XXXI Неделя науки СПбГПУ. Материалы межвузовской научной конференции. Ч. VI: С.92-93, 2003.

УДК 004.7

А.Д. Воронов (6 курс, каф. АиВТ), Л.К. Птицына, д.т.н., проф.

МЕТОДЫ И СРЕДСТВА ОПРЕДЕЛЕНИЯ ЭФФЕКТИВНОСТИ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к современным системам защиты информации, предъявляемые со стороны заказчиков и продиктованные сложившейся жизненной ситуацией, очень высоки. Современная система защиты информации должна решать множество сложных задач. При этом многие задачи должны выполняться непрерывно, следовательно, без параллелизма никак не обойтись. В связи с этим современные системы защиты должны строиться на базе быстродействующих программно-аппаратных средств. В настоящее время, к сожалению, не применяются стандартные методики анализа защищенности автоматизированных систем обработки данных (АСОД).

Наиболее часто используются неформальные классификационные подходы. При их реализации осуществляется категорирование: нарушителей (по целям, квалификации и доступным вычислительным ресурсам); информации (по уровням критичности и конфиденциальности); средств защиты (по функциональности и гарантированности реализуемых возможностей) и т.п. Примерами классификационных методик, получивших широкое распространение, могут служить разнообразные критерии оценки безопасности информационных технологий (ИТ), принятые во многих странах в качестве национальных стандартов, устанавливающие классы и уровни защищенности.

Очевидно, что возникает противоречие между возможностями современных подходов и требованиями к эффективности комплексных систем защиты информации. Для многих специализированных средств защиты существуют формальные модели для анализа качества их функционирования. Для комплексных систем модели нуждаются в модификации. Известные подходы к определению эффективности комплексных систем защиты информации не учитывают динамических характеристик их компонент. В связи с этим возникает объективная необходимость в развитии формальных подходов к проектированию, построению, исследованию и сопровождению комплексных систем защиты информации.

Традиционно для формального описания систем защиты применяется модель защиты с полным перекрытием, в которой рассматривается взаимодействие “области угроз”, “защищаемой области” и “системы защиты”.

При построении модели определяются:

$T = \{t_i\}$- множество угроз безопасности; $O = \{o_i\}$ - множество объектов (ресурсов) защищенной системы; $M = \{m_i\}$ - множество механизмов безопасности АС

Подобная множественная модель не отражает связей между объектами системы. Механизмы безопасности рассматриваются изолированно, а не в рамках единой системы. Данная модель не учитывает информацию о временных характеристиках развития угрозы и функционирования механизма защиты.

В процессе развития модели предусматривается введение еще двух элементов: V – набор уязвимых мест, определяемым подмножеством декартова произведения T*O: $v_k = \{t_i, o_i\}$ и B – набор барьеров, определяемый декартовым произведением V*M: $bi = \{t_i, o_i, m_k\}$.

Рассматриваемая модель образуется набором множеств <T, O, M, V, B>, описывающих систему защиты с учетом наличия в ней уязвимостей.

Механизмами защиты обеспечивается лишь некоторая степень сопротивляемости угрозам. Поэтому в качестве характеристик элемента набора барьеров $bi = \{t_i, o_i, m_k\}$, $bi \in$ B рассматривается набор $\langle P_\ell, L_\ell, R_\ell \rangle$, где $\langle P_\ell \rangle$ - вероятность появления угрозы, , L_ℓ - величина

ущерба при удачном осуществлении угрозы в отношении защищаемых объектов; R_ℓ - степень сопротивляемости механизма защиты m_k , характеризующаяся вероятностью его преодоления.

Тогда прочность барьера $bi = \{t_i , o_i , m_k\}$, характеризуется величиной остаточного риска, определяемого по формуле:

$Risk_i = P_\ell L_\ell (1 - R_\ell)$

Для определения величины защищенности S используется следующая формула:

$$S = 1 / \sum_{(\forall b_k \in B)} P_k L_k (1 - R_k\} ,$$

где $P_k , L_k \in (0.1)$, $R_k \in [0.1)$.

Представленный вариант определения риска ориентируется на идеальное функционирование системы защиты в условиях отсутствия угроз и не учитывает фактор изменения вероятностей во времени.

В докладе предлагается формальный подход, позволяющий получить количественные оценки эффективности комплексных систем защиты информации с учетом динамических характеристик систем защиты информации (ЗИ), функционирующих в условиях появления угроз. Характеристики, отражающие степень проявления основных свойств системы ЗИ, выводятся в результате преобразования моделей процессов функционирования в условиях параллельной и асинхронной обработки. Модели процессов строятся в базисе классов защищенности АСОД.