АКТУАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ

ПРЕДИСЛОВИЕ.

Миссия книги- профилактика КиберПреступности. Серия «Понятная КиберГигиена» содержит полезные советы по Информационной безопасности для начинающих и продвинутых пользователей, профессионалов и преподавателей учебных центров. Материалы могут быть использованы для проведения- АУДИТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, инструктажей, тренингов, консультаций, коучингов и мастер-классов по актуальным темам-

- Экспертиза веб-сайтов и приложений
- Соответствие требованиям Регуляторов
- Compliance management
- Antifraud management
- Методология
- Восстановление соответствия внутренней нормативной базы
- Регуляторные риски
- Защита Персональных Данных, чувствительной и конфиденциальной информации
- Соответствие Политики Информационной Безопасности
- Консультации, классы, коуч-сессии, лекции, тренинги, инструктажи, курсы по информационной безопасности и защите персональных данных
- Архитектурные решения кибербезопасности, и другие аспекты кибербезопасности.

В книге читатель найдёт полезные советы по соблюдению правил Цифровой Гигиены в Интернете и рекомендации по профилактике классического и новаторского мошенничества с использованием последних достижений информационных технологий, а также советы по безопасности в информационной среде. Авторы надеются, что Меры Кибербезопасности помогут читателям грамотно ориентироваться в операциях с криптовалютой, бороздить самые тёмные уголки ДаркНета и , возможно, уберегут кого-то от киберинцидентов, изощрённых хакерских атак и кражи чувствительной и конфиденциальной информации.

Профессионалы найдут полезные рекомендации по соответствию требованиям/ стандартам Регуляторов и методологии для требующей постоянного обновления Политики Информационной Безопасности предприятия.

1. ПРОГНОЗЫ КИБЕРБЕЗОПАСНОСТИ

Прогнозы Кибербезопасности. Подготовка к завтрашним угрозам, вызовам и стратегическим изменениям

Развитие генеративного искусственного интеллекта и стремительное распространение цифровых инициатив вынуждают организации отслеживать изменения в своей деятельности и управлять ими. По мере того, как руководители в сфере безопасности и управления рисками преодолевают последствия недавних изменений и переходят к этапам обновления, им необходимо учитывать перспективные стратегические планы при распределении ресурсов, выборе продуктов и определении приоритетности услуг и инициатив. Как же этим руководителям быть в курсе будущего цифровых технологий в постоянно меняющейся среде?

Глава содержит главные прогнозы экспертов по кибербезопасности на 2025 год и далее. Читатели получат ответы на свои важные вопросы, рекомендации по созданию успешной, готовой к адаптации программы кибербезопасности, адаптированной к цифровой эпохе и рекомендации, которые помогут вам достичь ваших целей.

Основные стратегические технологические тенденции этого года связаны с императивами и рисками в области искусственного интеллекта, новыми границами вычислений и взаимодействием человека и машины, Отслеживание этих тенденций поможет руководителям ИТ-отделов формировать будущее своих организаций с помощью ответственных и этичных инноваций.

В этой главе проводится попытка оценки состояния отрасли и того, как она должна измениться, чтобы мы могли успешно противостоять угрозам завтрашнего дня.

Исследователи и руководители видят развитие таких актуальных тем, как искусственный интеллект, облачные технологии, киберпреступность, шпионаж и программы-вымогатели, в будущем. Прогнозы на 2025 год: специалисты по безопасности и рискам будут готовиться к новым правилам и повышению устойчивости

В 2024 году регулирующие органы по всему миру представили множество предложений по политике и законодательству в области кибербезопасности и конфиденциальности, чтобы лучше управлять возникающими рисками, связанными с новыми технологиями, такими как генеративный искусственный интеллект (genAI), а также рисками, связанными с управлением отношениями с третьими сторонами. Руководители в сфере безопасности и управления рисками стремились обеспечить безопасность genAI, даже несмотря на то, что его варианты использования всё ещё развивались; почти в каждой отрасли происходили критические сбои в работе ИТ-систем из-за отсутствия планирования отказоустойчивости; и, несмотря на преуменьшение рисков, связанных с третьими сторонами, организации по всему миру столкнулись с увеличением числа нарушений в цепочках поставок программного обеспечения.

Поскольку ожидается, что в 2025 году киберпреступность обойдётся в 12 триллионов долларов, регулирующие органы будут играть более активную роль в защите данных потребителей, а организации перейдут к более активным мерам безопасности, чтобы ограничить материальный ущерб. Прогнозы Forrester в области кибербезопасности, рисков и конфиденциальности на 2025 год отражают то, как организациям необходимо развиваться, чтобы справляться с этими новыми видами рисков. Вот три из этих прогнозов:

Из-за отсутствия измеримой ценности 10% директоров по информационной безопасности откажутся от использования генного ИИ. Согласно статистическим данным за 2024 год, 35% директоров по информационной безопасности и ИТ-директоров по всему миру считают изучение и внедрение генного ИИ для повышения производительности сотрудников своим главным приоритетом. Рынок продуктов для обеспечения безопасности быстро распространил информацию о предполагаемых преимуществах генного ИИ для повышения производительности, но отсутствие практических результатов приводит к разочарованию. Мысль об автономном центре управления безопасностью, использующем генеративный искусственный интеллект, вызвала большой ажиотаж, но это далеко от реальности. В 2025 году эта тенденция сохранится, и специалисты по безопасности будут всё больше разочаровываться, поскольку такие проблемы, как недостаточный бюджет и

нереализованные преимущества ИИ, сокращают количество внедрений генеративного искусственного интеллекта, ориентированных на безопасность.

Расходы на коллективные иски, связанные с утечкой данных, превысят штрафы регулирующих органов на 50%. Расходы, связанные с утечкой данных, больше не ограничиваются штрафами регулирующих органов и затратами на устранение последствий. Исторически сложилось так, что киберрегуляторы не предпринимали достаточных мер для защиты клиентов и сотрудников, из-за чего эти же люди подавали коллективные иски и требовали возмещения ущерба. Расходы на коллективные иски при утечке данных огромны. А поскольку процент компаний, столкнувшихся с коллективными исками, достиг 13-летнего максимума, CISO попросят внести взносы в фонд защиты компаний от коллективных исков в 2025 году, в результате чего расходы от коллективных исков значительно превысят штрафы, налагаемые регулирующими органами.

Будет запрещено использование определённого стороннего программного обеспечения или ПО с открытым исходным кодом. Атаки на цепочки поставок программного обеспечения являются основной причиной утечек данных в организациях по всему миру. Растущее давление со стороны западных правительств, требующее от частных компаний составлять списки используемых в программном обеспечении материалов (SBOM), стало благом для прозрачности компонентов ПО, но эти SBOM подчёркивают роль стороннего ПО и ПО с открытым исходным кодом в продуктах, которые закупают правительства. В 2025 году правительство, располагающее этой информацией, ограничит использование ПО с открытым исходным кодом по соображениям национальной безопасности. Чтобы соответствовать требованиям, поставщикам программного обеспечения необходимо будет удалить проблемный компонент и заменить его функциональность. Дополнительные прогнозы связаны с Законом ЕС об искусственном интеллекте и безопасностью устройств Интернета вещей.

Взгляд на кибербезопасность

Прошедший год показал, что наша коллективная защита на самом высоком уровне находится в плачевном состоянии. Будь то компрометация цепочек поставок, взлом сетевых устройств, ставший возможным благодаря, казалось бы, бесконечному потоку уязвимостей нулевого дня, или взлом самих поставщиков базовых услуг, даже крупнейшие разведывательные организации и предприятия не могут обеспечить эффективную защиту. Учитывая, что «небезопасность» является неотъемлемым свойством

«нисходящей транзитивности», это не сулит ничего хорошего ни одному из нас как пользователям, потребителям и гражданам, зависящим от целостности этих вышестоящих организаций.

Истинным триумфом в этом коллективном провале стал сдвиг парадигмы в методах работы более продвинутых китайских хакеров (недавно в качестве примера можно привести «Вольт Тайфун», «Солт Тайфун» и другие менее известные группы хакеров). Эта часть китайского хакерского аппарата эффективно использовала наши коллективные уязвимости — в первую очередь повсеместное использование сетей без указания авторства (ORB) в качестве неуправляемых туннелей в наши страны.

Эти туннели создаются с помощью (иногда предоставляемых на аутсорсе) комбинаций небезопасных устройств, маршрутизаторов и сегментов виртуальных частных серверов в нескольких облаках, которые эффективно служат VPN для APT-атак, выходящих с ранее невиданных (нейтральных или безопасных) IP-адресов, физически расположенных в стране жертвы и регулярно меняющихся. В сочетании с более «старомодным» стилем взлома с помощью клавиатуры, при котором хакеры больше заботятся о том, чтобы не оставлять улик, не использовать специальные инструменты и, возможно, даже не сохранять данные (благодаря постоянно уязвимым устройствам, подключённым к интернету), эти туннели фактически обеспечили некоторым злоумышленникам уровень безнаказанности в отношении организаций-жертв и их растерянных правительств.

Если мы не готовы принять пассивную систему слежки, связанную с Китаем, в качестве постоянного элемента американской жизни (и жизни многих других западных стран, о которых не сообщается), коллективная кибербезопасность требует фундаментальной перестройки, которая должна включать в себя изменение менталитета частного сектора в сторону обмена информацией, раскрытия данных и сотрудничества, юридический пересмотр препятствий для обмена информацией, основанных на предполагаемой «ответственности», в сочетании с режимом быстрого, значимого и надёжного регулирования, защитой от ответственности и стимулами, а также повышением прозрачности и подотчётности. Нам нужно перейти к этапу «правды и примирения» в сфере кибербезопасности.

По сути, нам нужно коллективно работать над основными принципами, изложенными в введении к киберстратегии. В настоящее время коллективные сбои в системе безопасности допустимы, поощряются, а иногда даже вознаграждаются нашей нынешней парадигмой. Нам нужно работать над коллективным изменением системы стимулов, чтобы поощрять принятие

сложных решений и инвестиции в значимые улучшения системы безопасности.

С точки зрения правительства, политики и нормативно-правового регулирования нам также необходимо перераспределить ответственность за кибербезопасность между наиболее компетентными организациями как в частном, так и в государственном секторе. При этом нам нужно убедиться, что мы устранили препятствия, бюрократические проволочки, (мнимые или реальные) обязательства и снизили общий уровень паники и размывания ответственности, которые напрямую связаны с крупномасштабными инцидентами.

В эпоху гиперконсолидации в сфере кибербезопасности, когда на рынке доминируют крупные непокорные публичные компании, корпоративному руководству, как правило, сложнее делать «правильный выбор». Это требует сильного и чёткого руководства, ориентированного на безопасность, особенно в условиях принятия решений, которые могут негативно сказаться на коллективной безопасности и принести немедленную прибыль. Нам нужно донести до всех, что среднесрочная акционерная стоимость зависит от осознанного управления безопасностью организации.

Основные тенденции в сфере кибербезопасности демонстрируют растущее давление со стороны:

- Появление генеративного искусственного интеллекта (GenAI) в качестве основной технологии
- Сохраняющийся разрыв между безопасностью-предложением талантов и спросом
- Неуклонный рост популярности облачных технологий, который меняет состав цифровых экосистем
- Усиление нормативных обязательств и государственного надзора за кибербезопасностью, конфиденциальностью и локализацией данных
- Продолжающаяся децентрализация цифровых возможностей между предприятиями
- Задача управления рисками безопасности в постоянно меняющейся среде угроз

Руководители служб кибербезопасности работают над тем, чтобы сделать свои подразделения более гибкими и оперативными, опираясь на девять принципов.

В ответ на это руководители служб кибербезопасности работают над тем, чтобы сделать свои подразделения более гибкими и оперативными. Их действия и приоритеты сосредоточены на практиках, технических возможностях и структурных реформах, каждая из которых помогает руководителям служб кибербезопасности достичь двух целей:

- Организационная устойчивость для привлечения инвестиций в безопасность в условиях продолжающегося расширения цифровых экосистем (например, более широкого внедрения облачных технологий, гибридного формата работы и меняющейся среды угроз)
- Повышение эффективности функций кибербезопасности за счет использования возможностей GenAI, уделения приоритетного внимания программам обеспечения безопасности и корпоративной культуре, а также внедрения показателей, ориентированных на результат (ODM), для облегчения принятия решений

Сохраняющаяся повышенная угроза, переход в облако и нехватка квалифицированных кадров выводят безопасность на первое место в списке приоритетов и вынуждают директоров по информационной безопасности (CISO) увеличивать расходы на безопасность в своих организациях. Кроме того, организации в настоящее время оценивают свои потребности в платформе защиты конечных устройств (EPP) и обнаружении и реагировании на угрозы конечных устройств (EDR) и вносят коррективы, чтобы повысить свою операционную устойчивость и скорость реагирования на инциденты после сбоя CrowdStrike.

Внедрение ИИ и генеративного ИИ (GenAI) продолжает увеличивать инвестиции в такие рынки программного обеспечения для обеспечения безопасности, как безопасность приложений, защита данных и конфиденциальность, а также защита инфраструктуры. К 2025 году GenAI приведёт к резкому увеличению ресурсов кибербезопасности, необходимых для его защиты, что приведёт к ожидаемому увеличению расходов на программное обеспечение для обеспечения безопасности на 15%.

С момента выпуска GenAI злоумышленники всё чаще используют инструменты вместе с большими языковыми моделями (LLM) для проведения масштабных атак с использованием социальной инженерии. По

прогнозам к 2027 году 17% всех кибератак и утечек данных будут связаны с генеративным ИИ.

По мере того, как организации продолжают переходить в облако, аналитики Gartner ожидают роста популярности решений для облачной безопасности, а доля облачных решений на рынке будет увеличиваться. В 2025 году совокупный рынок брокеров безопасности доступа к облаку (CASB) и платформ защиты рабочих нагрузок в облаке (CWPP) достигнет 8,7 млрд долларов по сравнению с прогнозируемыми 6,7 млрд долларов в 2024 году.

Глобальная нехватка квалифицированных кадров в сфере кибербезопасности является основным фактором, стимулирующим инвестиции в рынок услуг по обеспечению безопасности (консультационные услуги по обеспечению безопасности, профессиональные услуги по обеспечению безопасности и управляемые услуги по обеспечению безопасности), который, как ожидается, будет расти быстрее, чем другие сегменты безопасности.

Основными стратегическими технологическими тенденциями на 2025 год являются:

1. **Риски, связанные с нечеловеческими личностями в IAM**

Управление «идентификационными данными, не принадлежащими человеку» (например, автоматизированными программами) необходимо для предотвращения угроз безопасности.

В настоящее время директора по информационной безопасности и руководители компаний сосредоточены на повышении устойчивости своих систем и устранении основных уязвимостей в системе безопасности. Ключевой проблемой сейчас является управление «идентификационными данными, не принадлежащими человеку», такими как системные учётные записи и автоматизированные программы, поскольку они могут стать мишенью для угроз безопасности.

Таким образом, управление идентификацией и доступом (IAM), которое когда-то считалось просто ИТ-задачей, теперь становится необходимым для всех команд и требует внимания высшего руководства. Этот сдвиг свидетельствует о более широком понимании роли IAM, которая превратилась из простой меры безопасности клиентов в операционную необходимость.

2. **Рост числа Центров противодействия кибермошенничеству**

Количество центров по борьбе с кибермошенничеством растёт, особенно в таких отраслях с большим количеством транзакций, как банковское дело и электронная коммерция.

Ещё одна тенденция в сфере кибербезопасности на 2025 год — рост числа центров по борьбе с кибермошенничеством, специализированных центров по обеспечению безопасности, которые объединяют экспертов, методы и инструменты для обеспечения безопасности и предотвращения мошенничества.

Эти центры являются важным шагом на пути к современной киберзащите, особенно для отраслей, в которых проводится множество онлайн-транзакций, таких как электронная коммерция, банковское дело, финансовые технологии, игры и другие. Хотя это не совсем новая концепция, она недавно набрала обороты. Считается, что 2025 год будет годом, когда центры по борьбе с кибермошенничеством станут повсеместными, и мы рады, что они станут нормой.

3. **Увеличение числа угроз, основанных на искусственном интеллекте**

Растёт число фишинговых и инъекционных атак с использованием ИИ, которые автоматизируют более сложные атаки. По мере того, как ИИ будет играть ключевую роль в операциях, фишинг и атаки с внедрением команд на основе ИИ будут представлять новые риски. Злоумышленники будут использовать автоматизированные процессы, чтобы вводить в заблуждение системы или пользователей, что приведёт к большей зависимости от инструментов ИИ при проведении комплексной проверки. Кроме того, кража личных данных в цифровом пространстве достигнет рекордного уровня, и компаниям будет сложно отличить подлинные личные данные от сгенерированных искусственным интеллектом, что потребует применения передовых методов проверки личности.

4. **Управление облачной безопасностью с помощью единой панели управления**

Единая панель управления облачной безопасностью позволяет быстрее обнаруживать угрозы и реагировать на них во всех приложениях.

Наличие единой панели мониторинга для отслеживания необычной активности в облачных системах, приложениях и рабочих нагрузках помогает командам по обеспечению безопасности в облаке быстрее и эффективнее

выявлять атаки и реагировать на них. Такая настройка дает им мощный инструмент для сокращения времени, необходимого организациям для решения проблем. Потребность настолько велика, что поставщики упростят для своих клиентов выбор места размещения панели управления».

5. **Сосредоточьтесь на безопасности производства и цепочки поставок**

Цепочки поставок уязвимы для атак третьих лиц, что требует более строгой кибербезопасности для взаимосвязанных сетей. Целостность цепочек поставок становится важнейшим трендом на рынке кибербезопасности. Недавние громкие утечки данных выявили уязвимости у сторонних поставщиков, что подчеркивает необходимость для организаций уделять внимание всем своим цепочкам поставок.

Взаимосвязь современных бизнес-экосистем с устаревшими системами означает, что один скомпрометированный поставщик может поставить под угрозу безопасность всей организации, что может иметь серьёзные последствия для потребителей и экономики в целом.

Чтобы устранить эти риски, компаниям, работающим в сфере производства и цепочек поставок, необходимо следовать передовым методам обеспечения кибербезопасности, устанавливать строгие правила для управления рисками, связанными с третьими сторонами, проводить регулярные проверки безопасности и следить за тем, чтобы все партнёры соблюдали строгие стандарты кибербезопасности.

6. **Продолжающееся использование искусственного интеллекта киберпреступниками**

Киберпреступники используют ИИ для создания сложных угроз, в том числе вредоносных программ, созданных с помощью ИИ, и дипфейков. Киберугрозы, основанные на искусственном интеллекте, становятся всё более изощрёнными и частыми, и в 2025 году киберпреступники продолжат использовать искусственный интеллект для создания новых и более сложных методов атак. Вредоносное ПО, созданное искусственным интеллектом, будет быстро развиваться, бросая вызов традиционным методам обнаружения и требуя столь же сложных средств защиты.

Киберпреступники также могут использовать технологию дипфейков, чтобы выдавать себя за руководителей компаний, что приведёт к росту числа случаев мошенничества в бизнесе и значительным финансовым потерям.

Достижения в области искусственного интеллекта для дипфейков также могут подорвать системы многофакторной аутентификации, которые полагаются на биометрические данные, ставя под угрозу важнейший уровень безопасности.

7. **Рост числа автономных облачных атак**

Злоумышленники всё чаще используют автоматизацию для масштабирования облачных атак, быстро собирая данные и учётные данные. Облачные атаки уже стали более быстрыми, и одна из современных тенденций в сфере кибербезопасности заключается в том, что злоумышленники всё чаще используют автоматизацию и искусственный интеллект. В 2025 году злоумышленники, скорее всего, продолжат использовать готовые инструменты с открытым исходным кодом, чтобы сделать свои атаки более успешными.

Благодаря инструментам, которые автономно выполняют задачи, которые раньше требовали больших усилий и участия человека, облачные атаки в 2025 году будут продолжаться, чтобы собирать больше данных или учётных данных и зарабатывать больше денег за считаные минуты с минимальными усилиями со стороны человека.

8. **Сокращение объемов операций по разборке и захвату**

Киберпреступники переходят к долгосрочным и дорогостоящим атакам, нацеленным на крупные корпорации и цепочки поставок.

Атаки по возможности и «лёгкие» цели по-прежнему будут оставаться мишенями, но злоумышленники начинают и будут продолжать признавать, что их вознаграждение будет больше и лучше, если они будут играть вдолгую.

Мы увидим, как более опытные злоумышленники будут атаковать более крупные корпорации или использовать небольшие взломы в качестве трамплина для проникновения в более известные организации, которые могут нанести больший ущерб всей цепочке поставок.

Киберпреступники будут нацеливаться на часто упускаемые из виду отрасли, которые не уделяют внимания безопасности, например, на производство бензина, строительство, сельское хозяйство.

9. **Ужесточение регулирования облачной безопасности**

Регулирующие органы устанавливают более строгие стандарты облачной безопасности из-за растущего использования облачных технологий и связанных с этим рисков. Регулирующие органы по всему миру признают широкое распространение облачных сервисов и растущие угрозы со стороны хакеров.

Некоторые громкие облачные взломы показали, что слишком многие организации (как частные, так и государственные) имеют очень слабую защиту в облаке. Они страдают от плохой облачной гигиены и недостаточных механизмов безопасности, особенно от обнаружения сложных облачных атак в режиме реального времени.

В результате регулирующие органы установят более строгие правила и заставят организации быстро усилить свою безопасность и лучше защищать данные пользователей и клиентов.

10. **Возросшая роль генеративного искусственного интеллекта**

Генеративный искусственный интеллект интегрируется в центры управления безопасностью, чтобы помогать людям в выполнении задач, а не заменять их. Ещё одна кибертенденция, которую мы увидим в 2025 году, заключается в том, что генеративный искусственный интеллект будет играть более важную роль в операциях по обеспечению кибербезопасности.

Основное внимание будет уделяться интеграции GenAI в центры управления безопасностью для расширения возможностей человека, а не для полной автоматизации его задач. Это соответствует тому, как организации в настоящее время внедряют ИИ, начиная с конкретных, наиболее важных сценариев использования в сфере безопасности.

11. **Развитие архитектуры нулевого доверия**

Модель «Никому не доверяй» расширяется, устраняя неявное доверие и постоянно проверяя всех пользователей и устройства. В эпоху, когда киберугрозы — это не вопрос «если», а вопрос «когда», и организации действуют по принципу «предполагай взлом», внедрение принципа нулевого доверия будет продолжаться. Модель нулевого доверия устраняет неявное доверие, которое предоставлялось пользователям и устройствам в устаревшей модели «замок и ров», и вместо этого основывается на принципе «никогда не доверяй, всегда проверяй. В рамках этой модели устройства и пользователи постоянно проходят аутентификацию и авторизацию.

12. **Уязвимости в документах, не поддающихся машинному чтению**

Старые рукописные и нецифровые документы уязвимы. Они становятся новой высокотехнологичной угрозой безопасности, создавая возможности для мошенничества и утечки данных.

Сегодня системы обнаружения мошенничества используют машиночитаемые данные, но многие документы, особенно написанные от руки, не могут быть прочитаны машинами. Это даёт хакерам возможность использовать такие документы, чтобы избежать обнаружения.

Если в 2025 году предприятия и государственные учреждения не перейдут на машиночитаемые форматы для таких документов, то неэтичные практики, такие как подделка подписей на финансовых документах или оценочных отчётах, будут только набирать обороты.

13. **Замена SIM-карты в качестве новой программы-вымогателя**

Подмена SIM-карты становится серьёзной угрозой, позволяющей обойти многофакторную аутентификацию и получить несанкционированный доступ к учётным записям пользователей.

Подмена SIM-карты станет новой программой-вымогателем в 2025 году. Мобильные устройства, которые и так важны для удаленной работы, также помогают обеспечить безопасность пользователей в Интернете из-за более широкого использования многофакторной аутентификации (MFA).

Однако подмена SIM-карты представляет собой прямую угрозу для многофакторной аутентификации. При использовании этого метода злоумышленник перенаправляет телефонный номер на другую SIM-карту, крадя токен двухфакторной аутентификации пользователя.

Это не только ставит под угрозу цифровые идентификаторы и личную информацию пользователя, но и представляет значительную опасность для организаций, поскольку позволяет получить несанкционированный доступ к корпоративным сетям, добавляет Раймер. Подмена SIM-карты — это мобильный эквивалент фишинга, и ожидается, что в 2025 году он станет более распространённым.

Агентский ИИ

Агентские ИИ-системы автономно планируют и выполняют действия для достижения поставленных пользователем целей. Агентский ИИ позволяет

создать виртуальную рабочую силу, которая может выполнять работу человека и дополнять его. По прогнозам Gartner, к 2028 году не менее 15% повседневных рабочих решений будут приниматься автономно с помощью агентского ИИ, по сравнению с 0% в 2024 году. Целенаправленные возможности этой технологии позволят создавать более адаптируемые программные системы, способные выполнять широкий спектр задач.

Агентский ИИ может помочь ИТ-директорам повысить производительность во всей организации. Эта мотивация побуждает как предприятия, так и поставщиков исследовать, внедрять инновации и создавать технологии и методы, необходимые для надёжного, безопасного и заслуживающего доверия агентского ИИ.

Платформы управления ИИ

Платформы управления ИИ являются частью развивающейся системы управления доверием, рисками и безопасностью ИИ (TRiSM) от Gartner, которая позволяет организациям управлять юридической, этической и операционной эффективностью своих систем ИИ. Эти технологические решения позволяют создавать, управлять и применять политики ответственного использования ИИ, объяснять, как работают системы ИИ, и обеспечивать прозрачность для укрепления доверия и подотчётности. По прогнозам к 2028 году в организациях, внедривших комплексные платформы управления ИИ, на 40% меньше инцидентов, связанных с этическими проблемами ИИ, по сравнению с организациями без таких систем.

Защита от дезинформации

Защита от дезинформации — это новая категория технологий, которая систематически выявляет недостоверную информацию и направлена на создание методологических систем для обеспечения целостности, оценки подлинности, предотвращения выдачи себя за другого человека и отслеживания распространения вредоносной информации. По прогнозам Gartner, к 2028 году 50% предприятий начнут внедрять продукты, услуги или функции, разработанные специально для защиты от дезинформации, по сравнению с менее чем 5% сегодня.

Ожидается, что широкое распространение и усовершенствованное состояние инструментов искусственного интеллекта и машинного обучения, используемых в неблаговидных целях, приведут к увеличению числа случаев дезинформации, нацеленной на предприятия. Если это не остановить,

дезинформация может нанести значительный и долгосрочный ущерб любой организации.

Постквантовая криптография

Постквантовая криптография обеспечивает защиту данных, устойчивую к рискам расшифровки с помощью квантовых вычислений. По мере развития квантовых вычислений за последние несколько лет ожидается, что некоторые широко используемые виды традиционной криптографии перестанут существовать. Переключиться на другие методы криптографии непросто, поэтому организациям требуется больше времени, чтобы подготовиться к надёжной защите конфиденциальных данных.

По прогнозам к 2029 году достижения в области квантовых вычислений сделают большинство традиционных методов асимметричной криптографии небезопасными для использования.

Окружающий невидимый интеллект

Окружающий невидимый интеллект обеспечивается сверхдешёвыми, небольшими интеллектуальными метками и датчиками, которые обеспечивают крупномасштабное доступное отслеживание и распознавание. В долгосрочной перспективе окружающий невидимый интеллект позволит глубже интегрировать распознавание и интеллект в повседневную жизнь.

В 2027 году первые примеры «окружающего» невидимого интеллекта будут направлены на решение насущных проблем, таких как проверка запасов в розничной торговле или логистика скоропортящихся товаров, позволяя недорого отслеживать и распознавать товары в режиме реального времени для повышения прозрачности и эффективности.

Энергоэффективные вычисления

в сфере ИТ влияют на экологичность во многих аспектах, и в 2024 году для большинства ИТ-организаций главным фактором является их углеродный след. Приложения, интенсивно использующие вычислительные ресурсы, такие как обучение ИИ, моделирование, оптимизация и рендеринг мультимедиа, вероятно, вносят наибольший вклад в углеродный след организаций, поскольку потребляют больше всего энергии.

Ожидается, что начиная с конца 2020-х годов для задач специального назначения, таких как искусственный интеллект и оптимизация, появятся

несколько новых вычислительных технологий, таких как оптические, нейроморфные и новые ускорители, которые будут потреблять значительно меньше энергии.

Гибридные вычисления

продолжают появляться новые парадигмы вычислений, в том числе центральные процессоры, графические процессоры, периферийные, специализированные интегральные схемы, нейроморфные и классические квантовые, оптические парадигмы вычислений. Гибридные вычисления сочетают в себе различные вычислительные, запоминающие и сетевые механизмы для решения вычислительных задач. Эта форма вычислений помогает организациям исследовать и решать проблемы, что позволяет технологиям, таким как искусственный интеллект, выходить за рамки текущих технологических ограничений. Гибридные вычисления будут использоваться для создания высокоэффективных инновационных сред, которые будут работать эффективнее, чем обычные среды.

Пространственные вычисления

Пространственные вычисления в цифровом формате расширяют возможности физического мира с помощью таких технологий, как дополненная и виртуальная реальность. Это следующий уровень взаимодействия между физическим и виртуальным опытом. Использование пространственных вычислений повысит эффективность организаций в ближайшие пять-семь лет за счёт оптимизации рабочих процессов и улучшения взаимодействия. По прогнозам , к 2033 году объём рынка пространственных вычислений вырастет до 1,7 триллиона долларов по сравнению со 110 миллиардами долларов в 2023 году.

Многофункциональные роботы

Многофункциональные машины способны выполнять несколько задач и заменяют специализированных роботов, которые предназначены для многократного выполнения одной задачи. Функциональность этих новых роботов повышает эффективность и обеспечивает более быструю окупаемость инвестиций. Многофункциональные роботы предназначены для работы в мире, где есть люди, что обеспечивает быстрое внедрение и лёгкую масштабируемость.

По прогнозам, к 2030 году 80% людей будут ежедневно взаимодействовать с умными роботами, в то время как сегодня этот показатель составляет менее 10%.

Неврологическое усовершенствование

Неврологическое усовершенствование улучшает когнитивные способности человека с помощью технологий, которые считывают и расшифровывают мозговую активность. Эта технология считывает мозговую активность человека с помощью однонаправленных интерфейсов «мозг-машина» или двунаправленных интерфейсов «мозг-машина» (BBMI). Она обладает огромным потенциалом в трёх основных областях: повышение квалификации людей, маркетинг нового поколения и производительность. Неврологическое усовершенствование улучшит когнитивные способности, позволит брендам узнавать, о чём думают и что чувствуют потребители, и расширит нейронные возможности человека для оптимизации результатов.

Полное представление о киберугрозах подлежит корректировке

Сообщества специалистов по кибербезопасности и кибербразведке будут испытывать серьёзные трудности из-за политизации и связанных с ней факторов. Последние несколько лет продемонстрировали относительно единодушную поддержку со стороны сообщества специалистов по кибербезопасности из частного сектора. Повышенное внимание к кибервойнам (в частности, к инструментам уничтожения данных) привели к довольно либеральной политической обстановке в отрасли, и несколько крупных поставщиков открыто заявляли о своей поддержке определённой группы и позиции. Недавние процессы вернули большинство поставщиков средств кибербезопасности к более нейтральной позиции.

Этот сдвиг, вероятно, ускорится и расширится там, где уже звучат заявления о «вооружённых» сообществах кибербразведчиков, а также из-за того, что руководители многих крупных технологических компаний становятся крупными политическими игроками. Кроме того, политические игроки высокого уровня потенциально ставят под сомнение всю систему разведки, в которую входит и кибербразведка.

Эти изменения приведут к значительной путанице, разногласиям и изменениям в том, как поставщики услуг кибербезопасности публикуют свои работы, а также в готовности ключевых руководителей занимать определённую позицию по любым темам, связанным с геополитикой.

Культура киберпреступности уже не та, что была раньше

Культура киберпреступности и вымогательства уже не та, что раньше. В то время как традиционные мотивы — например, корыстные преступления и спонсируемый государством шпионаж — продолжают существовать, новое поколение участников этой культуры оказывается движущей силой многих наиболее разрушительных атак.

Кибератаки, вымогательство и связанное с ними насилие в реальном мире распространяются в тех областях этой новой культуры, о которых ещё несколько лет назад никто и не подозревал. Жертвам теперь приходится беспокоиться о постоянном ущербе для репутации, который наносится новыми способами. Один из примеров — стремительный рост популярности мем-монет, связанных с программами-вымогателями и случаями вымогательства.

‘Мем-монета’, связанная с программой-вымогателем HellCat

Последствия физические для жертв киберпреступлений также будут усугубляться. В 2024 году мы стали свидетелями нескольких поразительных примеров такого рода атак в виде Snowflake и участия в них злоумышленников, связанных с The Com. Эта культура вымогательства и киберпреступности изобилует технически подкованными злоумышленниками, которые стремятся обойти традиционные методы реагирования и противодействия, основанные на социальной инженерии и доставке вредоносного ПО. Эти злоумышленники непредсказуемы и технически подготовлены, они способны использовать в своих целях передовые инструменты и методы.

В 2025 году это станет ещё более заметным по мере распространения этой культуры, а новый профиль злоумышленников продолжит бросать вызов существующим основам кибербезопасности и анализа угроз.

ИИ

Стремительный рост популярности ИИ в технологическом сообществе привёл к тому, что практически каждая компания, занимающаяся кибербезопасностью, и политическое объединение начали изучать ИИ и его потенциальные возможности. Кроме того, несколько известных групп, представляющих угрозу, и киберпреступники проводят исследования и испытания ИИ. Наконец, существует множество неизвестных аспектов ИИ,

что создаёт атмосферу неопределённости, разногласий, а иногда и ошибочных представлений.

Эти факторы создадут среду, в которой политики, знаменитости, технологические компании и ряд других организаций будут пытаться скрыть ошибки/скандалы/преступления/что угодно, утверждая, что во всём виноват ИИ. В число упомянутых случаев, скорее всего, попадут некоторые реальные ситуации, в которых ИИ сыграл свою роль, но не большинство. Это создаст дополнительную путаницу и недоверие к ИИ, что, в свою очередь, усугубит существующую путаницу и разногласия.

Повышенная нацеленность на плохо отслеживаемые и понятные технологии

В 2025 году злоумышленники будут всё чаще использовать технологии, которые одновременно широко распространены и плохо защищены, что позволит им избегать обнаружения и действовать относительно безнаказанно. Эта тенденция затронет периферийные сетевые устройства, такие как брандмауэры, маршрутизаторы и коммутаторы — критически важные компоненты современной инфраструктуры, которым часто не хватает надёжного мониторинга или современных средств защиты. Кроме того, широкое распространение мобильных устройств, таких как iPhone и смарт-часы, которые редко блокируются или тщательно отслеживаются на предмет подозрительной активности, сделает их основными целями.

Эти уязвимые места будут использоваться целым рядом злоумышленников, в том числе поставщиками шпионского ПО из частного сектора, APT-группами национальных государств, террористическими организациями и киберпреступниками, преследующими финансовые цели. Использование таких недостаточно контролируемых технологий позволит злоумышленникам взламывать сети, отслеживать ценных пользователей и обходить защитников, ограниченных присущими этим системам недостатками. В результате защитники должны пересмотреть стратегии борьбы с этими новыми угрозами, сократив разрыв между видимостью и защитой, прежде чем злоумышленники воспользуются этими уязвимостями.

Злоумышленники, нацелившиеся на облако, переключат внимание на взлом и монетизацию сервисов ИИ

Большая часть современных облачных угроз исходит от злоумышленников, преследующих финансовые цели. Они устанавливают майнеры для добычи криптовалюты или крадут ключи API, чтобы использовать сервисы жертвы

для таких атак, как рассылка спама. В большинстве случаев эти выплаты относительно невелики, и зачастую их инициируют злоумышленники из развивающихся стран, где минимальная финансовая выгода оправдывает затраченные усилия.

Феноменальный рост популярности ИИ — это тема, о которой многие устали слышать, но очевидно, что ИИ оказал огромное влияние на мир и на то, как работают компании. Компании быстро создают команды для интеграции ИИ в свои продукты, чтобы повысить эффективность, качество обслуживания клиентов и общие возможности. По мере роста спроса на ИИ и его внедрения большинство этих организаций будут переходить на облачные решения на основе ИИ. Эти предложения гораздо быстрее интегрируются, чем создание собственного решения на основе ИИ: они более экономичны, не требуют специализированного оборудования, обладают более высокой доступностью и часто предоставляют функции предварительно обученных моделей, которые в противном случае потребовали бы значительных инвестиций.

Как и в случае с любым крупным технологическим прорывом — например, с мобильными или облачными вычислениями, — злоумышленники найдут способы использовать эту новую уязвимость. В 2024 году мы видели, как злоумышленники использовали ИИ для улучшения своих инструментов. Возможно, более показательным был отчёт, в котором злоумышленники захватили облачные сервисы ИИ и использовали LLM и инфраструктуру жертвы для осуществления незаконной деятельности. В результате этой атаки появилось приложение LLM, которое обеспечивало взаимодействие, не соответствующее обычным средствам защиты, встроенным в сервис. Облачная учётная запись жертвы оплатила вычислительные ресурсы и токены злоумышленника.

Эта атака, скорее всего, послужит образцом для других действий по захвату облачных сервисов ИИ в 2025 году. Сфера применения, несомненно, расширится за пределы больших языковых моделей и охватит другие инструменты ИИ, такие как генераторы изображений и видео. В конечном счёте компаниям следует оценить типы приложений на базе ИИ, которые они используют, и то, как злоумышленники могут использовать их в своих целях или для получения прибыли, причём последнее, вероятно, будет происходить всё чаще.

Облачные приложения с искусственным интеллектом стоят дорого, и расходы увеличиваются по мере усложнения проекта. В 2024 году злоумышленники продавали ключи API для облачных сервисов и сервисов ИИ на основе SaaS. В 2025 году ожидается рост спроса на монетизацию взломанных ИИ и облачных ресурсов.

В 2025 году Mac может стать ахиллесовой пятой организаций

Одна из часто упоминаемых причин возросшей популярности компьютеров Mac в организациях — их предполагаемая «более высокая безопасность». Хотя утверждение «на Mac не бывает вредоносных программ» было в достаточной мере опровергнуто реальностью, по-прежнему бытует мнение, что «они безопаснее остальных». Злоумышленники не разделяют это мнение, но оно является естественным выводом для пользователей, уставших от ужасной репутации Windows в плане безопасности и столкнувшихся с экспоненциально растущим количеством вредоносных программ, нацеленных на платформу Microsoft.

Восприятие может быть опасным, особенно когда организации распределяют ограниченные ресурсы. Стоит задуматься о том, что в 2024 году наблюдался заметный рост числа вредоносных программ, ориентированных на macOS, в частности, программ-вымогателей, таких как Amos Atomic, Banshee Stealer, Cuckoo Stealer, Poseidon и другие. Эти программы-вымогатели не требуют постоянного подключения и стремятся украсть всё за один взлом, включая учётные данные для онлайн-аккаунтов и облачных хранилищ.

Для этого они используют простую, но эффективную формулу: поскольку один и тот же пароль используется для входа в систему, установки программного обеспечения и разблокировки Keychain — базы данных, в которой хранятся все остальные пароли в macOS, — просто запросите у пользователя пароль для установки какого-либо программного обеспечения. Любое вредоносное ПО, которое успешно подменяет диалоговое окно ввода пароля «для установки» поддельной программы, сразу же получает ключи от королевства. На помощь злоумышленникам приходит встроенный AppleScript, который делает подделку диалогового окна ввода пароля тривиальной задачей.

Ни «универсальный пароль», ни диалоговое окно с паролем, который легко подделать, не поддаются быстрому исправлению. Это технологии, которые были встроены в операционную систему с самого начала; не стоит ожидать, что Apple исправит их в ближайшее время. Следовательно, мы ожидаем, что авторы вредоносных программ будут продолжать злоупотреблять ими в течение 2025 года.

Две ключевые стратегии защиты для организаций:

- Внедрите менеджеры паролей и научите пользователей не использовать встроенное в Apple приложение «Пароли» и «Связку ключей» для хранения корпоративных учётных данных.

- Установите надёжное решение для обеспечения безопасности, чтобы устранить многочисленные пробелы в правилах защиты от вредоносных программ XProtect, которые Apple обновляет нечасто.

В отличие от тех, кто крадёт информацию методом «бей и беги», более целенаправленные злоумышленники, преследующие цели на уровне государства, такие как шпионаж, по-прежнему заинтересованы в том, чтобы оставаться незамеченными. Мы видели, как они изучали различные способы закрепиться на скомпрометированном устройстве с тех пор, как Apple ввела уведомления пользователей о фоновых входах в систему в Ventura. Троянские программы, часто запускаемые приложения, заражение сред разработки, таких как Visual Studio и Xcode, или использование забытых сред командной строки Unix, таких как zshenv и zshrc, — все эти методы можно встретить в дикой природе.

Содержимое вредоносного файла ~/.zshenv, выполняемого для каждого сеанса Zsh

Вредоносный файл ~/.zshenv, используемый BlueNoroff

Пожалуй, самое распространённое поведение на любом устройстве — это поведение самого пользователя; следовательно, компрометирующее программное обеспечение, которое, как известно, пользователь применяет или должен использовать, скорее всего, станет фаворитом в наступающем году. Внимательно следите за приложениями для повышения производительности, которые используются в организации, а также за интегрированными средами разработки и другими инструментами. Для защитников это означает, что «списки разрешений» или «исключения» из вашей политики безопасности — это слабое место, которое требует тщательного контроля (т. е. сведения к минимуму) и постоянной бдительности. Если ваша организация что-то разрешает, потому что блокировать это слишком неудобно, подумайте, что ещё можно сделать, чтобы снизить вероятность злоупотребления этим процессом (например, регулярная проверка версий, мониторинг аномального создания процессов или сетевого трафика).

Прежде всего, несмотря на распространённое мнение, важно помнить, что компьютеры Mac не более «безопасны по своей природе», чем любое другое вычислительное устройство. Они могут быть скомпрометированы и регулярно подвергаются взлому, и их необходимо учитывать в общей стратегии безопасности организации как основную цель для злоумышленников.

Нормализация и таргетинг зашифрованных служб связи

Растущая распространённость спонсируемых государством вторжений, особенно со стороны таких групп, как «Солёный тайфун» из Китая, проникающих в западные телекоммуникационные сети, привлечёт внимание широкой общественности к зашифрованным сервисам связи, таким как Signal и ProtonMail.

По мере роста обеспокоенности по поводу конфиденциальности и слежки всё более широкий сегмент пользователей, не обладающих техническими знаниями, будет отдавать предпочтение безопасным платформам для обмена сообщениями и электронной почте, чтобы защитить личные сообщения от внутреннего и внешнего мониторинга. Этот сдвиг будет и дальше усиливаться под влиянием СМИ, государственной политики и стратегического направления новой администрации Белого дома.

По мере того, как зашифрованные сервисы будут получать всё более широкое распространение, они также будут привлекать повышенное внимание киберпреступников и государственных структур. Угрозы будут развиваться и включать в себя перехват или кражу зашифрованных данных во время передачи, использование уязвимостей в этих платформах и злоупотребление инструментами безопасной связи в рамках вредоносных кампаний.

Эта двойственная динамика — публичное использование шифрования для обеспечения конфиденциальности и его использование злоумышленниками — сделает зашифрованные сервисы связи одновременно критически важной защитой и ценной целью в 2025 году.

Программа-вымогатель не умирает, как и Ваши данные

Сейчас существует больше организованных операций с использованием программ-вымогателей, чем когда-либо прежде. Инструменты совершенствуются, а и без того минимальные барьеры для проникновения продолжают снижаться. Кроме того, мощные платформы и инструменты для программ-вымогателей, такие как LockBit и ALPHV, широко распространяются и попадают в руки злоумышленников. Злоумышленники с более низким уровнем квалификации используют эти инструменты в рамках своих стандартных операций, даже если конечной целью не является получение финансовой выгоды, а известные инструменты для программ-вымогателей получили новую жизнь благодаря растущему использованию в сообществах хактивистов. Программы-вымогатели теперь являются общедоступным инструментом, которым могут пользоваться

злоумышленники с разными возможностями и мотивами, и так будет продолжаться до 2025 года.

CyberVolk ransomware

Кроме того, такие злоумышленники, как Dispossessor и RansomHub, монетизировали данные даже после того, как жертва выполнила их требования. Плата злоумышленнику, использующему программы-вымогатели, в обмен на обещание удалить данные — это уловка. Компрометированные данные продолжают существовать благодаря мошенникам-аффилированным лицам и сообществам, которые распространяют данные о взломах среди злоумышленников. У взломанных данных нет срока годности, и эти злоумышленники не соблюдают «контракты». Защита данных и предотвращение этих атак на ранних этапах в 2025 году будут иметь решающее значение как никогда.

Безопасность и управление рисками

В 2025 году в сфере кибербезопасности произойдут тектонические сдвиги, каких мы не видели в прошлые годы. Эти исторические преобразования приведут к объединению искусственного интеллекта, данных и платформ, что в целом изменит методы работы и внедрения инноваций как для защитников кибербезопасности, так и для злоумышленников. Подобные сдвиги не будут просто серией отдельных достижений. Они приведут к переосмыслению того, что означает безопасность в мире, который становится всё более цифровым, и, несомненно, заставят компании пересмотреть фундаментальные стратегии. Организации должны быть внимательными и осмотрительными при подготовке к этим изменениям. Эти прогнозы служат предвестниками будущего, в котором унифицированные платформы безопасности, прозрачный искусственный интеллект и межфункциональные альянсы не только выгодны, но и необходимы для долгосрочной устойчивости и доверия.

Традиционные разрозненные системы кибербезопасности больше не могут справляться с изощрёнными и частыми современными угрозами. В связи с этим компаниям необходимо перейти к единой унифицированной платформе для защиты данных. Этот переход к платформенной архитектуре обеспечит не только эффективность, но и комплексную защиту, которая адаптируется к меняющимся угрозам и способствует росту бизнеса.

В гонке за превосходством в области ИИ данные являются топливом, которое питает эффективные адаптивные модели. Крупные, авторитетные

организации, уже располагающие огромными массивами данных, имеют значительное преимущество — они могут обучать модели ИИ в больших масштабах, создавая цикл обратной связи, который постоянно укрепляет защиту. Это преимущество будет только расти по мере того, как модели, ориентированные на данные, будут опережать конкурентов, особенно новичков. Однако мы также можем ожидать, что лидеры отрасли будут сотрудничать с новыми стартапами, объединяя обширные массивы данных с инновационными методами. Учитывая это, чтобы ИИ завоевал доверие пользователей, особенно в отсутствие глобальных систем ИИ, организациям необходимо будет демонстрировать прозрачность в том, как модели ИИ принимают решения и управляют данными. Это, несомненно, установит новый стандарт подотчётности и лояльности к бренду во всей отрасли.

Следовательно, по мере увеличения объёма работ, связанных с ИИ, отрасль столкнётся с ещё одной серьёзной проблемой — энергопотреблением. В настоящее время центры обработки данных потребляют около 4% электроэнергии, и, согласно прогнозам, к 2030 году этот показатель может более чем удвоиться. Чтобы устойчиво удовлетворять растущий спрос, компаниям необходимо внедрять энергоэффективные стратегии, в том числе технологии охлаждения на основе ИИ, платформы ИИ на квантовой основе и унифицированные платформы безопасности, которые устраняют избыточные процессы. Чтобы обеспечить рост ИИ в соответствии с требованиями устойчивого будущего, необходимо не только защищать центры обработки данных, но и уделять приоритетное внимание модернизации энергосетей, прокладывая путь к устойчивому миру, управляемому ИИ.

Переход к операциям SOC под управлением ИИ добавляет ещё один важный аспект — доверие. В то время как ИИ будет выполнять основные задачи, такие как сканирование уязвимостей и обнаружение угроз, аналитики-люди сосредоточатся на стратегии высокого уровня и принятии решений. Такой подход подчёркивает необходимость прозрачности в отношении моделей ИИ, сбора данных и процессов принятия решений. По мере ужесточения нормативно-правовой базы во всём мире создание надёжных структур управления (в том числе советов по ИИ) будет иметь решающее значение для соблюдения стандартов и укрепления доверия между клиентами и заинтересованными сторонами.

Будущее квантовых вычислений таит в себе как преобразующий потенциал, так и серьёзные риски. Хотя квантовые атаки на существующие системы шифрования пока невозможны, стремление к квантовому превосходству ускоряется. Противники, поддерживаемые государством, используют стратегию «собирать урожай сейчас, расшифровывать позже» — они собирают зашифрованные данные сейчас, чтобы расшифровать их, когда

квантовые технологии станут более совершенными. Эта надвигающаяся угроза государственным секретам, интеллектуальной собственности и военным коммуникациям повышает ставки для современных организаций. Проактивная устойчивая к квантовым технологиям дорожная карта имеет решающее значение, начиная с внедрения квантово-устойчивых алгоритмов, передовых криптографических библиотек и квантового распределения ключей (QKD). По мере того, как Национальный институт стандартов и технологий (NIST) завершает разработку стандартов постквантовой криптографии, лидеры должны действовать стратегически, сопоставляя возможности квантовых технологий с надёжной защитой конфиденциальных данных, чтобы быть готовыми к миру, в котором используются квантовые технологии.

Внедрение специализированных веб-браузеров корпоративного уровня станет ещё одним дальновидным шагом для организаций в 2025 году. Традиционные потребительские браузеры часто уязвимы для фишинга, вредоносного ПО и утечек данных. Поскольку более 95% организаций сообщают об инцидентах, связанных с безопасностью, которые происходят в браузерах на всех устройствах, компании должны предоставлять сотрудникам безопасные специализированные среды для просмотра веб-страниц. Gartner прогнозирует, что к 2030 году корпоративные браузеры станут основой для обеспечения безопасной цифровой работы, что необходимо для создания устойчивых передовых систем защиты, поддерживающих бесперебойную совместную работу распределённых сотрудников.

По мере того, как данные всё больше влияют как на безопасность, так и на взаимодействие с клиентами, роли ИТ-директора и директора по маркетингу станут более взаимозависимыми. ИТ-директор и директор по маркетингу будут объединять усилия, чтобы использовать данные и искусственный интеллект для безопасного и персонализированного взаимодействия с клиентами. Внимание ИТ-директора к управлению данными и прозрачности ИИ в сочетании с приверженностью директора по маркетингу этичному использованию ИИ во взаимодействии с клиентами будет иметь решающее значение для сохранения доверия и обеспечения соответствия требованиям. Такое сотрудничество позволяет компаниям быть не только лидерами в области безопасности, но и новаторами в области ответственного взаимодействия с клиентами на основе данных.

В конечном счёте, эти изменения указывают на будущее, в котором организации, придерживающиеся единого, прозрачного и совместного подхода, будут задавать тон в сфере кибербезопасности. Для компаний эта трансформация — это не просто обеспечение безопасности, но и повышение устойчивости, укрепление доверия клиентов и получение преимуществ в

быстро развивающемся цифровом мире. В совокупности эти прогнозы подчёркивают новые принципы кибербезопасности — единство платформ, прозрачность данных и стратегическое партнёрство, — которые будут определять успех в 2025 году и далее.

Заключение

Изучив последние тенденции в сфере кибербезопасности и прогнозы экспертов на 2025 год, мы пришли к выводу, что кибербезопасность будет заключаться в опережении всё более сложных угроз с помощью более умных и быстрых технологий.

Поскольку киберпреступники становятся всё более изощрёнными, компании и частные лица должны следить за новыми тенденциями в сфере кибербезопасности, которые появятся в новом году, чтобы защитить свои данные и системы.

По мере развития технологий развиваются и методы, которые киберпреступники используют для их взлома. В 2025 году кибербезопасность будет как никогда важна, поскольку компании, правительства и частные лица столкнутся с новыми проблемами в защите своих данных и систем от новейших угроз кибербезопасности.

Ожидается, что в 2025 году угрозы кибербезопасности будут расти, а атаки с использованием искусственного интеллекта, такие как дипфейки и автоматизированный взлом, станут более изощрёнными. Тенденции будут сосредоточены на усилении защиты от искусственного интеллекта, внедрении компаниями безопасности с нулевым доверием и усилении защиты облачных сред и персональных данных.

От искусственного интеллекта (ИИ) до облачной безопасности — организации вкладывают значительные средства в предотвращение всё более изощрённых кибератак.

Следующим важным шагом в области кибербезопасности, вероятно, станет интеграция искусственного интеллекта и машинного обучения в системы безопасности. Эти технологии позволят быстро анализировать огромные объёмы данных, выявлять закономерности и необычную активность, что упростит обнаружение и предотвращение кибератак.

Стоит обратить внимание вот на эти основные тенденции в сфере кибербезопасности-

- Киберугрозы, основанные на искусственном интеллекте, развиваются, делая атаки более изощрёнными и сложными для обнаружения.
- Управление идентификацией и доступом (IAM) теперь имеет важное значение для всех команд.
- Архитектура нулевого доверия все чаще используется для противодействия растущим угрозам с использованием подхода “никогда не доверяй, всегда проверяй”.
- Центры по борьбе с киберпреступностью становятся критически важными для таких уязвимых отраслей, как финансы и электронная коммерция.
- Облачная безопасность развивается благодаря управлению с помощью одной панели управления.
- Генеративный искусственный интеллект будет играть большую роль в операциях по обеспечению кибербезопасности.

Текущее состояние кибербезопасности и существующий профиль угроз и злоумышленников говорят нам о том, что для решения проблем 2025 года потребуются активные и целенаправленные действия. Что это значит на практике? Основываясь на мнениях аналитиков и экспертов, рекомендуется компаниям при планировании на следующий год сосредоточиться на следующих ключевых областях-

- Повысьте прозрачность и эффективность обнаружения угроз: уделяйте приоритетное внимание мониторингу недостаточно защищенных технологий, таких как периферийные устройства и облачные сервисы ИИ. Инвестируйте в инструменты, которые обеспечивают глубокую аналитику сетевой активности и поведения конечных устройств.
- Укрепляйте сотрудничество: устраняйте разобщённость, обмениваясь информацией об угрозах с коллегами по отрасли и государственными партнёрами. Открытый диалог и сотрудничество необходимы для противодействия коллективным угрозам.
- Укрепляйте нормативно-правовую базу: выступайте за реформы, которые снизят юридические барьеры для обмена информацией, и

привлекайте поставщиков и подрядчиков к ответственности за их роль в экосистеме безопасности.

- Инвестируйте в устойчивость: укрепляйте защиту от программ-вымогателей и кражи данных, обеспечивая безопасность учётных данных, внедряя надёжные планы восстановления и информируя сотрудников о новых способах атак.

- Устраните упущенные из виду уязвимости: пересмотрите свои представления о безопасности — будь то предполагаемая безопасность компьютеров Mac или доверие к встроенным инструментам шифрования — и примите меры по снижению рисков в этих областях.

Дальнейшее развитие требует сильного лидерства, решительных действий и готовности к переменам. Из-за прошлых успехов злоумышленников мы знаем, что компаниям нужна помощь в обеспечении кибербезопасности.

2. НАДЛЕЖАЩАЯ vs. ДОЛЖНАЯ ОСМОТРИТЕЛЬНОСТЬ

Due Care vs Due Diligence

Понимание нюансов между “надлежащей осмотрительностью” и “должной осмотрительностью” важно для эффективного управления рисками, особенно в сложной области кибербезопасности. Хотя оба термина играют ключевую роль в создании надежной системы безопасности для снижения рисков, они существенно различаются по своему применению и направленности. В повседневной жизни эти понятия относятся к общим мерам предосторожности, которые мы принимаем, чтобы избежать вреда. Напротив, в контексте регулирования или соблюдения требований, особенно в области кибербезопасности, они приобретают более специализированное значение и играют различные роли в обеспечении безопасности организации.

Термины “должная и надлежащая осмотрительность“ чрезвычайно важны для управления рисками, но имеют разные значения в зависимости от контекста, в котором они используются. Самое главное, что эти две концепции различаются в зависимости от того, имеете ли вы в виду реальные сценарии или нормативную среду.

В повседневной жизни должная осмотрительность относится к нашим привычкам, политике и процедурам, которые мы используем для обеспечения нашей безопасности и избежания неприятностей. Должная осмотрительность означает, что мы принимаем необходимые меры предосторожности в данной ситуации. Например, мы проводим должную осмотрительность при расследовании обнаруженной потенциальной проблемы.

В условиях регулирования или соблюдения требований Due Diligence по-прежнему означает наличие политик и процедур для защиты вашей организации. Надлежащая осмотрительность, с другой стороны, фокусируется на деятельности сторонних организаций по управлению рисками.

Рассмотрим “должную осмотрительность” в сравнении с “необходимой осмотрительностью” в рамках регулирования и комплаенса в кибербезопасности. Мы также рассмотрим действия, которые можно предпринять, чтобы интегрировать любой из них в общую стратегию управления рисками.

Надлежащая осмотрительность в повседневной жизни относится к привычным действиям, политикам и процедурам, которые мы используем для обеспечения безопасности и избежания рисков. Речь идет о последовательном выполнении правил политики информационной безопасности предприятия. В контексте кибербезопасности это означает постоянные усилия организации по обеспечению безопасности своих данных и систем. Это включает внедрение и поддержание соответствующих мер безопасности, регулярное обновление программного обеспечения для исправления уязвимостей и обеспечение того, чтобы все сотрудники были обучены передовым методам обеспечения безопасности.

Должная осмотрительность, в общем смысле, предполагает принятие необходимых мер, чтобы избежать вреда в конкретной ситуации. Речь идет о выполнении необходимой домашней работы. В сфере кибербезопасности, особенно в рамках нормативной базы, должная осмотрительность относится к комплексному процессу, который организация предпринимает для понимания киберрисков, связанных со сторонними партнерами, поставщиками и приобретениями, и управления ими. Это означает тщательную оценку состояния безопасности этих внешних организаций, постоянный мониторинг их соответствия и обеспечение того, чтобы они соответствовали стандартам кибербезопасности организации.

Обе концепции важны не только в повседневном управлении рисками, но становятся еще более важными в среде регулирования и соблюдения требований, где ставки выше. Должная осмотрительность и должная осмотрительность в кибербезопасности связаны с упреждающими и реактивными мерами. В то время как надлежащая осмотрительность направлена на предотвращение инцидентов безопасности с помощью текущего обслуживания и передовых практик, надлежащая осмотрительность касается следственных действий, предпринимаемых для обеспечения того, чтобы внешние стороны не привносили новые риски в организацию.

В этой главе мы углубляемся в сравнение “должной осмотрительности” и “надлежащей осмотрительности” в области кибербезопасности, особенно через призму нормативно-правовой базы. Мы рассмотрим нюансы каждой концепции, как они взаимодействуют и почему обе необходимы во всеобъемлющей стратегии управления рисками. Кроме того, мы предоставим полезную информацию об интеграции этих принципов в практику кибербезопасности вашей организации, чтобы улучшить вашу оборонительную позицию и обеспечить соответствие требованиям в постоянно меняющейся среде угроз.

Что такое надлежащая осмотрительность в кибербезопасности

Надлежащая осмотрительность относится к усилиям, прилагаемым отдельным лицом или организацией, чтобы избежать причинения вреда другим людям или имуществу. В контексте кибербезопасности и бизнеса, должная осмотрительность - это уровень суждений, внимания и осмотрительности, которые можно было бы разумно ожидать от разумного человека при определенных обстоятельствах. По сути, речь идет о принятии упреждающих мер и внедрении необходимых мер для обеспечения безопасности деятельности организации и соответствия стандарту медицинской помощи, который признан отраслевыми нормами или требованиями законодательства. В кибербезопасности это может включать регулярные обновления протоколов безопасности, постоянное обучение персонала и оперативное реагирование на известные уязвимости.

Вот обновленные и расширенные примеры надлежащей осмотрительности в современном ландшафте кибербезопасности:

- Контролируйте свою сеть и защищайте ее от вредоносной активности

В эпоху постоянно развивающихся киберугроз постоянный мониторинг вашей сети имеет решающее значение. Вы должны убедиться, что ваша служба безопасности оснащена новейшими инструментами и информацией для оперативного обнаружения новых уязвимостей и угроз и реагирования на них. Это включает внедрение передовых систем обнаружения угроз, использование мониторинга безопасности в режиме реального времени и регулярный просмотр журналов доступа.

- Обучите своих сотрудников кибербезопасности осведомленности

Человеческая ошибка остается одной из существенных уязвимостей в кибербезопасности. Проведите всестороннее обучение всех сотрудников, охватывающее такие темы, как фишинг, управление паролями и методы обеспечения безопасности Интернета. Регулярно обновляйте учебные материалы, чтобы отразить последние киберугрозы и гарантировать, что все сотрудники понимают последствия несоблюдения политик компании.

- Применяйте политики, стандарты, исходные данные и процедуры

Разработайте и поддерживайте четкую, всеобъемлющую политику кибербезопасности, которая описывает позицию и практику вашей организации. Это должно основываться на тщательной оценке рисков с учетом конкретных угроз и уязвимостей, имеющих отношение к вашему бизнесу. Регулярно пересматривайте и обновляйте свои политики, чтобы адаптироваться к новым киберрискам и изменениям законодательства. Убедитесь, что все сотрудники осведомлены об этих политиках и понимают свою роль в их соблюдении.

- Создавайте резервные копии критически важной корпоративной информации и данных

Регулярные резервные копии являются краеугольным камнем должной осмотрительности в кибербезопасности. По возможности автоматизируйте процессы резервного копирования, чтобы обеспечить согласованность и надежность. Надежно храните резервные копии как на месте, так и за его пределами, и регулярно тестируйте их, чтобы убедиться в возможности их эффективного восстановления. Рассмотрите возможность использования облачных сервисов для резервирования и убедитесь, что они соответствуют вашим требованиям безопасности.

- Защитита сети Wi-Fi

Сети Wi-Fi являются обычными точками входа для злоумышленников. Обеспечьте безопасность своей сети, используя надежное шифрование (например, WPA3), скрывая SSID сети и регулярно меняя пароли. Контролируйте доступ к сети и отслеживайте ее на предмет несанкционированных устройств или необычной активности. Используйте сегментацию сети для защиты конфиденциальных данных и систем от доступа через сеть Wi-Fi.

- Будьте в курсе событий и соблюдайте нормативные акты

Надлежащая осмотрительность также означает быть в курсе последних правил и стандартов кибербезопасности, актуальных для вашей отрасли. Это включает в себя такие нормативные акты, как GDPR, HIPAA, или отраслевые стандарты, такие как ISO 27001. Убедитесь, что ваши методы работы соответствуют этим правилам, и внедрите процесс постоянного обновления по мере их развития.

- Планирование реагирования на инциденты

Подготовьте план реагирования на инциденты, в котором описывается, как ваша организация будет реагировать на инцидент, связанный с кибербезопасностью. Этот план должен включать шаги по локализации, ликвидации, восстановлению и анализу после инцидента. Регулярно тестируйте и обновляйте план, чтобы убедиться в его эффективности и в том, что весь соответствующий персонал знаком со своими ролями во время инцидента.

Применяя эти методы, организации демонстрируют должную заботу о кибербезопасности, значительно снижая профиль рисков и повышая устойчивость к киберугрозам. Помните, надлежащая осмотрительность - это не разовое усилие, а постоянное стремление поддерживать и улучшать вашу позицию в области кибербезопасности перед лицом динамичного ландшафта угроз.

Что такое должная осмотрительность в кибербезопасности?

С другой стороны, должная осмотрительность - это расследование или проявление осторожности, которые разумное предприятие или физическое лицо должно предпринять перед заключением соглашения или контракта с другой стороной или действием с определенным стандартом осмотрительности. Это более комплексный процесс, который включает в себя исследование и понимание рисков, связанных с деловой активностью или принятием решения. В кибербезопасности под должной осмотрительностью часто понимаются шаги, предпринимаемые для оценки состояния безопасности и практики сторонних поставщиков или партнеров, чтобы

убедиться, что они соответствуют стандартам безопасности организации. Это включает оценку потенциальных рисков кибербезопасности, проверку соответствия поставщика соответствующим стандартам и законам, а также постоянный мониторинг их эффективности и соблюдения согласованных протоколов безопасности.

Вот обновленные методы и рекомендации по проведению Due Diligence в сегодняшней среде кибербезопасности:

Политика вендора управлении рисками

Политика поставщика управления рисками (VRM) имеет решающее значение для определения того, как ваша организация оценивает, отслеживает и снижает риски, связанные со сторонними поставщиками. Эта политика требует следующее:

Документация процессов принятия решений: включайте критерии выбора новых поставщиков, такие как проверка их практики кибербезопасности, сертификаты (например, ISO 27001 или SOC 2) и, возможно, даже проверки биографических данных ключевого персонала.

Описание текущего обслуживания и мониторинга: Подробные процедуры непрерывного мониторинга и периодической переоценки соответствия поставщиков стандартам кибербезопасности. Это может включать регулярные аудиты безопасности, обзоры обновлений системы безопасности и планирование реагирования на инциденты.

Адаптация к возникающим угрозам: Регулярно обновляйте политику, чтобы отразить последние киберугрозы и нормативные требования, гарантируя, что ваша организация и ее поставщики остаются согласованными в своей защите от киберрисков.

Эффективная комплексная проверка требует глубокого понимания потенциальных угроз безопасности, исходящих от сторонних поставщиков.

Ключевые практики включают:

- Базовая оценка безопасности: Проведите тщательную первоначальную оценку безопасности всех поставщиков, чтобы установить базовые показатели для будущего мониторинга. Это должно касаться их политик безопасности, планов реагирования на инциденты, методов обработки данных и любых предыдущих инцидентов безопасности.

- Непрерывный мониторинг: Внедрите системы и процедуры для непрерывного мониторинга состояния безопасности поставщиков. Это может включать регулярные отчеты о безопасности, оповещения в режиме реального времени или инструменты автоматического сканирования.
- Независимые аудиты и тестирование на проникновение: В зависимости от чувствительности задействованных данных и систем рассмотрите возможность проведения независимых аудитов безопасности или тестов на проникновение систем поставщиков или запросите доступ к их последним оценкам безопасности.
- Регулярные аудиты безопасности являются краеугольным камнем должной осмотрительности в области кибербезопасности, помогая выявлять и устранять уязвимости до того, как они могут быть использованы. Эти аудиты должны:

- Изучить широкий спектр факторов: посмотреть на ИТ-системы, конфигурации, технологии, инфраструктуру, методы обработки данных и соблюдение соответствующих нормативных актов.
- Результатом являются практические выводы: Убедитесь, что любые уязвимости или области, требующие улучшения, выявленные в ходе аудитов, были оперативно устранены. Это может включать работу с поставщиком для внесения необходимых изменений или переоценку отношений с поставщиками, если они не могут соответствовать вашим стандартам безопасности. Аудиты проводится квалифицированными профессионалами: Привлекайте опытных аудиторов или компании по кибербезопасности для проведения этих аудитов, обеспечивая тщательную экспертизу.

Обновления, отражающие изменения в законодательстве

Должная осмотрительность в кибербезопасности заключается не только в защите от киберугроз, но и в обеспечении соответствия все более сложной нормативно-правовой базе. Регулярно обновляйте свои методы проведения due diligence в соответствии с законами и нормативными актами, такими как GDPR, HIPAA или CCPA, и отраслевыми стандартами.

Включение фреймворков

Включите в свои процессы due diligence установленные фреймворки кибербезопасности, такие как NIST или ISO 27001. Эти фреймворки предоставляют структурированные методологии для оценки и улучшения

практики кибербезопасности как в вашей организации, так и среди сторонних поставщиков.

Должная осмотрительность в кибербезопасности - это динамичный и критически важный процесс снижения рисков, связанных со сторонними поставщиками и партнерами. Внедряя надежную политику управления рисками поставщиков, постоянно отслеживая позиции сторонних производителей в области безопасности, проводя регулярные аудиты безопасности и оставаясь в курсе изменений нормативных актов, организации могут значительно повысить свою кибербезопасность и продемонстрировать приверженность защите своих данных, систем и репутации.

Важность должной и надлежащей осмотрительности в кибербезопасности

В сложном мире кибербезопасности должная осмотрительность и комплексная проверка - это не просто модные словечки, а фундаментальные принципы, лежащие в основе надежной системы безопасности. Их важность трудно переоценить, поскольку в совокупности они способствуют активному и ответственному подходу к управлению киберрисками и их снижению.

Надлежащая осмотрительность относится к постоянным усилиям, которые организация предпринимает для поддержания и улучшения своих мер кибербезопасности. Речь идет о принятии разумных мер для защиты данных и систем от ущерба, которые включают регулярные обновления протоколов безопасности, непрерывное обучение персонала и оперативное реагирование на известные уязвимости. Практика надлежащей осмотрительности означает, что организация активно работает над соблюдением стандарта безопасности, который признан разумным и достаточным отраслевыми и правовыми стандартами.

С другой стороны, должная осмотрительность - это процесс расследования, который организация предпринимает для понимания рисков кибербезопасности, связанных с внешними партнерами, поставщиками или приобретениями. Речь идет об обеспечении того, чтобы у этих третьих сторон были приняты адекватные меры безопасности, и чтобы их практика соответствовала требованиям и стандартам безопасности вашей организации. Должная осмотрительность имеет решающее значение в контексте цепочки поставок и партнерства, где слабые места в системе безопасности одного предприятия могут привести к уязвимостям по всем направлениям.

Почему они важны

Соблюдение правовых и нормативов: Оба принципа часто требуются различными нормативными актами. Организации, которые не проявляют должной осмотрительности и осмотрительности, могут столкнуться с юридическими последствиями, включая штрафы.

- Репутация и доверие: Клиенты и партнеры доверяют организациям, которые серьезно относятся к кибербезопасности. Должная осмотрительность и осмотрительность являются видимыми признаками приверженности организации защите своих данных и данных ее клиентов.
- Управление рисками: Упреждающее управление рисками с помощью должной осмотрительности и осмотрительности помогает предотвращать инциденты безопасности и снижает последствия, когда они все же происходят. Это крайне важно для минимизации простоев, финансовых потерь и ущерба репутации.
- Принятие стратегических решений: комплексная проверка предоставляет ценную информацию, которая может служить основой для принятия стратегических решений, особенно касающихся слияний, поглощений или вступления в партнерские отношения. Понимание состояния безопасности другой организации помогает оценить риски и выгоды деловых отношений.

Рекомендации по обеспечению должной и надлежащей осмотрительности являются неотъемлемой частью ваших политик безопасности. Внедрение должной осмотрительности и осмотрительности в политику кибербезопасности вашей организации - это не просто лучшая практика; это необходимость в современном ландшафте угроз. Вот как вы можете убедиться, что эти принципы являются неотъемлемой частью ваших стратегий безопасности:

- Установите четкие политики и процедуры: Разработайте и задокументируйте четкие политики, которые определяют приверженность вашей организации должной осмотрительности и должной осмотрительности. Они должны включать рекомендации по регулярным оценкам безопасности, реагированию на инциденты, управлению поставщиками и обучению сотрудников.

- Регулярные оценки рисков: Проводите регулярные и тщательные оценки рисков для выявления потенциальных уязвимостей и определения их приоритетности. Это должен быть непрерывный процесс, адаптирующийся по мере появления новых угроз и изменения обстоятельств вашей организации.
- Непрерывный мониторинг и совершенствование: Внедрите непрерывный мониторинг вашей ИТ-среды для быстрого обнаружения аномалий и потенциальных угроз. Регулярно пересматривайте и обновляйте свои меры безопасности, чтобы убедиться, что они эффективны и соответствуют текущим стандартам.
- Программа управления поставщиками: Разработайте комплексную программу управления поставщиками, которая включает в себя проверки должной осмотрительности перед привлечением новых поставщиков и постоянный мониторинг существующих. Убедитесь, что ваши поставщики придерживаются тех же стандартов безопасности, что и вы.
- Обучение и осведомленность: развивайте культуру безопасности в вашей организации. Регулярно обучайте всех сотрудников новейшим угрозам кибербезопасности и передовым практикам. Убедитесь, что они понимают свою роль в поддержании уровня безопасности организации.
- Осведомленность о правовых и нормативных актах: Будьте в курсе последних законов и нормативных актов в области кибербезопасности, которые влияют на вашу отрасль. Убедитесь, что ваша политика и практика соответствуют этим требованиям, демонстрируя как должную осмотрительность, так и осмотрительность.
- План реагирования: Разработайте надежный инциденты. В этом плане должно быть указано, как эффективно реагировать на инцидент безопасности, минимизируя ущерб и быстро восстанавливаясь. Регулярно тестируйте и обновляйте этот план, чтобы убедиться, что он эффективен, когда это необходимо.
- Документируйте все: ведите подробные записи обо всех ваших усилиях по обеспечению кибербезопасности, включая оценки рисков, оценки поставщиков, учебные занятия, обновления системы безопасности и реагирование на инциденты, связанные с этим. Эта документация может служить доказательством должной осмотрительности и осмотрительности в случае возникновения юридических проблем или нарушения безопасности.

Включение должной осмотрительности и должной осмотрительности в ваши политики кибербезопасности - это не разовое усилие, а постоянное обязательство, определяемое юридическими условиями и требованиями

соблюдения нормативных требований. Придерживаясь этих передовых практик, организации могут не только защитить себя от множества киберугроз, но и создать репутацию заслуживающих доверия и ответственных в эпоху цифровых технологий.

Разумная осторожность в кибербезопасности

Разумная осторожность в кибербезопасности относится к стандарту поведения, ожидаемому от организации или отдельного лица для защиты информационных систем и конфиденциальных данных от киберугроз. Это уровень осмотрительности, который разумно ожидать от благоразумного физического или юридического лица при аналогичных обстоятельствах. Эта концепция особенно важна в правовом и нормативном контекстах, поскольку неспособность продемонстрировать разумную осмотрительность может привести к возникновению ответственности и штрафных санкций.

Вот некоторые ключевые аспекты того, что разумная осторожность может включать в себя в контексте кибербезопасности:

- Регулярные оценки рисков: проведение текущих оценок для выявления и понимания потенциальных рисков в области кибербезопасности, с которыми сталкивается организация.
- Внедрение мер безопасности: Принятие соответствующих отраслевых стандартов безопасности, таких как брандмауэры, шифрование, антивирусное программное обеспечение и системы обнаружения вторжений для защиты от известных угроз.
- Обучение и осведомленность сотрудников: Регулярное обучение всех сотрудников передовым методам кибербезопасности, потенциальным угрозам (таким как фишинг) и важности соблюдения протоколов безопасности.
- Разработка политики и правоприменение: разработка, внедрение и обеспечение соблюдения комплексных политик и процедур кибербезопасности, которые регулярно пересматриваются и обновляются.
- Реагирования на инциденты планирования: имея вполне определенные и проверенные реагирования на инциденты план позволяет быстро и эффективно решать нарушений требований безопасности или инцидентах.

- Управление данными: обеспечение надлежащих методов управления данными, включая регулярное резервное копирование, шифрование данных и безопасные методы удаления данных.
- Управление поставщиками: проведение должной проверки сторонних поставщиков, чтобы убедиться, что они также соблюдают разумные методы и стандарты кибербезопасности.
- Соблюдение законов и нормативных актов: понимание и соблюдение соответствующих законов, нормативных актов и отраслевых стандартов, которые относятся к кибербезопасности и защите данных.
- Непрерывный мониторинг и совершенствование: Регулярный мониторинг инфраструктуры безопасности на предмет нарушений или слабых мест и постоянное стремление улучшить меры безопасности на основе возникающих угроз и передовых практик.

Проявляя разумную осторожность, организация не только защищает себя от множества киберугроз, но и закладывает основу для соблюдения законодательства и нормативных требований, укрепляет доверие с клиентами и партнерами и способствует распространению культуры осведомленности о безопасности и ответственности во всей организации.

Обычная осмотрительность/осторожность в кибербезопасности

“Обычная осторожность” в контексте кибербезопасности относится к стандарту осторожности, который разумное лицо или организация должны проявлять при нормальных обстоятельствах для защиты информации и систем от киберугроз. Это юридическая концепция, часто используемая для определения халатности или ответственности в случаях утечки данных или киберинцидентов. Идея заключается в том, что если физическое лицо или организация не принимают мер предосторожности, которые разумно предпринял бы любой разумный субъект, их можно считать проявившими халатность.

В сфере кибербезопасности осуществление обычной осторожности обычно включает:

- Внедрение базовых мер безопасности: Это включает использование брандмауэров, антивирусного программного обеспечения и шифрования, поддержание исправленных систем в актуальном состоянии и обеспечение физического доступа к критически важной инфраструктуре.