Для разработки нормативных документов "*Профиль защиты*" и "*Задание по обеспечению безопасности*" предлагается использовать набор детализированных требований безопасности, систематизированных с учетом привязки к объектам информационных технологий и к существующим классам требований СТБ 34.101.

Приводится пример формирования пакетов функциональных и гарантийных требований безопасности.

Описаны подходы при сертификации средств реализации требований безопасности на базе пакетов функциональных и гарантийных требований безопасности.

ФУНКЦИОНАЛЬНЫЕ И ГАРАНТИЙНЫЕ ПАКЕТЫ ТРЕБОВАНИЙ К СРЕДСТВАМ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

С.К. ТУРБИН, М.А. ТАЛАЛУЕВА

Рассматривается задача формирования требований по управлению безопасностью в виде пакетов требований.

В практике имеются случаи, когда на ранних этапах разработки информационных систем нельзя четко описать объект, угрозы безопасности и на этой основе сформулировать задачи безопасности. В этих случаях целесообразно разрабатывать не профиль защиты (ПЗ), а пакеты функциональных и гарантийных требований.

По существу разработка пакета – первый шаг к созданию некоторого профиля защиты или семейства ПЗ, и к использованию в задании по обеспечению безопасности (ЗБ).

Опыт формирования пакетов весьма ограничен. На сегодняшний день практическими примерами пакетов являются уровни гарантии оценки, определенные в СТБ 34.101.3, которыми следует пользоваться для формирования гарантийных пакетов.

Пакеты, предназначены для многократного использования:

- потребителями в качестве пособия при обосновании требований к средствам управления безопасностью;
- экспертами (испытателями) при проверке соответствия представленных на сертификацию средств управления безопасностью заданным функциональным и гарантийным требованиям безопасности.

Эффект от использования пакетов состоит:

- в уменьшении стоимости разработки ПЗ и (ЗБ);
- в сокращении сроков и объемов работ при разработке ПЗ или ЗБ при выборе или определении требований к средствам управления безопасностью.

КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

С.К. ТУРБИН, В.К. ФИСЕНКО

Основными целями защиты информации являются обеспечение ее конфиденциальности, целостности и доступности. Поэтому целесообразно провести классификацию всего множества средств защиты по целевому назначению. С учетом того, что в соответствии с принципом суперпозиции сложная техническая система подразделяется на средства непосредственно исполнительные и средства, поддерживающие эффективное функционирование первых, установлено следующее множество классов средств защиты информации $\{ A_i \}$:

A_1 — класс средств обеспечения конфиденциальности;

A_2 — класс средств обеспечения целостности;

A_3 — класс средств обеспечения доступности;

A_4 — класс средств контроля (аудита) безопасности;

A_5 — класс средств управления безопасностью.

Задача распределения средств защиты информации из заданного множества $\{S_j\}$ по классам $\{A_i\}$ решается путем логической проверки наибольшего соответствия совокупности признаков целевой направленности средства $(n_{1j},...n_{ij},...n_{Ij})$ классификационным признакам A_i – го класса $(r_{1i},...r_{mi},...r_{mI})$ – $max_{ji}\ (n_{ij} \Lambda\ r_{mi}) => S_j \in A_i$.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

А.В. ПРИБЫЛЬСКИЙ, Т.Г. ТАБОЛИЧ

В условиях рыночной экономики резко обостряется конкурентная борьба между производителями товаров и услуг за потенциальных заказчиков и потребителей. Большинство предприятий РБ пока не занимают лидирующих позиций в этой борьбе на белорусском и зарубежных