О. В. Л у к и н о в а Москва, ИПУ РАН)**. О семантической формализации понятий процесса проектирования систем защиты.**

В докладе рассматривается семантический подход к проектированию комплексной системы защиты (КСЗ) ИС от компьютерных вторжений. В процессе разработки КСЗ решаются следующие задачи: 1) формирование и согласование целей, стратегий, критериев защиты и ограничений, накладываемых бизнесом; 2) формирование и согласование предполагаемых угроз; 3) формирование требований к КСЗ; 4) выбор вариантов средств защиты, удовлетворяющих требованиям и функционально-стоимостным критериям.

Автоматизированное решение этих задач требует представления процесса проектирования в некотором формализованном виде. Для этого был использован аппарат семантических сетей в виде онтологий. Структура рассматриваемой онтологии $O = \langle O_B, O_{C_i} \rangle$. Здесь O_B — онтология верхнего уровня, O_{C_i} — онтологии, детализирующие понятия, входящие в O_B. Каждая из онтологий описывается формализмом $O = \langle C, R, F \rangle$. Здесь $C = \{C_1, C_2, \ldots, C_n\}$ — конечное непустое множество понятий предметной области.

В ходе анализа были выделены следующие концепты.

1. Бизнес-модель — множество бизнес-процессов, реализованных в сетевой среде, выступающая в качестве объекта защиты.

2. Модель угроз, т. е. совокупность условий и факторов, которые могут привести к возможному нарушению уровня безопасности бизнес-процессов.

3. Комплексная система защиты {КСЗ} представляет собой некоторую совокупность защитных средств.

4. Средство защиты {СЗ} — программно-аппаратный продукт, функции безопасности которого обеспечиваются набором тех или иных защитных механизмов.

5. Защитный механизм включает в себя совокупность методов защиты, реализующих какое-либо свойство безопасности, соответствующее определенному уровню критериев.

6. Функциональные требования к КСЗ: $R = \{R_1, R_2, \ldots, R_m\}$, $R_i \subseteq C \times C$, $R = R_T \cup R_P \cup R_A \cup R_{Atr}$ есть конечное множество бинарных отношений, где R_T — антисимметричное, транзитивное, нерефлексивное бинарное отношение наследования, задающее таксономию на множестве понятий C; R_P — транзитивное, бинарное отношение партономии (часть-целое); R_A — конечное множество ассоциативных отношений между понятиями C; R_{Atr} — конечное множество атрибутов понятий C и отношений R; F — конечное множество описательных интерпретаций понятий.

Онтология $O_B = \langle C_B, R_A \rangle$ представлена на рис. Чтобы подчеркнуть иерархическую структуру $\forall\ C_i \in C_B$, над ними вводится отношение $R_P = \{$Включают в себя$\}$.

Каждый из концептов C_B представляется онтологиями O_{C_i}. {Бизнес-модель} включает в себя: а) среду функционирования, т. е. платформенные и прикладные компоненты, которая содержит уязвимости, объекты и каналы атак; б) бизнес-логику (виды деятельности и их взаимосвязь), определяющую ограничения, накладываемые на защиту в интересах эффективного исполнения бизнес-процессов, и критерии защиты. {Модель угроз} содержит в себе иерархии концептов {Объект атаки}, {Уязвимость}, {Канал атаки}, {Возможности нарушителя}, {Потенциально опасные атаки}. Класс {Требования} содержит в себе функциональные требования к системе защиты. Класс {КСЗ} представляется таксономией СЗ, каждое из которых реализуется совокупностью защитных механизмов.

Представленная модель может быть использована для организации процедуры компьютерного проектирования КСЗ.

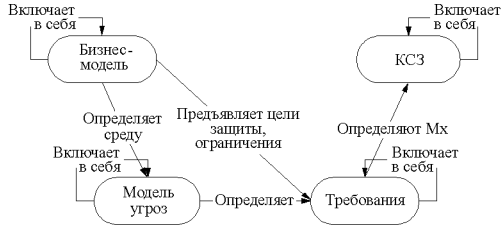

Рис. Онтология верхнего уровня O_B