ТЕХНОЛОГИИ БЛИЖНЕЙ БЕСКОНТАКТНОЙ СВЯЗИ И ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сабериан М.А..

Утин Л. Л. – к.т.н, доцент

В последние годы наблюдается устойчивая тенденция развития технологий ближней бесконтактной связи NFC. Известно, что внедрение новых средств связи способствует появлению дополнительных угроз нарушения конфиденциальности, целостности, доступности, сохранности и подлинности информационных ресурсов. В докладе предлагаются к обсуждению проблемные вопросы в области защиты информации при применении технологий NFC.

Технологии ближней бесконтактной связи являются одним из альтернативных решений передачи данных с мобильного телефона к приемному устройству. NFC — технология с открытой платформой, стандартизированная в ECMA-340 и ISO/IEC 18092.Эта технология может применяться:

для обмена файлами между телефонами (отдельно либо в сочетании с каналом Bluetooth);

эмуляции смарт-карт;

в качестве средства оплаты за проезд в общественном транспорте;

для открытия электронных замков в квартиру или машину;

в качестве удостоверения личности, страховой карты и т.д.

Достоинствами данной технологии является низкое время установления связи (менее 0,1 с. (для сравнения в технологии Bluetooth данный параметр равен 6 с)), сложность перехвата электромагнитного излучения злоумышленником из-за малого радиуса действия (менее 20 см), простота реализации и ряд других.

Следует отметить, что не смотря на достоинства данной технологии ей присущи определенные недостатки:

до настоящего времени существует потенциальная опасность заражения банковской системы вирусами, которая может осуществиться при использовании мобильного телефона в качестве средства по оплате платежей;

использование средств постановки помех в диапазоне 13,56 МГц приводит к срыву сеансов связи с использованием технологии NFC;

потенциальная возможность утечки персональных данных при осуществлении связи.

Для защиты от утечки применяют различные методы шифрования, антивирусные программы. Проведенный анализ показал, что в настоящее время подходы к шифрованию данных в мобильной связи меняются. Так в дополнение к шести основным принципам Керкгоффса ужесточаются требования к пропускной способности, объему оперативной памяти. В докладе предлагается к обсуждению полученные результаты исследований возможностей различных криптографических алгоритмов шифрования, которые могут быть использованы для шифрования информации с использованием технологий NFC/