Тренды глобального рынка кибербезопасности

Пандемия Covid 19 и связанный с ней режим вынужденной изоляции стали ключевым фактором, способствовавшим скачкообразному росту объемов интернет - экономики. Кроме этого, развитие цифровизации поддерживают такие факторы как прогресс цифровых технологий, расширение сферы применения мобильных и облачных приложений, увеличение спроса на услуги IoT и беспилотной авиации и многое другое.

Быстрый рост рынка, появление новых областей использования цифровых приложений создает новые уязвимости, новые возможности и угрозы. Технологии используемые для кибератак прогрессируют вместе с рынком. Важный тренд в развитие киберугроз - это рост числа сложных, целевых атак, ориентированных на определенные конечные точки, локальные устройства или даже конкретных пользователей. Главным мотивом становится хищение информации с целью получения денег.

В этих условиях бизнес, государственные и некоммерческие структуры высоко мотивированы на быстрое внедрение последних технологических достижений в сфере кибербезопасности. Главным ограничением становится финансовый фактор: малый бизнес и стартапы сейчас составляют значительный сегмент в глобальной экономике, но они не могут выделять больших бюджетов на обеспечение собственной цифровой безопасности. Важно, что это открывает возможность для формирования экосистемных преимуществ для малого бизнеса, за счет

создания единых систем обеспечения кибербезопасности МСП в рамках государственной поддержки отрасли.

Согласно экспертным оценкам, объем мирового рынка кибербезопасности по состоянию на 2022 год может составить $154 - $174 млрд. Возможный среднегодовой темп роста рынка составляет 9% - 14%.

Основные усилия разработчиков систем кибербезопасности в настоящее время сосредоточены на минимизации угроз для мобильных приложений, облачных решений а также для IoT. Также большое внимание уделяется системам разведки и наблюдения, дающим возможность своевременно обнаруживать кибератаки и своевременно реагировать на них. Перспективным решением считается использование в системах кибербезопасности технологий искусственного интеллекта.

С точки зрения моделей бизнеса интересной новацией является развитие киберстрахования: услуг призванных компенсировать финансовые потери, связанные с возможными хакерским атаками. Важно, что компании страхующие такие риски формируют требования к

стандартам качества защиты от киберугроз. Другой определяющий тренд развития бизнеса в сфере кибербезопасности - это быстрый рост аутсорсинговых услуг. Эффективная защита требует высокой профессиональной квалификации и компаниям становится выгодно нанимать опытных сторонних специалистов.

Быстрый прогресс технологий, таких как квантовые вычисления и большие языковые модели может создать новые вызовы на глобальном рынке услуг в сфере кибербезопасности.