляет способность мозга адекватно воспринимать происходящее, обращая преувеличенное внимание на обычные (нормальные) признаки и упуская из виду другие, может быть, более важные.

Когнитивная перегрузка

Даже при сохранении физической способности идентифицировать объекты, личности, место и события продолжительное изучение одних и тех же видеоматериалов чревато когнитивной (познавательной) перегрузкой и может привести к предвзятому, необъективному восприятию. В этом случае мозг преобразует определенные видимые индикаторы в нарратив, игнорируя иные сигналы и импульсы, что впоследствии формирует «рациональный», но при этом не обязательно точный вывод о том, что на самом деле произошло.

Подверженность предвзятому восприятию во многом обусловлена прошлым опытом, который провоцирует мозг обрабатывать информацию по уже известным, наработанным стандартам, если речь идет о преступлении, аналогичном тем, с которым оператор мониторинга (расследователь) уже имел дело в прошлом. Мозг так устроен, что он предпочитает идти по уже проторенному пути. В нём происходит конфликт между тем, что хорошо известно, и тем, что в реальности. Этот феномен носит названия «эффект иллюзорной истины» или «эффект иллюзии правды». Он, кстати, регулярно используются в политике и рекламе.

Аффективная (эмоциональная) реакция

Данный фактор имеет отношение к секции мозга, именуемой «амигдала», которая ассоциируется с расстройствами тревожного спектра. Он может провоцировать так называемую «викарную травму» - тип стрессовой реакции, которая возникает, когда человек становится свидетелем боли и страданий других людей, сопереживает им (викарную травму иногда называют «вторичным стрессом»). Будучи распространенным явлением в среде профессионалов охраны и безопасности, она часто оказывает воздействие на мировоззрение, основные убеждения и предположения, изменяет отношение к себе и другим, влияет на поведение и взаимодействие с окружающими. В конечном итоге, может исказить умозаключения в процессе расследования преступления.

Как преодолевать негативное воздействие отмеченных факторов и явлений? Эксперты советуют:

В ходе расследования регулярно брать паузу для отдыха. Интенсивность – не всегда эффективность. Ученые подметили, что такие паузы, заполненные прогулкой на свежем воздухе, перекусом или любым другим занятием подальше от компьютера, по продолжительность от 10 до 30 минут, поддерживают оптимальную концентрацию и минимизируют проявления усталости.

Сохранить когнитивный баланс и гарантировать объективные результаты легче всего с помощью разностороннего мышления. В идеале – предоставить своему коллеге возможность просмотреть видеозаписи и затем сравнить впечатления. Если это сделать нельзя, то можно сыграть роль «адвоката дьявола» в отношении своего заключения. Вы критически анализируете свои умозаключения, подключив когнитивный процесс, в котором не доверяете своему чутью или не хотите, чтобы вами овладела та или иная эмоция.

Что касается аффективных эмоциональных реакций, то пытаться их игнорировать бесполезно. Надо их не игнорировать, но использовать с пользой. Они ведь могут служить своего рода барометром вашего состояния, сигнализируя об усталости, переутомлении. Тогда необходимо взять паузу на отдых.

Сергей Шеметов
Кибербезопасность организации в условиях ограниченного бюджета. Статья вторая

В первой статье (см. выпуск журнала №95) рассматривались возможности и варианты пентеста, позволяющие вовремя понять и предупредить попытки злоумышленника попытаться проникнуть в вашу инфраструктуру.

В данной статье характеризуется и сравнивается каждый из элементов защиты.

Бесплатные и недорогие инструменты

Не всегда целесообразно с экономической точки зрения приобретать дорогие решения. На рынке имеется множество бесплатных и недорогих инструментов, которые могут значительно улучшить уровень киберзащиты.

- **Бесплатные антивирусы:** некоторые антивирусные программы предлагают базовую защиту от вирусов и вредоносных программ, а их бесплатные версии могут быть вполне достаточными для малого и среднего бизнеса.

- **Многофакторная аутентификация (MFA):** один из самых эффективных способов защитить данные и системы, при этом многие сервисы предоставляют MFA бесплатно.
- **Шифрование данных:** Важно обеспечить шифрование данных как в процессе хранения, так и при их передаче. На рынке можно найти бесплатные решения для шифрования файлов.
- **Обновление ПО и патчи:** Регулярное обновление программного обеспечения является важнейшей и необходимой частью стратегии безопасности. Устаревшие версии программ и операционных систем часто становятся уязвимыми для атак. На практике многие компании забывают об этой мере безопасности, подвергая организацию неоправданным рискам.

Обучение сотрудников компании

Наиболее слабый элемент любой системы безопасности — это люди. Фишинг, социальная инженерия и другие мошеннические атаки на персонал остаются главными способами взлома систем. Обучение сотрудников основам безопасности — одно из самых экономичных решений.

Рекомендуется проводить регулярные тренинги по безопасности, обучая сотрудников распознавать фишинговые письма, не переходить по сомнительным ссылкам. Разработать простые инструкции по безопасности для сотрудников, включая правила работы с паролями, использование VPN и другие рекомендации.

Сегментирование данных и ограничение прав доступа

Для защиты информации важно ограничить доступ к критически важным данным. Разделите данные на категории, установив различные уровни доступа для сотрудников в зависимости от их роли в организации. Это поможет минимизировать ущерб от утечки информации или атаки.

Кроме того, важно настроить систему контроля доступа. Используйте принцип наименьших привилегий: предоставляйте сотрудникам доступ только к тем данным и системам, которые необходимы для выполнения их задач.

Регулярно проверяйте, кто имеет доступ к чему, и обновляйте эти права по мере изменений в штате.

Внедрение решений по мониторингу

Мониторинг и обнаружение угроз на ранних стадиях —ключ к успешной защите от кибератак. Для небольших организаций на рынке много недорогих решений, которые позволяют мониторить сеть и систему на наличие подозрительной активности.

Включите в вашу инфраструктуру:

- IDS/IPS (системы обнаружения и предотвращения вторжений): недорогие решения для мониторинга трафика и выявления подозрительных действий.
- Логирование и анализ событий: использование простых систем для анализа логов, которые могут помочь в своевременном обнаружении атак. Для малых организаций есть решения, которые предоставляют базовую защиту, и зачастую они включают в себя функции для мониторинга и выявления угроз.

При создании своего технологического стека вам также придется учитывать расходы на специалистов, осуществляющих мониторинг внедренных решений. Другой вариант - использовать технологии искусственного интеллекта.

Отслеживание поведения с помощью продвинутого ИИ

Большая часть того, что может делать ИИ — мониторинг и выявление закономерностей или аномалий. Технология развивается, и теперь ИИ может анализировать собранные данные о

поведении в сети. Эта технология достаточна эффективна. Она очищает данные и выдает результаты, помогающие понять методы атак и как защищаться от них.

Есть еще одно преимущество, ради которого стоит инвестировать в ИИ, это автоматизация процессов. Автоматизация повышает производительность и обеспечивает высокую окупаемость инвестиций. Средства автоматизации, помогающие управлять, проверять, исправлять и отслеживать вашу безопасность, однозначно должны быть в вашем бюджете. Эти средства заменяют множество ручных, повторяющихся задач, позволяющих сотрудникам сосредоточиться на стратегических задачах вместо рутинной работы. Главное – понять свою конечную цель, связанные с ней процессы, чтобы определить, что и как использовать.

Некоторые категории включают:

- Мониторинг и оповещение об угрозах безопасности.
- Системы обнаружения и предотвращения сетевых вторжений.
- Обновления программного обеспечения для устройств, подключенных к сети.
- Инструменты ведения журнала безопасности.
- Отслеживание состояния активов.

Планирование потенциальных угроз:

Разработка плана реагирования на инциденты не требует больших затрат, но может радикально уменьшить последствия кибератаки. В плане необходимо:

- Определить, как будет реагировать команда на инциденты, кто за что отвечает.
- Разработать процедуру извлечения данных и восстановления систем.
- Регулярно тестировать и обновлять план.

Использование облачных решений

Облачные сервисы могут предложить организации надежную защиту данных за разумные деньги. Многие крупные облачные провайдеры имеют встроенные механизмы безопасности, такие как шифрование, резервное копирование, автоматические обновления. Использование облачных решений позволяет снизить затраты на аппаратные средства и сделать защиту более масштабируемой.

Инвестирование в людей

Использование средств бюджета на повышение квалификации, обучения и сертификации персонала организации всегда является мудрым вложением. Сотрудники более качественно выполняют свои обязанности. Уменьшается текучесть кадров. Кибербезопасность — динамичная, постоянно меняющаяся экосистема, и команде нужно постоянно учиться способам противостояния киберкриминалу.

Наряду с техническими навыками следует подумать о том, как помочь сотрудникам развивать soft-skills. Вложения здесь окупаются так же, как инвестиции в hard-skills. В такой стрессовой среде как кибербезопасность специалисты, обладающие навыками общения, весьма востребованы. Такого рода инвестиции в команду демонстрируют ваше стремление, чтобы сотрудники были успешными, вносили больший вклад в решение задач. Для тренингов и занятий по ознакомлению с киберрисками и угрозами не нужен большой бюджет. Возможно, вы потратите какое-то время на программу занятий, но безопасность данных клиентов и партнеров стоит того.

Обеспечить кибербезопасность в организации с ограниченным бюджетом — вполне осуществимая задача. Комбинируя грамотный подход, использование бесплатных и недорогих

инструментов, обучение сотрудников и оптимизацию инфраструктуры, можно значительно повысить уровень безопасности, не выходя за рамки бюджета. Важно помнить, что безопасность — это процесс, а не одноразовая мера, и регулярное обновление и проверка внедренных решений поможет держать угрозы под контролем.

Главное — это грамотно оценивать риски и использовать доступные ресурсы с максимальной эффективностью.

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

Пять важных моментов, которые вы должны знать об угрозах вымогательства

Программы-вымогатели продолжают оставаться в числе наибольших угроз бизнесу, несмотря на предпринимаемые специалистами по кибербезопасности всевозможные меры. Хакеры постоянно меняют тактику, все чаще нацеливаются на компании среднего размера, берут на вооружение инновации, связанные с искусственным интеллектом. Их атаки грозят широкомасштабными нарушениями бизнес процессов, утечками массивов конфиденциальной информации, огромным материальным и финансовым уроном.

Одно из ведущих изданий в международной отраслевой прессе по вопросам охраны и корпоративной безопасности Chief Security Officer разместило аналитический материал эксперта Р. Пейдж о ключевых моментах, которые профессионалы должны учитывать, противодействуя вымогательским атакам.

1. Чрезмерная концентрация внимания на используемых криминалом технологиях генеративного искусственного интеллекта чревата недооценкой давно и хорошо известных угроз

Хотя генеративный ИИ в целом способен умножить существующие риски и угрозы, традиционные, сравнительно простые схемы (фишинг, социальная инженерия) сохраняют высокую эффективность.

Проведенное британской компанией Sophos (разработка программного обеспечения и оборудования для безопасности) исследование о вымогательских программах в 2024 году показало, что не устраненные уязвимости в системе кибербезопасности, скомпрометированные учетные данные, вредоносные имейл-сообщения, банальные фишинговые наживки остаются главными причинами успешности вымогательских атак. Хакеры используют в своих целях плохо управляемую или совсем не управляемую цифровую корпоративную среду. Поэтому ни в коем случае нельзя недооценивать такие фундаментальные меры защиты как мультифакторная аутентификация, обязательное латание выявленных брешей в информационной защите, своевременное обновление программного обеспечения и носителей информации. Эти процедуры не должны приноситься в жертву повальному увлечению искусственным интеллектом.

2. Средние предприятия наиболее уязвимы

Реальность такова, что крупный бизнес уже не является исключительным объектом программ-вымогателей. Не меньшему риску сегодня подвергаются и средние по размеру компании. Консалтинговая фирма Rapid7 провела исследование и выяснила, что, например. американские компании с доходом 5 млн долларов подвергаются вымогательским атакам вдвое чаще, чем компании с доходом 30-50 миллионов, и в 5 раз чаще, чем компании с доходом 100 миллионов долларов (https://www.rapid7.com/research/report/ransomware-radar-report/). Отчасти такая картина объясняется стремлением преступников выбирать более легкую добычу, поскольку крупный бизнес намного надежнее защищен от киберугроз, чем малый и средний бизнес. В то же время важно иметь в виду, что партнерские отношения с меньшими по размеру компаниями также несут угрозу для крупных корпораций.

3. Атаки, нацеленные на кражу данных, требуют изменения приоритетов информзащиты

В последние годы прослеживается такая тенденция: получив доступ к наиболее ценной интеллектуальной собственности организации, преступники все чаще угрожают сливом информации, если не будет выплачен выкуп. Такие атаки могут нанести технологическим компаниям непоправимый ущерб, отмечают эксперты Positive Technologies, ведь в результате утечки данных конкуренты получают доступ к исходному коду продукта или данным исследований и разработок. Компания Coveware подсчитала, что 87% хакерских взломов в последнем квартале 2024 года включали угрозу эксфильтрации данных.

Эксперты рекомендуют сконцентрировать усилия вокруг защиты данных, мониторинга рисков, быстрого обнаружения угроз. Для этого требуется установить многоуровневую систему защиты, прежде всего наиболее ценных, критических важных баз данных.

4. Повышенные риски для критической инфраструктуры

Многие организации, занятые в сфере энергетики, коммунальных услуг, не спешат с модернизацией программного обеспечения и технологий, что делает их сравнительно легкой добычей для хакеров-вымогателей. Специалисты выражают обеспокоенность, что уязвимость компаний критической инфраструктуры может иметь далеко идущие последствия для национальной безопасности. Проникновение в сети таких организаций может храниться хакерами в тайне долгое время, на случай будущих возможных цифровых войн.

5. Коллапс периметров защиты

По мере расширения цифрового периметра организаций увеличивается и площадь для потенциальных хакерских атак. Периметр сегодня включает дивайсы интернета вещей, облачные приложения, VPN-шлюзы, другие инструменты доступа в сеть. Периметр нельзя считать прочным, если нарушаются правила пользования действующими учетными записями, не закрываются дыры в системе кибербезопасности, не используется многофакторная аутентификация, не устраняются слабости в практике управления идентификационными данными и паролями.

Хотя значение продвинутых технологий и инструментов безопасности никем не оспаривается, оно не должно заслонять от нас важность защиты цифрового «парадного входа», годами наработанных навыков и приемов. Досадные распространенные ошибки и ляпы, как, к примеру, слабые пароли, или незащищенные дистанционные доступы в сеть, могут обнулить усилия и затраты на самые современные и дорогие технологии, в том числе и искусственного интеллекта.

Глобальные риски: сегодня, завтра, в среднесрочной перспективе (исследование)

Почти не замеченным мировой прессой результатом последнего давосского форума (World Economic Forum - WEF) явилось проведенное организаторами форума традиционное исследование «The Global Risks Report 2025», в ходе которого были опрошены без малого тысяча экспертов по вопросам политики, экономики, военных конфликтов.

«Стоящие перед человечеством риски становятся все более сложными и острыми, акцентирующими эволюцию парадигмы мирового порядка в направлении большей нестабильности, поляризации общества, разрушения доверия, небезопасности», пишет в предисловии отчета управляющий директор WEF Саадия Захиди. «Более того, наблюдаемая тенденция развивается на фоне слабости правительственных структур перед лицом старых и зарождающихся новых рисков, делающих мир более хрупким и уязвимым».

Авторы исследования попытались заглянуть в будущее, измерить соотношение глобальных рисков и угроз для человечества. Участвовавших в опросе экспертов попросили расставить в порядке первоочередной опасности 5 рисков сегодняшнего дня, а также - как они видятся в 2027 году и через 10 лет, в 2035 году. Получилась следующая картина:

Глобальные риски 2025 года

1. Вооруженные межгосударственные конфликты
2. Экстремальные климатические катаклизмы
3. Геоэкономическая конфронтация
4. Недостоверная и ложная информация
5. Социальная поляризация

Сюда не попало неравенство в развитии, которое рассматривается как один из важных, центральных рисков для мира.

В докладе отмечается «затухающее стремление» к многостороннему сотрудничеству и взаимодействию. В подтверждение этой тенденции авторы доклада ссылаются на статистику: в 2016 году под эгидой ООН находилось более 100 000 миротворцев в разных регионах мира, а в 2024 году – всего 68 000. Налицо опасность, что все больше правительств теряют веру не только в институт ООН, но и вообще в способность многостороннего международного сотрудничества решать насущные проблемы, говорится в докладе.

Прогнозируемые риски в 2027 году

1. Недостоверная и ложная информация
2. Экстремальные климатические катаклизмы
3. Вооруженные межгосударственные конфликты
4. Социальная поляризация
5. Кибервойны и шпионаж

В отчете исследования подчеркивается, что распространение и усовершенствование цифровой среды, наращивание компьютерных мощностей на фоне растущей социальной поляризации ставят людей в более уязвимую позицию с точки зрения онлайновой безопасности, подрывая их веру в институты, в информацию.

Прогнозируемые глобальные риски в 2035 году

1. Экстремальные климатические катаклизмы

2. Утрата биоразнообразия и коллапс экосистемы
3. Критическое изменение систем и подсистем Земли
4. Дефицит природных ресурсов
5. Недостоверная и ложная информация

Респонденты поставили на первое место природные стихии, которые обычно рассматривались как угрозы в долгосрочной перспективе, но, похоже, сегодня воспринимаются как главная опасность для мира уже в обозримом будущем. Две три участников опроса выразили «максимальную озабоченность» загрязнением окружающей среды. Вредные для экологии последствия производства и потребления вызывают изменения климата, загрязнения, утрату биоразнообразия – «тройной планетарный кризис», принятый в ООН термин, который подчеркивает взаимозависимость этих проблем и их коллективное воздействие на экосистемы планеты, общества и экономику.

Обращает также на себя внимание третий по приоритетности пункт: «критическое изменение систем и подсистем Земли». Здесь имеются в виду взаимодействия и "обратные связи" посредством материальных и энергетических потоков, между циклами, процессами и "сферами" подсистем Земли - атмосферой, гидросферой, криосферой, геосферой, педосферой (почвенной оболочкой Земли), литосферой (земной корой и верхней частью мантии), биосферой, магнитосферой, а также влиянием человеческих сообществ на эти компоненты.

Полный текст доклада см. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf

Рецензия

Premier CISO—Board & C-Suite: Raising the Bar for Cybersecurity

By Michael Oberlaender. Self-published; 191 pages

Профессор Евгений Спэффорд из Purdue University (США) однажды так сформулировал один из важнейших принципов управления корпоративной безопасностью: «Если вы возглавляете службу безопасности, но не обладаете правом устанавливать правила и наказывать провинившихся, то в случае провала должны винить только себя».
(https://www.technologyreview.com/2004/10/31/232154/yoran-and-spafs-law/).

Автор рецензируемой книги Микаель Оберлэндр подробно разбирает отношения руководителя информбезопасности с советом директоров компании. Он выражает мнение многих экспертов, что слишком часто на эту должность подбирают кандидата по главенствующему критерию технологических знаний и навыков, полагая, что этого достаточно, чтобы успешно решать вопросы безопасности.

Однако технологии сами по себе не способны решать многоаспектные и сложные задачи корпоративной безопасности. Многое зависит от умения (и желания) начальника по безопасности установить тесные контакты с акционерами и топ-менеджерами, завоевать их доверие и уважение. Для этого необходимо научиться говорить с ними на понятном им языке. То есть на языке бизнеса, а не технологии.

Оберлэндер фокусирует внимание на прагматических, практических аспектах работы директора по информационной безопасности. Теории в книге совсем немного. Зато предостаточно конкретных рекомендаций, основанных на богатом опыте работы автора на этой должности в ряде организаций.

Лидерами не рождаются. Ими становятся. Лидерские компетенции выковываются в процессе неустанного труда, накопления опыта, постоянного обучения всему новому. Для всех, кто хочет быть успешным в сфере корпоративной безопасности, книга чрезвычайно полезна.