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

рынках. Одной из причин такого положения является доступность к информации предприятия, выпускающего конкурентную продукцию. Одним из путей выхода из такой ситуации могли бы стать мероприятия, направленные на усиление информационной безопасности предприятия, т.е. на защиту информации [1]. Защита информации на любом предприятии может быть представлена в виде трех уровней:

1. Защита от конкурентов технико-экономических показателей выпускаемой продукции или научно-исследовательских и опытно-конструкторских разработок, в особенности в перспективных направлениях.

2. Защита внутренней текущей информации предприятия, в том числе данных о себестоимости продукции, складских запасах, наличии технических проблем.

3. Защита информации или данных, которые в том или ином виде присутствуют в выпускаемых изделиях.

Первых два уровня относятся к организационно-техническим мерам обеспечения безопасности, и их реализация сводится в основном к следующим действиям [1]:

- организация пропускного режима и службы безопасности,
- отбор работников при приеме на работу,
- заключение контрактов с работниками, в которых отражается ответственность за передачу информации третьим лицам,
- защита информации в локальной вычислительной сети (ЛВС) предприятия; введение в штат сотрудников, отвечающих за безопасность информации внутри сети.

К третьему уровню защиты информации может относиться защита технологии изготовления изделия (например, микросхемы), которая может быть восстановлена при анализе изделия, а также защита информации, хранящейся в самом изделии. Примером изделий, содержащих нуждающуюся в защите информацию, являются выпускаемые НИРУП "ЦНИИТУ" электронные пластиковые карты (ЭПК). В настоящее время НИРУП "ЦНИИТУ" постоянно наращивает выпуск телефонных ЭПК, освоена первая опытная партия банковских ЭПК, планируется освоение ЭПК для других применений — в качестве пропусков для проходных, автостоянок, для автоматизации выдачи зарплаты на предприятиях и т.д. Важнейшим техническим показателем и необходимым условием востребованности на рынке для телефонных ЭПК является защищенность их от несанкционированной перезарядки, для банковских ЭПК — их защищенность от несанкционированного доступа к содержащимся в ЭПК платежным ресурсам. По данному показателю ЭПК НИРУП "ЦНИИТУ" соответствуют современному научно-техническому уровню [2].

Литература

1. Тимченко И.М. Организационно-технические меры обеспечения комплексной безопасности предприятия: методология, специальные технические средства//Конспект лекций научно-практического семинара для руководителей предприятий Министерства промышленности Республики Беларусь по теме: "Обеспечение безопасности хозяйственной деятельности предприятия в рыночных условиях" (Минск, 18-19 февраля 2003 года). - Мн.: Институт экономики НАНБ, 2003. – С. 45-49.

2. Вечер Д.В., Прибыльский А.В., Реуцкий В.С., Таболич Т.Г. Сравнение кристаллов пластиковых карт по степени защиты информации//В этом сборнике. – С.

ЗАЩИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТРАНЫ ПРИ РЕГУЛИРОВАНИИ ИНТЕЛЛЕКТУАЛЬНОЙ МИГРАЦИИ

М.В. АЗАРЕНКО, А.Г. ПАЦЕЕВА

Организация защиты информации предполагает наличие целого комплекса разноцелевых разработок, повышающих эффективность управления не только техническими процессами, но и человеческими факторами. С формальной стороны человеческие отношения и в этой области регулируются правовыми нормами, например, законом РБ "О государственных секретах". Законодательство РБ предусматривает защиту большого набора разнообразных видов тайн, которые объединяются общей категорией — конфиденциальностью [1]. Разрабатываются основные организационные принципы защиты информационных ресурсов страны.

При такой разработке целесообразно учесть один из важных источников утечки информации - миграцию научных кадров [2]. Действительно, основными создателями научного и научно-технического информационного продукта являются научные кадры. Результаты научной деятельности, как правило, принадлежат ученому или научному коллективу, их создавшему. В свою очередь, государство заинтересовано в том, чтобы практическая реализация этих результатов осуществлялась в пределах страны, где информационный продукт был создан. Правовое регулирование вопросов собственности на ту или иную информацию заложено в патентном праве. С другой стороны, большое количество информации, идей, разработок, технологических нововведений до официального оформления прав собственности принадлежат их создателям. В силу того, что человек считает более выгодным для себя реализовать свои инновации и права на них в условиях другой страны, эти информационные ресурсы теряются для стран-доноров. Для стран с переходной экономикой, какой является Республика Беларусь, это создаёт проблемную ситуацию — чем интереснее разработки ученого для мировой науки или для иностранных компаний, тем выше вероятность того, что он уедет в другую страну, с более благоприятными социально-экономическим условиями. Страна в этом случае терпит не только информационные, но и прямые