Уязвимости ПО, атаки на квантовый интернет – чего ждать от преступников?

Аналитическое агентство Gartner прогнозирует, что к 2025 году около 40% крупных компаний начнут внедрять квантовые технологии и проводить пилотные проекты на их основе. По данным отчета McKinsey & Company за 2023 год, инвестиции в квантовые технологии достигли нового максимума — 2,35 миллиарда долларов. Интерес к квантовым технологиям проявляют не только корпорации, но и злоумышленники, ищущие новые способы организации кибератак.

Специалисты Positive Technologies совместно с «КуБорд», QApp и «Российским квантовым центром» представили исследование « Безопасность квантовых технологий в сфере IT ». В нем названы главные киберугрозы, которые угрожают квантовым технологиям: кража информации, уязвимости ПО и атаки на квантовый интернет.

Главные угрозы квантовых технологий

Среди ключевых угроз выделены 5 аспектов.

Эксперты также подчеркивают угрозы, связанные с постквантовой криптографией. Тактика «сохрани сейчас — расшифруй потом» (store now, decrypt later) позволит злоумышленникам в будущем расшифровывать данные, используя мощный квантовый компьютер. Для защиты некоторые компании начинают внедрять метод постквантового шифрования.

Квантовые технологии активно развиваются в России. Основным драйвером являются дорожные карты направлений «Квантовые вычисления» и «Квантовые коммуникации», которые курируют «Росатом» и РЖД. Квантовые технологии стали одной из сквозных тем в национальном проекте « Экономика данных ». Исследовательские центры, госкорпорации, бизнес и университеты выступают инициаторами проектов, связанных с изучением квантовых технологий в России.

Комплексной защиты квантовых технологий от киберугроз пока нет, что связано с вариативностью их развития. Вендоры видят одним из перспективных направлений защиты открытие новых багбаунти программ для выявления уязвимостей квантовых систем.

Важным шагом для будущей кибербезопасности является концепция квантового распределения ключей, над которой ведутся работы, и которая обещает создание более защищенных каналов связи.