ИЕРАРХИЧЕСКАЯ СТРУКТУРА КОМПЛЕКСА МОДЕЛЕЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОРГАНИЗАЦИИ

Яхонтов Иван Владимирович
Финансовый университет при Правительстве РФ, Москва, аспирант

Введение

Насколько важна любая информация, относящаяся к бизнесу понятно многим. Пользуясь собранной и обработанной информацией, можно успешно конкурировать на своем рынке и захватывать новые. Информация помогает в поиске партнеров и способствует четкому определению позиции по отношению к ним.

Кроме того, при переходе к рыночной экономике информация становится товаром и должна поэтому подчиняться специфическим законам товарно-рыночных отношений. В этих условиях проблема защиты информации весьма актуальна и для организаций любой формы собственности.

Вопросы безопасности - важная часть концепции внедрения новых информационных технологий во все сферы жизни общества. Широкомасштабное использование вычислительной техники и телекоммуникационных систем в рамках территориально-распределенной сети, переход на этой основе к безбумажной технологии, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости.

Системный подход обеспечивает адекватную многоуровневую защиту информации, рассматриваемую как комплекс организационно-правовых и технических мероприятий. Кроме того, при реализации механизмов защиты должны использоваться передовые, научно обоснованные технологии защиты, обеспечивающие требуемый уровень безопасности, приемлемость для пользователей и возможность наращивания и модификации СЗИ в дальнейшем.

Следовательно, при моделировании информационной системы (ИС) предприятия необходимо учитывать угрозы защиты информации и методы противодействия угрозам. Для этого следует разработать модель системы защиты информации, отвечающую определенным требованиям в зависимости от пот-

ребностей ИС. Для этого разумно будет использовать системный подход, анализ существующих систем и их недостатки.

Анализ подходов к моделированию систем защиты информации показал, что ни одна из представленных моделей не удовлетворяет в полной мере основным критериям. Таким образом, анализ моделей средств защиты информации показывает, что ни один из подходов в полной мере не отвечает предъявляемым требованиям. Модели в основном используются на этапе эксплуатации и сопровождения. Также некоторые модели используются и на этапе проектирования ИС, но только для получения частных оценок уровня защищенности ИС.

Разработка комплекса моделей

Для решения всех задач поставленных перед разрабатываемой моделью СЗИ организации, предлагается реализовывать её в виде комплекса моделей. Архитектура разработанного комплекса моделей представляет собой иерархическую структуру, отображенную на рисунке 1.

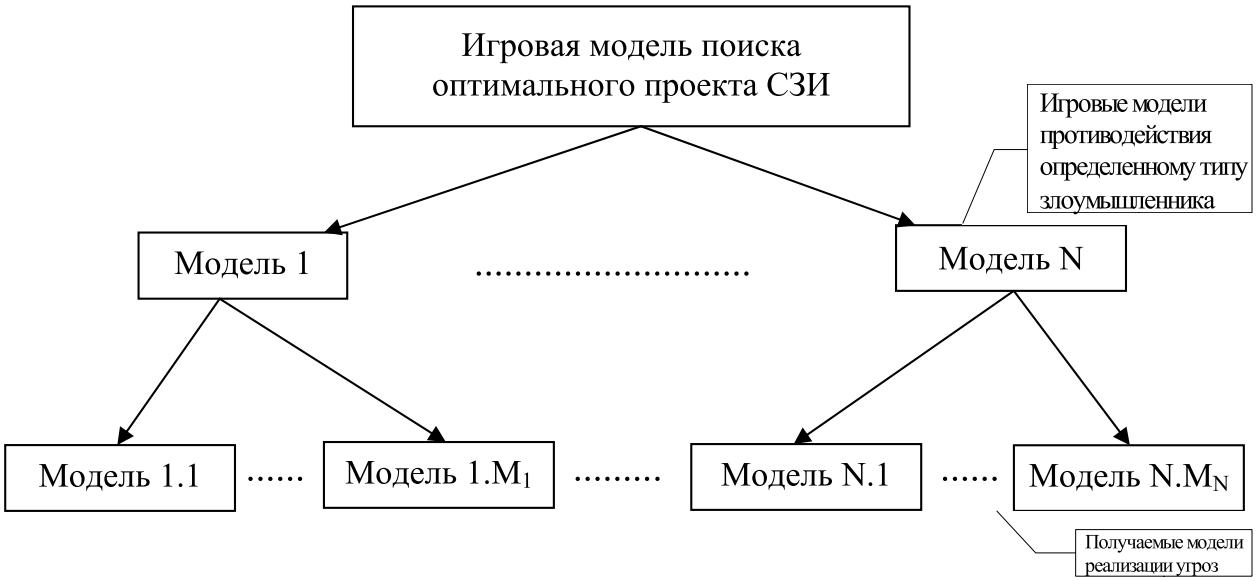

Рис. 1. Иерархическая структура комплекса моделей

Во главе иерархии находится игровая модель поиска оптимального проекта. Исходными данными для данной модели являются показатели обобщенных рисков при противодействии определенному типу злоумышленника и вероятности атаки со стороны того или иного типа злоумышленника. Вероятности атаки должны быть определены отдельно, а показатели обобщенных рисков

поставляют модели, лежащие на среднем уровне иерархии - игровые модели противостояния определенному типу злоумышленника, для которых, в свою очередь, исходными данными являются риски, связанные с реализацией злоумышленником той или иной угрозы, и вероятности того, что злоумышленник будет пытаться осуществить именно эту угрозу. Вероятности нацеленности злоумышленника на реализацию угрозы определяются отдельно, а значения рисков поставляются моделями низшего уровня - полумарковскими моделями реализации угроз.

Разработка модели злоумышленника

Модель исследования оптимальности проекта системы защиты информации предполагает построение модели злоумышленника. Как известно злоумышленники могут быть разных типов. Они могут быть внутренними и внешними, они могут отличаться по уровню подготовки, по уровню оснащения, по целям, которые они перед собой ставят и т.д. Следовательно, необходимо разработать модель злоумышленника, которая формально описывала бы все разнообразие существующих типов злоумышленников.

В рамках описанного комплекса моделей для исследования оптимальности проекта системы защиты информации – модель злоумышленника представляет собой множество

$M=\{\{T\}, \{M^{param}\}, P_k\}$,

где: {T} - множество угроз доступных злоумышленнику. При этом элемент T из множества {T} представляет собой следующее

T;={Pт, {VI}, {E}},

где: Pт - вероятность выбора данной угрозы злоумышленником для эксплуатации; {VI} - множество уязвимостей системы защит информации, причем элемент Vlj из множества {VI} представляет собой следующее

$Vlj = \{P_{init}, S_{param}\}$,

где: P_{init} - вероятность инициализации; S_{param} - множество требований к злоумышленнику. {E} — множество переходов между уязвимостями защиты информации, причем элемент Ej из множества {E} представляет собой следующее

$Ei=\{ P_i^{перех}, P_i^{усп}, \mu_i, \sigma_i \}$,

где: $P_i^{перех}$ - вероятность выбора пути по данному переходу; $P_i^{усп}$ - вероятность успеха; μ_i, σ_i - параметры логнормального закона распределения вероятности пребывания в предыдущем состоянии при выборе пути по данному переходу; S_{param} - множество требований к злоумышленнику. $\{M_{param}\}$ - множество

параметров злоумышленника; P_k — вероятность столкновения системы защиты именно с данным типом злоумышленника.

Заключение

В статье приведен сравнительный анализ различных моделей СЗИ, выявлены основные плюсы и минусы каждой. Представлены рекомендации по созданию архитектуры СЗИ. Даны рекомендации по созданию модели действий злоумышленника для получения оценки эффективности СЗИ и поиска возможных путей ее улучшения.

Список источников

1. Герасименко В.А, Малюк А.А. Основы защиты информации / В.А. Герасименко, А.А. Малюк - М.: Московский Государственный Инженерно-физический институт (технический университет), 1997.

2. Кельтон В., Лоу А. Имитационное моделирование. Классика CS. / Пер. с англ. / В. Кельтон, А. Лоу - 3-е изд. - СПб.: Питер; Киев: Издательская группа BHV, 2004. 847 с.

3. Арьков П.А. Подход к проектированию системы защиты информации автоматизированной системы // XI Региональная конференция молодых исследователей Волгоградской области: тезисы докладов / ВГТУ Волгоград 2006, с. 198.