информационных систем требуется соблюдение надежности и безотказности, то данные условия обеспечиваются преимущественно за счет аппаратного и программного резервирования. Пусть дана распределенная информационная система, для которой необходимо обосновать состав и технические параметры подсистем резервирования (в рамках технологии отказоустойчивости) и определить параметры системы предотвращения вторжений. Для данной информационной системы моделируются экстремальные режимы функционирования по внешним и внутренним рабочим нагрузкам, а также вся известная номенклатура внешних информационных угроз. В отсутствии системы предотвращения вторжений, аппаратного и программного резервирования информационной системы отмечаются снижения эффективности ее функционирования при сочетании предельных значений диапазона рабочих нагрузок и реализаций всей номенклатуры внешних угроз. Экспериментальным путем подбираются параметры алгоритма управления параллельными вычислениями системы предотвращения вторжений на уровне данных и решаемых задач, благодаря которым добиваются своевременного определения угроз и выбора эффективных мер по противодействию им. Пострадавшие в результате реализации информационных угроз элементы информационной системы заменяются на время их восстановления на резервные элементы, которые функционировали до этого в зеркальном режиме, но без коммуникации со внешними абонентами информационной системы. Эффективность защитных мероприятий за период моделирования определяется как отношение предотвращенного ущерба информационной системе (в денежных единицах) к сумме стоимостей системы предотвращения вторжений и технологии отказоустойчивости с учетом аппаратного и программного резервирования информационной системы. По результатам имитационного моделирования обосновываются требования к системе предотвращения воздействий с параллельными вычислениями и к составу системы аппаратного и программного резервирования, реализующей технологию повышения отказоустойчивости.

ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНОЛОГИИ NFC

Ю.С. Камышев, Ю.А. Скудняков

Одним из современных способов защиты информации является NFC (Near field communication) – коммуникация ближнего поля либо ближняя бесконтактная связь. Это технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на близком расстоянии; анонсирована в 200 4г. Эта технология является простым расширением стандарта бесконтактных карт, которое объединяет интерфейс смарт-карты и считывателя в единое устройство. Устройство NFC может поддерживать связь и с существующими смарт-картами, и со считывателями стандарта ISO 14443, и с другими устройствами NFC и, таким образом, совместимо с существующей инфраструктурой бесконтактных карт, уже использующейся в общественном транспорте и платежных системах. NFC нацелена прежде всего на использование в цифровых мобильных устройствах. NFC – это беспроводная дистанционная технология, которая работает на расстоянии не более 10 сантиметров. NFC работает на частоте 13,56 МГц. NFC всегда включает инициатор и цель. Инициатор активно генерирует радиочастотное поле, которое может влиять на пассивную цель. Также возможна NFC-связь между двумя устройствами при условии, что оба устройства включены [1]. Но у данной технологии есть и минусы, например, эксплойт 0day, подслушивание (так как это радиосигнал), модификация данных (например, устройствами глушения RFID), атака с использованием ретрансляции и т.д. Исходя из вышеизложенного, можно сделать вывод о том, что NFC на сегодняшний день является весьма небезопасным протоколом, с помощью которого в том числе и передаются банковские данные. В связи с этим риск потерять деньги весьма велик. На сегодняшний день это самая распространенная технология в данном сегменте и остается только надеяться, что платежные данные не попадут третьим лицам.

Литература

1. Near Field Communication (NFC) Technology and Measurements [Электронный ресурс]. – URL: www.rohde-schwarz.com (дата обращения: 18.05.2018).