XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V : С.211-212

УДК 004.05

А.П.Лубанец (асп., каф. Телематика), В.С.Заборовский, д.т.н., проф.

НАУЧНО-ТЕХНИЧЕСКИЕ АСПЕКТЫ КОМПЛЕКСНОГО ПОДХОДА ПРИ РАЗРАБОТКЕ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современный ритм жизни общества обусловлен развитием постиндустриальной экономики и глобалистическими идеями. Важно отметить тот факт, что огромную роль в становлении «информационного периода» с его неизбежной атрибутикой сыграло появление цифровых технологий, приведших к изменениям привычных вещей, в частности, к появлению информационных систем (ИС) различного уровня и назначения.

В общепринятой трактовке, ИС – это система, предназначенная для хранения, передачи или обработки данных. По законодательству РФ, ИС – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы. Международная организация стандартов (МОС, ISO – International Organization for Standardization) понятие информационная система трактует иначе: ИС называют совокупность, состоящую из персонала, одного либо нескольких компьютеров, соответствующих средств программирования, физических процессов, средств телекоммуникаций и других объектов, образующих автономное целое, способное осуществлять обработку данных или передачу данных. ИС в трактовке МОС состоит из пяти подсистем, это подсистемы аппаратного, программного, информационного, организационного и правового обеспечения. Таким образом, комплексного понятия в этих определениях в полной мере нет, а понимание терминов затруднено разночтением. Отсюда возникают большие сложности с понятиями «информационная безопасность» (ИС) и «система информационной безопасности» (СИБ). Поэтому необходимо уточнение понятия данных терминов.

Прежде чем сформулировать объект защиты, разберемся, а что же есть ИС «де-факто». Следует понимать, что ИС это:

- не более чем один из множества способов управления объекта субъектом;
- инструмент, средство, а не задача или цель;
- обязательно полный жизненный цикл информации: сбор сведений об объекте в виде данных, обработка и хранение информации, вывод и распространение информации, управление на основании информации;
- наличие обратной связи;
- масштабируемая, открытая и прозрачная система;
- научное обоснование архитектуры, принципов построения компонентов и подсистем поведения системы, а также ее поведения.

Составные компоненты ИС во взаимосвязи:

- объект: то чем управляет субъект;
- система сбора данных: позволяет извлечь информацию;
- информационный ресурс: позволяет хранить и перерабатывать извлеченную информацию;
- информационная технология: позволяет осуществлять ввод/вывод и распространение информации
- субъект: управляет объектом;

– средства информационного взаимодействия: позволяют сформировать информационную инфраструктуру и информационное пространство.

В контексте приведенных выше положений ИС как объект защиты представляет из себя совокупность следующих компонент:

– приложение: информационный ресурс и информационная технология;
– пользователи и обслуживающий персонал: субъекты;
– коммуникации: средства информационного взаимодействия;
– система безопасности: средства обеспечения информационной и физической безопасности и политика информационной и физической безопасности.

В рамках уточнения подхода к созданию СИБ, следует упомянуть о том, что теории управления Г.Форда и К. Мацусита и, как следствие, современная конъюнктура рынка труда, привели к обострению проблемы социальной инженерии. Под социальной инженерией подразумевается набор приемов, с помощью которых злоумышленник может собрать необходимые для взлома системы данные, злоупотребляя доверчивостью и/или халатностью сотрудников. Именно поэтому при рассмотрении ИС как объекта защиты центральным объектом современных СИБ является компонент «пользователи и обслуживающий персонал».

В результате вышеизложенного подхода можно сделать следующие выводы:

1) ИС обязана проектироваться с выполнением следующей парадигмы: при разработке СИБ для ИС должна обеспечиваться максимальная проработка системы на стадии ее проектирования, должна обеспечиваться работоспособность в процессе ее эксплуатации, необходимо наличие мер и средств по быстрому вводу ИС в штатный режим работы в критических ситуациях;

2) проектирование СИБ для ИС – сложная научно-техническая задача;

3) при проектировании должна быть ориентация на архитектуры систем гарантированной ИБ;

4) должна вестись разработка новых криптографических алгоритмов и пересмотр существующих стандартов в сторону увеличения стойкости криптосистем;

5) управление СИБ должно быть основано на принципах обеспечения целостности, управляемости, доступности и наблюдаемости ИС.