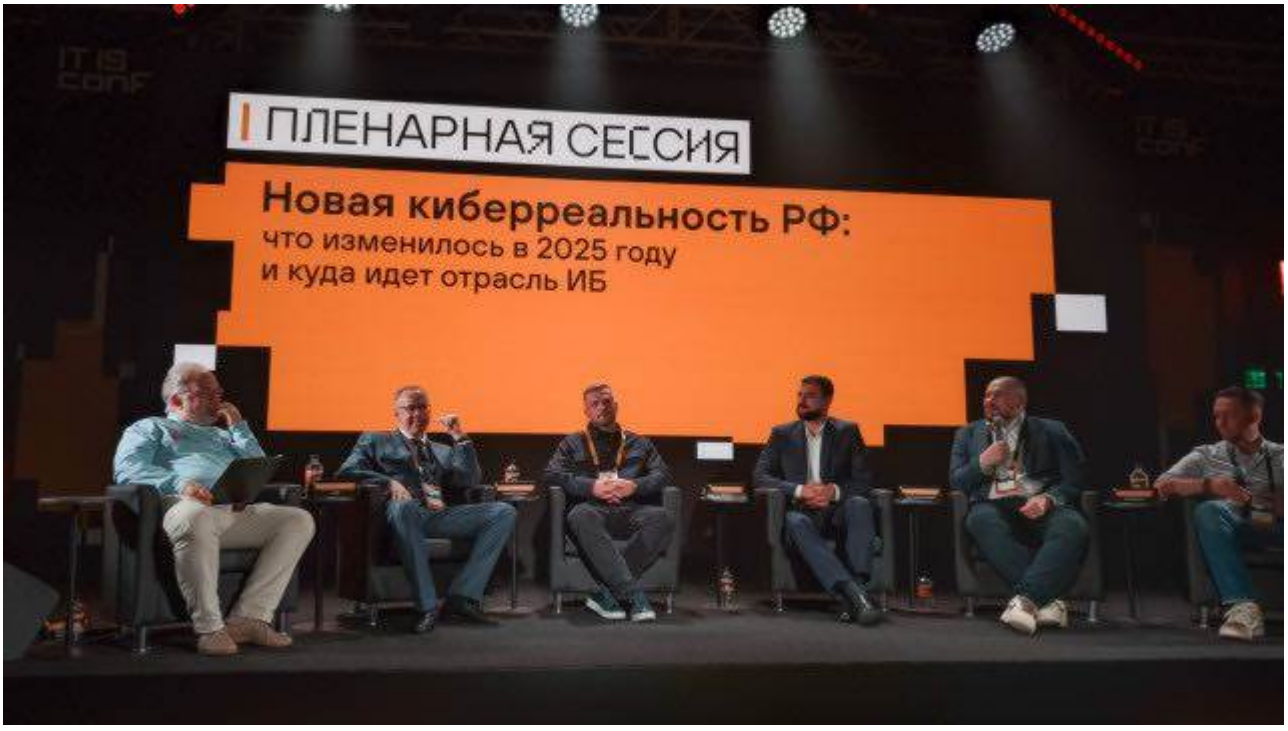
Новая киберреальность. Изменения и перспективы ИТ и ИБ отрасли в 2025



Эксперты по информационной безопасности и ИТ со всей страны съехались в Екатеринбург, чтобы обсудить актуальные вопросы кибербезопасности и ознакомиться с инновационными решениями рынка.

На 200%, по оценкам специалистов, может вырасти количество кибератак в России по итогам 2025 года, а в дальнейшем — на 50% ежегодно. Увеличивается не только число взломов и утечек данных, но и их сложность и масштаб. Это связано, в том числе и с использованием преступниками инструментов искусственного интеллекта (ИИ), а также атаками не напрямую, а через подрядчиков. Защиту бизнеса в этих условиях и новые тренды в отрасли информационной безопасности (ИБ) обсудили участники IT IS conf — крупнейшей на Урале конференции в сфере информационных технологий и информационной безопасности.

Значительная часть конференции была посвящена проблеме использования искусственного интеллекта в сфере информационной безопасности. С одной стороны, ИИ позволяет прогнозировать новые киберугрозы и анализировать уязвимости в коде. С другой — эту технологию все активнее используют злоумышленники для кибератак.

«Мы говорим об ИИ не первый год, но кардинальные изменения правил игры на рынке произошли с появлением OpenAI (американской технологической компании, которая разработала, в том числе, ChatGPT — прим. ред.). А поскольку гиперкриминал, в отличие от легального бизнеса легче на подъем, именно он начал активно использовать искусственный интеллект в различных сценариях. С помощью больших языковых моделей злоумышленники начинают реализовывать как классические сценарии фишинга, так и разрабатывать собственные модели и обучать их для проведения хакерских атак», — отмечает эксперт по кибербезопасности, автор блога «Бизнес без опасности» Алексей Лукацкий.

Эксперт по кибербезопасности, автор блога «Бизнес без опасности» Алексей Лукацкий

Легальный рынок кибербезопасности пока только присматривается к использованию искусственного интеллекта, оглядываясь на регуляторов. Однако эксперты сходятся во мнении: за ИИ — будущее. По их словам, активное внедрение искусственного интеллекта может привести к появлению совершенно новых векторов атак и методов защиты.

«ИИ, как и любой мощный инструмент, должен использоваться с осторожностью. Мы движемся к автоматизации задач управления информационной безопасностью, что ведет к обесчеловечиванию систем защиты — они становятся автономными. Такие системы могут принимать сложные решения и управлять критически важными объектами без участия человека. Это действительно меняет ландшафт угроз. Но с другой стороны, ИИ — очень сильный инструмент, который радикально изменит нашу отрасль, позволит создать новые средства защиты и даже новые подходы к обеспечению информационной безопасности», — отмечает генеральный директор УЦСБ Валентин Богданов.

Генеральный директор УЦСБ Валентин Богданов

Помимо защиты от кибератак, искусственный интеллект рассматривается как потенциальное решение проблемы нехватки кадров. И здесь встает другой вопрос: а не заменит ли ИИ специалистов в сфере ИТ и информационной безопасности (ИБ). Большинство участников дискуссии согласились, что на данный момент такой угрозы нет — ИИ может оказывать поддержку человеку, но никогда не вытеснит его полностью.

Министр цифрового развития и связи Свердловской области Михаил Пономарьков

«Пока существует человек со своими деструктивными намерениями и желанием нанести вред, будут и профессионалы по безопасности. Ни одна компания не может чувствовать себя полностью защищенной от внешних угроз», — считает руководитель отдела информационной безопасности «Дикси Юг» Александр Танчук.

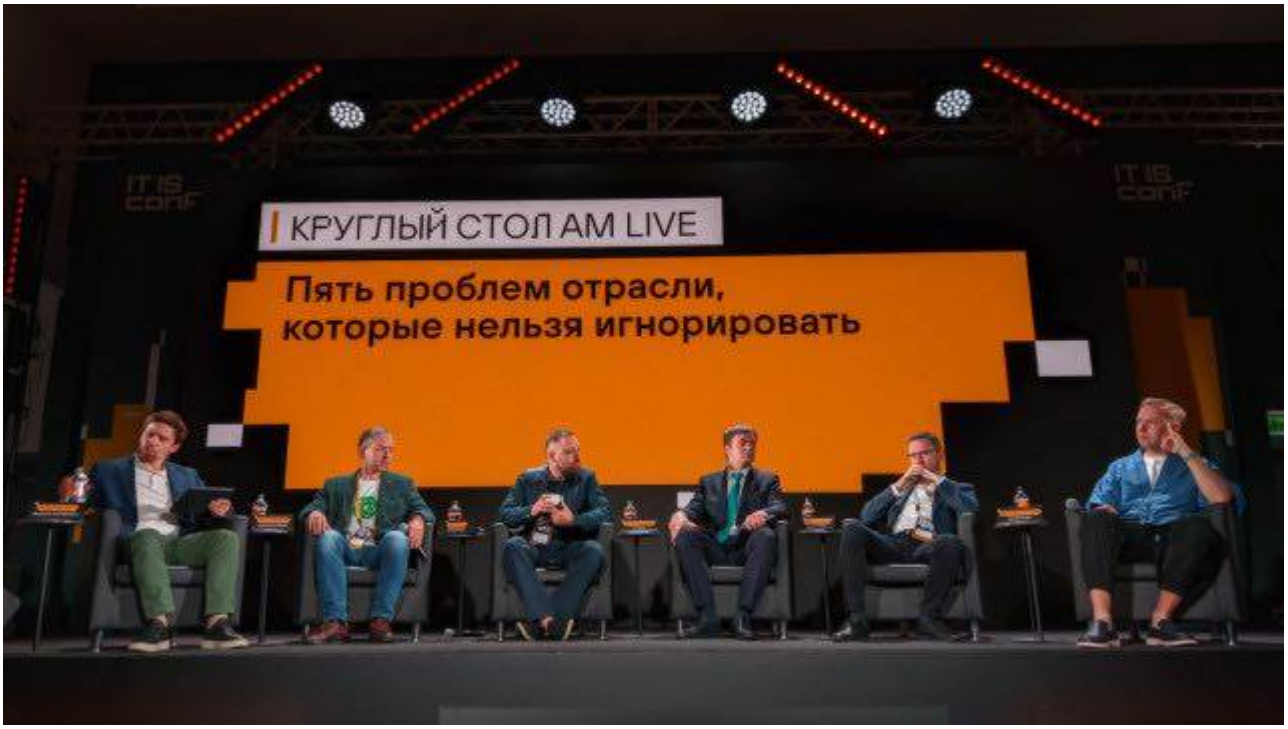
Директор департамента информационной безопасности компании «Аквариус» Константин Закатов

С ним солидарен директор департамента информационной безопасности компании «Аквариус» Константин Закатов, который отмечает, что ИИ не обладает такой же

логикой и необходимыми нейронными связями как человек, чтобы понять, что он сделал неправильный вывод из полученного массива данных.

Валентин Богданов также уверен, что искусственный интеллект не заменит специалиста по безопасности, но будет работать «на нас и для нас».

«Многие задачи низкого уровня могут быть выполнены ИИ: анализ логов, разбор простейших инцидентов. Думаю, в нашей сфере будет появляться все больше автоматизации», — отмечает эксперт.



Помимо темы искусственного интеллекта и роста числа кибератак, участники дискуссий обсудили и другие важные проблемы отрасли.

Согласно опросу, проведенному модератором круглого стола AM Live «Пять проблем отрасли, которые нельзя игнорировать», основателем и генеральным директором Anti-Malware.ru Ильей Шабановым, «боли» бизнеса выглядят так:

- 47% — нехватка кадров;
- 45% — дефицит бюджета;
- 33% — проблемы импортозамещения;
- 31% — усложнение ИТ-инфраструктуры;
- 27% — ужесточение требований регулятора к информационной безопасности.

Автор блога ZLONOV.ru, Алексей Комаров, считает, что при нехватке кадров существует два пути решения проблемы: автоматизация и применение ИИ или обучение и повышение квалификации ИТ-персонала. По его словам, любой ИТ-специалист может стать отличным специалистом по информационной безопасности, а к квалификации ИБ-специалиста без ИТ-бэкграунда могут возникнуть вопросы.

Однако опрос участников IT IS conf показал, что немногие готовы к автоматизации процессов. Объяснение этому дал руководитель отдела продвижения продуктов «Код Безопасности» Павел Коростелев.

Руководитель отдела продвижения продуктов «Код Безопасности» Павел Коростелев.

«Автоматизация решает рутинные задачи, однако при этом стоимость ошибки значительно возрастает. Зачастую бизнес-процессы, написанные на бумаге, сильно отличаются от фактического бизнес-процесса. Если человек способен скорректировать эти несоответствия в ходе работы, то искусственный интеллект — нет», — отмечает Коростелев.

По словам эксперта, уже через пару лет количество киберугроз значительно возрастет, а число специалистов, отвечающих за информационную безопасность, сократится.

«У нас будет слишком много новых угроз за короткий промежуток времени, чтобы использовать текущие методы реагирования», — поделился прогнозами представитель «Кода Безопасности».

Решить проблему дефицита кадров можно несколькими способами. Например, УЦСБ сотрудничает с вузами и «выращивает» кадры под свои нужды.

«Мы создали в университете две лаборатории по кибербезопасности, у нас есть стендовая база, на которой ежегодно обучается около 40 студентов. На самом деле остро стоит проблема с специалистами уровня middle и high, но это общемировая тенденция — высококлассных специалистов по информационной безопасности немного по определению», — рассказал Валентин Богданов.

Что касается специалистов среднего уровня, то генеральный директор УЦСБ советует поддерживать необходимый уровень компетенций сотрудников: обучать и мотивировать развиваться.

По аналогичной схеме действует и компания «Газинформсервис»: там ведут талантливых студентов с третьего-четвертого курса.

Это вторая по остроте проблема, практически не уступающая вопросу кадрового дефицита. Бюджета на информационную безопасность всегда будет недостаточно, и его можно бесконечно увеличивать.

Участники дискуссии поделились своим взглядом на возможные решения этой проблемы.

1. **Приоритезация**

«Необходимо вести системную работу по приоритезации ИТ-ресурсов и бизнес-процессов, которые нужно защищать любой ценой, сосредоточиться на наиболее вероятных или наиболее серьезных угрозах, проработать их в первую очередь», — считает Павел Коростелев.

2. **Маленькие быстрые победы**

«При ограниченности бюджетов оптимально придерживаться стратегии быстрых побед — то есть сосредотачиваться на тех аспектах защиты, которые дают быстрый результат при небольших затратах. Даже слабая защита лучше, чем ее полное отсутствие. Общий уровень опасности можно снизить и с помощью бесплатных инструментов, доступных без дополнительных внедрений», — отмечает Алексей Комаров.

3. **Взаимодействие**

«Денег всегда будет недостаточно. Информационная безопасность и ИТ должны работать вместе, а не конкурировать за бюджеты. Необходимо правильно ставить цели и достигать консенсуса — какие риски можно считать менее критичными и важными, а какие — более значимыми», — считает Константин Закатов.

Эти две проблемы получили примерно равное количество голосов и тесно связаны друг с другом. С одной стороны, необходимо соответствовать новым технологическим трендам, а с другой — заниматься импортозамещением существующих решений. И не всегда удается успешно реализовать оба направления одновременно.

Впрочем, уже сейчас большинство компаний перешли на отечественные решения, а многие начали отказываться от ПО и оборудования зарубежных вендоров задолго до событий 2022 года. Однако к российским аналогам и продуктам по-прежнему предъявляются две основные претензии: высокая цена и не всегда нужное качество.

С 30 мая вступили в силу новые штрафы за утечку персональных данных. За повторную утечку теперь применяют оборотный штраф, то есть в процентах от общей выручки компании.

«Само по себе требование по защите данных существует с 2013 года, но с введением оборотных штрафов стоимость недооценки угроз кибербезопасности выросла. Построить систему безопасности в некоторых случаях будет дешевле, чем платить за утечку», — рассказывает Алексей Лукацкий.

По словам эксперта, регулятор уже выпустил практически все требования к информационной безопасности — сейчас в основном меняются правила, связанные с ответственностью и категорированием критической информационной инфраструктуры.

«Ранее государство оставляло это на усмотрение бизнеса, который по понятным причинам старался либо не классифицировать себя, либо занижать категории. Сейчас же оно взяло это на себя. Буквально месяц назад были приняты новые правила: именно государство будет определять, кого и как защищать, а бизнесу придется пересматривать подходы к системам защиты», — добавил эксперт.

В 2025 году IT IS conf проходила не один, а два дня. В ней приняло участие более 600 человек — экспертов в сфере информационных технологий и безопасности со всей страны, руководителей ИТ-компаний, специалистов по кибербезопасности бизнес-структур и государственных компаний.

В рамках конференции эксперты в тематических треках рассказали, как обеспечить информационную безопасность, поделились методами построения безопасной разработки, обсудили возможность создания «открытых» ИБ-систем и многое другое. Также в течение двух дней на конференции работала выставка решений наиболее востребованных отечественных разработчиков.

Помимо обсуждения глобальных отраслевых трендов и вызовов, на IT IS conf участников ждали практические решения в мастерской Центра кибербезопасности УЦСБ. В этой технической секции слушатели конференции вместе со спикером выполняли задания и тестировали решения по информационной безопасности.

Источник: rbc.ru