Анализ угроз, уязвимостей, ошибок кода программного обеспечения

Кармашов В.А.
Магистр, Московский Технологический Университет
E-mail: karma001@yandex.ru

Введение.

Безопасность программного обеспечения (ПО) в широком смысле является свойством данного ПО функционировать без проявления различных негативных последствий для конкретной компьютерной системы. Под уровнем безопасности ПО понимается вероятность того, что при заданных условиях в процессе его эксплуатации будет получен функционально пригодный результат. Причины, приводящие к функционально непригодному результату могут быть разными: сбои компьютерных систем, ошибки программистов и операторов, дефекты в ПО. При этом дефекты принято рассматривать двух типов: преднамеренные и непреднамеренные. Первые являются, как правило, результатом злоумышленных действий, вторые — ошибочных действий человека.

Основные особенности ПО.

В общем случае, процесс разработки ПО состоит из нескольких стадий, которые описываются моделью жизненного цикла:

1. Системный анализ.
2. Анализ требований.
3. Проектирование.
4. Кодирование.
5. Тестирование.
6. Сопровождение.

На каждом этапе могут быть допущены ошибки, которые в итоге могут стать причиной появления уязвимостей ПО, используемых злоумышленником для атак на ПО.

Использование при создании ПО сложных операционных систем, инструментальных средств разработки ПО импортного производства увеличивают потенциальную возможность внедрения в программы преднамеренных дефектов диверсионного типа. Помимо этого, при создании целевого ПО всегда необходимо исходить из возможности наличия в коллективе разработчиков программистов — злоумышленников, которые в силу тех или иных причин могут внести в разрабатываемые программы недокументированные возможности и разрушающие программные средства (РПС).

Одним из важнейших частей проектирования является разработка общего метода решения задачи (алгоритмизация), на котором важно продумать всё до мелочей, потому что ошибки на этом этапе очень опасны. Ход процесса проектирования и его результаты зависят не только от заданных требований, но так же и от выбранной модели процесса, опыта проектировщика.

Заключение.

Необходимой составляющей проблемы обеспечения информационной безопасности программного обеспечения является общегосударственная система стандартов и других

нормативных и методических документов по безопасности информации, а также международные стандарты и рекомендации по управлению качеством программного обеспечения, которые позволяет предъявить к создаваемым и эксплуатируемым программных комплексам требуемый уровень реализации защитных функций. Изложенный материал, позволит при изучении технологии проектирования систем обеспечения безопасности программного обеспечения избежать многих ошибок, которые могут существенно повлиять на качество проекта и эффективность конечной системы в целом при ее реализации на объектах информатизации различного назначения.

Библиографический список.

1. Багров Е.В. Мониторинг и аудит информационной безопасности на предприятии//Вестник Волгоградского государственного университета. Инновационная деятельность.2011.№ 5. С 50-56
2. Мартин, Р. Чистый код: создание, анализ и рефакторинг / Р. Мартин. — СПб.: Питер, 2010. — 464 с.
3. Герасименко В.А. Защита информации в АСОД.- М.: Энергоиздат, 1994.
4. Защита программного обеспечения: Пер. с англ./ Д. Гроувер, Р. Сатер, Дж. Фипс и др./ Под редакцией Д. Гроувера.- М.: Мир, 1992.
5. Зегжда Д.П., Шмаков Э.М. Проблема анализа безопасности программного обеспечения// Безопасность информационных технологий. — 1995.- № 2.- С.28-33.