МНЕНИЕ ЭКСПЕРТА

Миниатюризация беспроводных устройств, возможность их прямой имплантации в орган, использование «беспроводной зарядки» и более длительный срок эксплуатации – это, конечно, огромный шаг вперед. Если после тестирования на людях будут достигнуты положительные результаты, то следующим шагом должно стать постепенное снижение стоимости, что сделало бы устройство доступным различным категориям пациентов, перенесших операцию по замене сердечного клапана.

Однако следует учитывать тот факт, что предлагаемая система не является «замкнутой», и сигналы в организм человека поступают извне. Это означает риски случайного или, что еще хуже, сознательного вмешательства в передачу электромагнитных сигналов, например с целью значительного превышения их мощности. Последствия этого могут быть самыми драматическими. И в этой связи хотелось бы упомянуть два факта.

Еще в 2016 эксперты компании MedSec сообщали, что кардиостимуляторы и кардиодефибрилляторы компании St. Jude Medical (ныне Abbott) содержат многочисленные уязвимости, которые несут потенциальную угрозу здоровью, а возможно – и жизни пациентов. При этом сам производитель – компания St. Jude Medical – решительно опровергала данные сообщения. И только после вмешательства FDA (Food and Drug Administration, Управление по контролю качества продуктов и лекарств США) было установлено, что риски реальные, и почти 500 000 пациентов в 2017 г. было предложено пройти процедуру обновления программного обеспечения после сертификации FDA выпущенной Abbott «заплатки» на ПО. Эксперты по информационной безопасности считают, что атаки на кардиостимуляторы и другие медицинские устройства в самом скором будущем могут стать настоящей золотой жилой для вымогателей и шантажистов, которые могут атаковать не только пациентов, но и производителей подобных устройств, а также сами медицинские информационные системы. В этой связи необходимо обратить внимание на статистику, приводимую компанией InfoWatch, за первое полугодие 2017 г.: 17% инцидентов утечки информации пришлось на медицинские организации, а по доле целевых утечек информации в 49% случаев сфера здравоохранения вошла в топ-3. В 2016 г. более 50% IT-затрат медицинских организаций в ЕС приходилось на обеспечение информационной безопасности. И несмотря на это, весной 2017 г. вирус WannaCry атаковал в том числе Национальную систему здравоохранения (NHS) Великобритании, из-за чего многие медицинские учреждения объявили, что будут принимать только экстренных пациентов.

Поэтому при разработке носимых беспроводных устройств необходимо руководствоваться принципом «не навреди» в квадрате, с учетом качественного и количественного роста степеней риска.

Александр Антипов, *директор по развитию бизнеса компании «Ай-ФОРС» (ГК ФОРС)*