УДК 004
ББК 32.81

МОДЕЛЬ СБОРА ИНФОРМАЦИИ О КОРПОРАТИВНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

А.А. Бешта

Дополнен существующий подход к описанию корпоративной вычислительной сети (КВС), предложена формальная модель КВС, разработана структура для представления информации о КВС, описана схема сбора и хранения информации в реальной системе.

Ключевые слова: *корпоративная вычислительная сеть, формальное описание, структура представления информации, агент сбора информации.*

Как показывает практика, размер корпоративных вычислительных сетей (КВС) постоянно растет, увеличивается количество технологий, используемых при обработке информации, увеличивается число рабочих станций и пользователей. В связи с этим усложняется процесс анализа защищенности КВС.

Все множество компонентов, входящих в КИС, можно разделить на четыре класса: аппаратный, программный, организационный и правовой.

К аппаратному уровню относится физическая инфраструктура КВС, которая обеспечивает функционирование верхних уровней КВС. Она включает узлы КВС и сетевое оборудование, связывающее узлы между собой в единую структуру.

К программному уровню относится программное обеспечение (ПО), установленное на узлах КВС. Можно выделить следующие уровни ПО: операционной системы, драйвера, пользовательские приложения, а также программные средства защиты КВС.

На организационном уровне представлены бизнес-процессы и информационные потоки, которые основываются на некоторых взаимосвязанных элементах КВС программного и аппаратного уровней.

На правовом уровне представлены нормативно-правовые документы, связанные с КВС.

Для анализа защищенности такую классификацию необходимо дополнить элементами, которые в нее не входят, а именно: показатели защищенности КВС, активы КВС, уязвимости.

Структура КВС приведена на рисунке 1.

Формально КВС рассматривается следующим образом:

$$S = \{E^S, LS\}, \quad (1)$$

где E^S – множество элементов КВС;

LS – множество связей между элементами КВС, $L_A^S \subseteq E^S \times E^S$.

Каждый элемент КВС E^S представляет собой описание с помощью некоторых свойств этого элемента:

$$E_j^S = \left\{P_{jk}^S\right\}, \quad (2)$$

где P_{jk}^S – свойство элемента.

При этом следует учитывать, что свойством одного объекта также может быть объект, обладающий другими свойствами. Отсюда:

$$P_{jk}^S = \left\{T_{vk}^S, f_{jk}^S\right\}, \quad (3)$$

где T_{vk}^S – тип свойства объекта, может принимать значения $T_{vk}^S = P_{jk}^S \vee E_{,}^S$

f_{jk}^S – обязательность наличия у объекта E_k^S свойства P_{jk}^S.

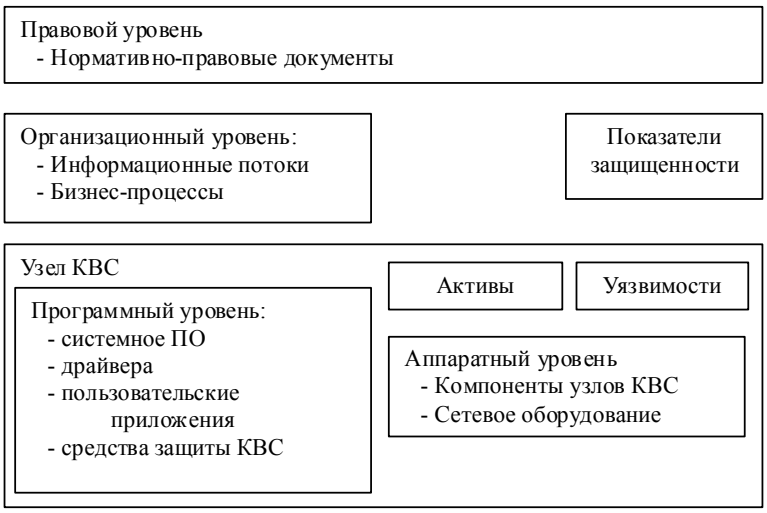

Рис. 1. Структура КВС

Связи между элементами КВС L^S представляются следующим образом:

$$L^S = L^S_{is-a} \cup L^S_{part-of},$$
$$L^S_{is-a} \cap L^S_{part-of} = \mathrm{O}, \qquad (4)$$

где L^S_{is-a} – отношение категоризации между объектами КВС;

$L^S_{part-of}$ – отношение принадлежности между объектами КВС.

Множество элементов КВС E^S включает подмножества элементов особых типов:

- множество активов КВС $E^S_A, E^S_A \subseteq E^S$;
- множество уязвимостей элементов КВС $E^S_V, E^S_V \subseteq E^S$;
- множество узлов КВС $E^S_H, E^S_H \subseteq E^S$;
- множество компонентов КВС E^S_P, $E^S_P \subseteq E^S$;
- множество средств защиты КВС E^S_{SC}, $E^S_{SC} \subseteq E^S$.

Информационный актив КВС представляет собой информацию, подлежащую защите, и описывается следующим образом:

$$A_k = \left\{A_k^{name}, A_k^{value}\right\}, A_k \in E^S_A, \qquad (5)$$

где A_k^{name} – наименование информационного актива КВС;

A_k^{value} – условная ценность информационного актива КВС.

Пусть средство защиты КВС *SC* – программная система, которая позволяет с некоторой вероятностью закрыть уязвимости других компонентов и защитить активы КВС с использованием информации о других элементах КВС и вычислительных ресурсов узлов КВС. В связи с разнообразием принципов и методов работы компонентов КВС довольно сложно учитывать особенности каждого из них. Поэтому предлагается учитывать общие характеристики *SC*: тип компонента и уязвимости, на который это средство направлено, объем используемых ресурсов узлов КВС, вероятность устранения уязвимости.

Для работы средств защиты требуются следующие ресурсы: процессорное время, память ОЗУ, канал обмена информацией.

Таким образом, *SC* можно описать в следующем виде:

$$SC_i = \{E^S_P, \{\ ^S_{VE_P}\}, p_{SC}, R_{SC_i}\}, \qquad (6)$$

где E^S_P – множество элементов КВС, на которые направлено средство защиты;

$E^S_{VE_P}$ – множество уязвимостей элемента КВС;

R_{SC_i} – ресурсы, необходимые для работы средства защиты;

p_{SC} – вероятность успешного закрытия уязвимостей в элементе КВС E^S_P.

В итоге эффективностью средства защиты является вероятность p_{SC} устранения множества уязвимостей $E^S_{VE_P}$ для компонентов E^S_P при использовании ресурсов R_{SC_i}.

Вычислительные ресурсы R_{SC_i}, требуемые для работы средства защиты, определяются следующим образом:

$$R_{SC_i} = \left\{ r_{SC_i}^{cpu}, r_{SC_i}^{mem}, r_{SC_i}^{net} \right\}, \quad (7)$$

где $r_{SC_i}^{cpu}$ – процессорная нагрузка, вызываемая работой СЗ;

$r_{SC_i}^{mem}$ – объем оперативной памяти, требуемый для работы СЗ;

$r_{SC_i}^{net}$ – пропускная способность сетевого соединения узла КВС, необходимая для работы СЗ.

В соответствии с представленной моделью КВС, структура для хранения знаний может выглядеть следующим образом (рис. 2).

Для наполнения этой информационной структуры предлагается следующая схема сбора информации (рис. 3).

Сервер хранения информации содержит централизованную базу для хранения информации. На каждом компоненте КВС размещается агент сбора информации, который получает необходимые сведения и передает их на сервер хранения.

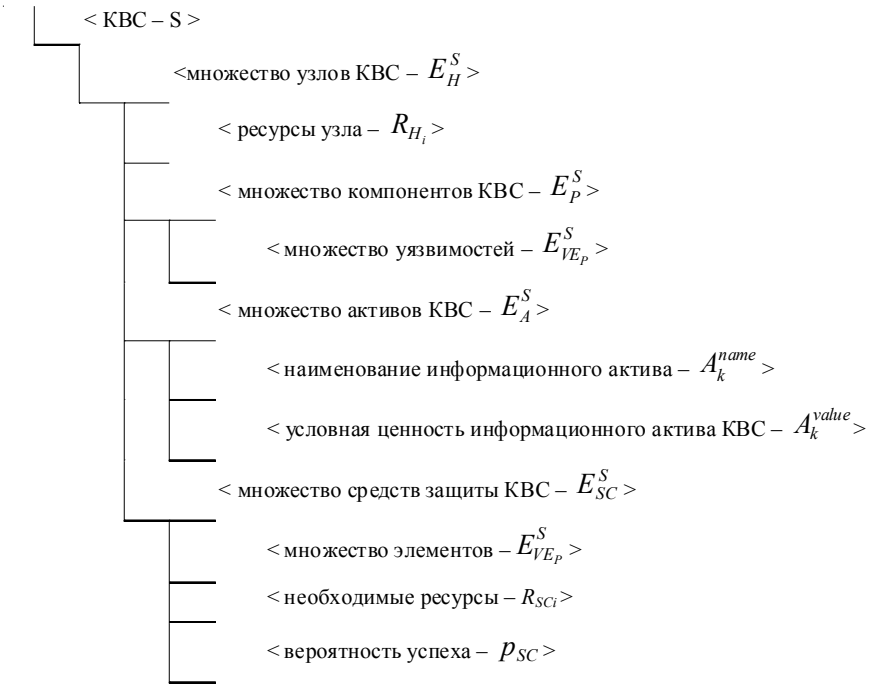

Рис. 2. Структура представления информации о КВС

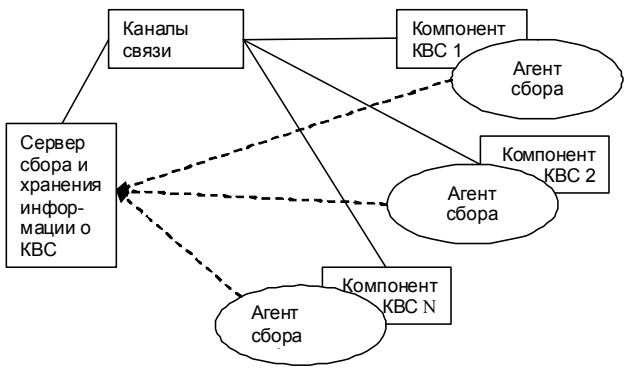

Рис. 3. Схема сбора информации о КВС

Данная модель представления знаний имеет свои плюсы. Во-первых, это возможность представления разнородной информации о характеристиках элементов КВС: технические характеристики, программные компоненты, активы, связи с другими элементами КВС. Возможно отображение информационных потоков в КВС. Помимо этого, модель позволяет учитывать такие характеристики, как стоимость активов, уязвимости компонентов, а отсюда учет возможного ущерба и риска.

THE MODEL OF GATHERING INFORMATION ABOUT CORPORATE COMPUTER NETWORK

A.A. Beshta

Complement the existing approach to the corporate computer network (CCN) description, a formal model of CCN is proposed, the structure of presentation of information about CCN is developed, the schema of gathering and storing of information in real system is described.

Key words: *corporate computer network, formal model, structure of information presentation, gathering information agent.*