измерения и разрешающей способности по дальности, которые определяются длительностью отклика – его основного пика. При использовании сложных сигналов эта противоречивая взаимосвязь разрешима, т. е. можно увеличивать длительность сложного сигнала, его энергию, сохраняя неизменной ширину спектра. При этом максимальная длительность сигнала будет ограничиваться допустимой мощностью передатчика. Поэтому для повышения точности измерения и разрешающей способности по дальности можно увеличивать ширину спектра.

В рамках поставленной задачи, на основе результатов проведенных экспериментов, выполнены численные расчеты корреляционных свойств полученных сложных сигналов, которые имеют тесную взаимосвязь с двухпараметрической функцией неопределенности.

Литература

1. Лущицкий В.В., Савельев В.Я., Ткаченко Ф.А. Анализ работы и расчет основных характеристик генератора на диодах Ганна с варакторной перестройкой частоты // Радиотехника и электроника. 1984. Вып.13. С. 69–73.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ХРАНЕНИЯ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

О.В. Базылева, Г.А. Пухир

Развитие высоких технологий и тренд мобильности привели к тому, что современное мобильное устройство – смартфон или планшет зачастую используется в качестве мобильного офиса, центра развлечений и инструмента для потребления Интернет-контента. Высокая концентрация деловых и персональных данных приводит к тому, что абстрактная стоимость информации перевешивает цену самого устройства.

В то время как мобильные приложения изначально предлагались как инструменты для повышения производительности и информации, рынок быстро расширялся из-за требований пользователей и наличия инструментов для разработчиков. Ежедневно люди оперируют десятками программ на смартфонах. Многие из них передают конфиденциальную информацию, которая может заинтересовать злоумышленников. Исследователи обнаружили присутствие небезопасных приложений практически в каждой отрасли, включая производственные и финансовые услуги. По оценкам экспертов RiskIQ, более 11 % приложений для банковских операций содержат вредоносное ПО или подозрительный код.

К типовым уязвимостям мобильных приложений по отношению к данным пользователей можно отнести:

1. Небезопасное хранение конфиденциальных данных в незашифрованном виде.
2. Слабые серверные элементы управления на клиентском устройстве.
3. Недостаточную защиту транспортного уровня.
4. Инъекцию на стороне клиента, позволяющую реализовать доступ пользователя к произвольному, ненадежному веб-контенту.
5. Слабую авторизацию и аутентификацию.
6. Неправильную обработку сеансов.
7. Реализацию ненадежных входов, позволяющую приложениям общаться между собой, что может быть использовано злоумышленником для атаки.
8. Утечку данных ввода/вывода, обычно используемые для административных или нефункциональных целях из сторонних каналов.
9. Плохое управление криптоключами с возможностью их восстановления.
10. Раскрытие конфиденциальной информации, учитывая, что скомпилированные исполняемые файлы могут быть подвергнуты реверс-инжинирингу.

Представленная проблема демонстрирует важность срочного решения вопроса безопасности мобильных устройств, как с точки зрения пользователей, так и разработчиков.

Со стороны разработчиков необходимо, чтобы каждое приложение разрабатывалось путем тщательного ознакомления с передовыми методами кодирования, а затем постоянно оценивалось для выявления потенциально возможных недостатков. Одним из наиболее эффективных способов повышения безопасности приложений можно отнести защиту сервисов, к которым подключаются приложения.