УДК 004.056.53

В.В. Коленко, аспирант,
А.В. Нарожный, к.т.н.,
А.Ф. Сафонова, к.т.н.
Одесский национальный политехнический университет

МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ

В.В. Коленко, О.В. Нарожний, Г.Ф. Сафонова. **Математичні моделі та методи процесів захисту інформації.** Моделями процесів захисту інформації в комп'ютерних системах названі такі, які дозволяють визначати (оцінювати) загальні характеристики зазначених систем і процесів. Основне призначення загальних моделей полягає у створенні передумов для об'єктивної оцінки загального стану комп'ютерної системи з точки зору заходи уразливості або рівня захищеності інформації в ній.

V.V. Kolenko, A.V. Narozhny, A.F. Safonova. **Mathematical models and methods of information protection processes.** The general models of processes of information protection in the computer systems are those which allow to determine general descriptions of the indicated systems and processes. The basic purpose of general models is in creation of preconditions for the objective estimation of the general state of the computer system from point of measure of vulnerability or level of information protection in it.

Введение. Современный прогресс в области компьютерных технологий и средств мультимедиа привел к разработке новых методов, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций.

Общими моделями процессов защиты информации в компьютерных системах названы такие, которые позволяют определять (оценивать) общие характеристики указанных систем и процессов.

Назначение общих моделей состоит в создании предпосылок для объективной оценки общего состояния компьютерной системы с точки зрения меры уязвимости или уровня защищенности информации в ней.

Необходимость в таких оценках возникает при анализе общей ситуации с целью выработки стратегических решений при организации защиты информации. [1].

Материал и результаты исследования: Цели защиты информации в системе могут быть представлены как организация оптимального функционирования.

При этом понятие оптимального функционирования может быть сформулировано в соответствии с постановками оптимизационных задач: при заданных ресурсах для обеспечения максимального результата, или обеспечить требуемый результат при минимальных затратах [2].

На рис. 1 приведена общая модель процесса выбора средств защиты информации системы.

В модели использованы следующие обозначения:

C - финансовые средства, которыми располагает противник;

{L}- множество количественных оценок потерь Системы, в случае успешной реализации угроз информации;

{LZ}- множество количественных оценок потерь Системы в случае применения средств защиты информации;

{MR}- множество параметров использования ресурсов Системы;

{P}- множество нарушителей;

T - время, которым располагает атакующая сторона для реализации угроз;

{TS}- технологическая схема функционирования Системы;

{U}- множество угроз информации;

{Z}-множество средств защиты информации;

γ - вектор использования средств защиты информации в Системе.

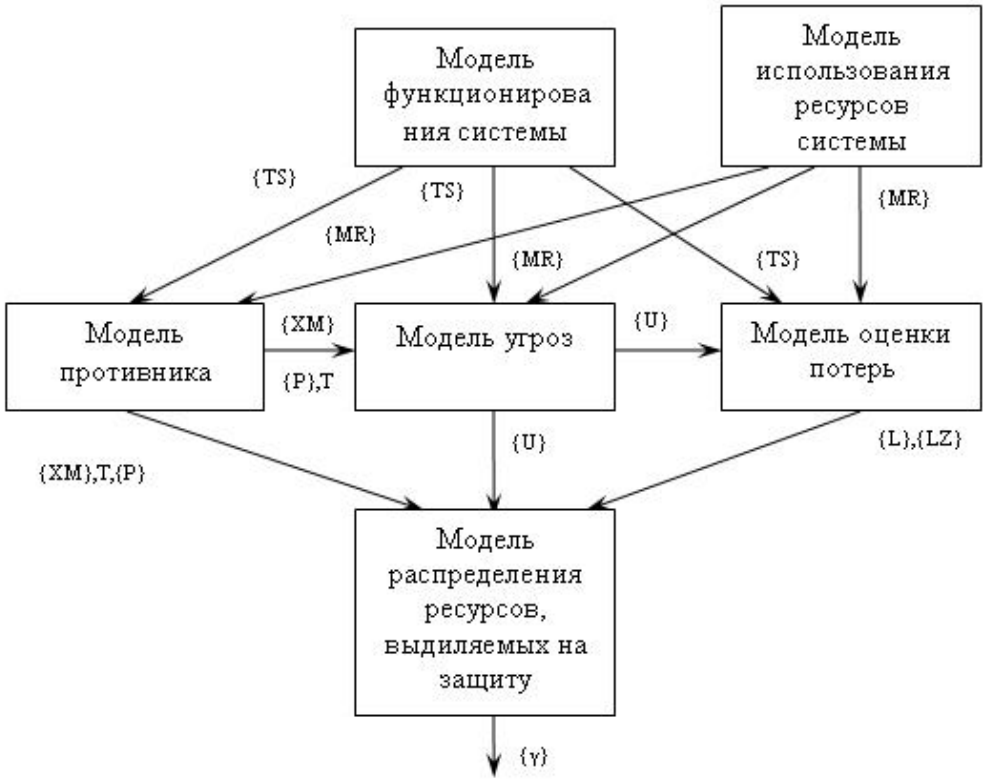

Рис. 1. Общая модель процесса выбора средств защиты информации.

Сформулируем задачи, которые должны быть решены для выбора средств защиты информации системы [2]:

1. Разработать модель функционирования системы и модель использования ее ресурсов.

2. Построить модель вероятного противника, оценить его возможности.

3. Разработать модель угроз информации системы.

4. Разработать модель оценки потерь.

5. Исходя из возможностей противника, а также на основании модели угроз, необходимо построить вероятную модель распределения ресурсов на защиту информации.

Рассмотрим формальное описание каждой из перечисленных моделей. [4]

Модель функционирования системы может быть формально представлена в виде функции:

$$F \rightarrow \{TS\}; \quad (1)$$

где:

{TS}- формальное описание технологии функционирования системы.

В качестве исходных данных функции будет выступать система обработки информации.

Результат указанной функции - формальное описание технологии функционирования системы.

Модель использования ресурсов системы представляет собой функцию:

$$F(\{TS\}) \rightarrow \{MR\}; \quad (2)$$

где:

{MR}- формальное описание ресурсов, используемых системой на различных этапах обработки информации.

Модель противника представляет следующую функцию:

$$F(\{TS\},\{MR\}) \rightarrow (\{P\},C,T,\{XM\}); \quad (3)$$

где:

{P}- множество категорий злоумышленников;

{XM}-множество средств для реализации противником деструктивных действий;

C- финансовые возможности противника;

T- время, которым располагает атакующая сторона.

Модель угроз описывает следующий функционал:

$$F(\{MR\},\{TS\}) \rightarrow \{U\}; \quad (4)$$

где:

{U}- формально описанное множество угроз информации системы.

Модель оценки возможных потерь описывается следующим образом:

$$F(\{TS\},\{MR\},\{U\}) \rightarrow (\{L\},\{LZ\}); \quad (5)$$

где:

{L}- потери системы, вызванные успешной реализацией угроз;

{LZ}- потери системы, вызванные с применением средств зашиты информации.

Модель распределения ресурсов, выделяемых на защиту информации:

$$F(\{U\},\{L\},\{LZ\},\{XM\},\{P\},\{Z\},T,C) \rightarrow (\gamma); \quad (6)$$

где:

{Z}-множество средств защиты информации.

Порядок взаимодействия моделей. На первом этапе производится разработка модели функционирования системы. Результаты этого этапа будут использованы во всех последующих моделях процессов защиты информации. Итогом моделирования является технология функционирования системы.

После получения описания технологии функционирования системы необходимо определить ресурсы системы, то есть определить, какие ресурсы используются системой для решения задач по обработке информации. Далее, необходимо описать схему использования ресурсов. В дальнейшем эта схема необходима для определения возможных объектов атак злоумышленников, а также при формировании каналов утечки информации и т.д.[1]

Следующим этапом является разработка модели противника. Для этого необходимы результаты предыдущих этапов: технология функционирования и схема использования ресурсов.

Указанные данные помогут классифицировать возможного противника, что в свою очередь позволит в дальнейшем построить адекватную систему защиты информации.

Результатом построения модели противника является множество возможных категорий злоумышленников.

После окончания предыдущего этапа формируется модель угроз информации. Исходными данными для моделирования будут технология функционирования системы и схема использования ресурсов.

Результатом этого этапа моделирования есть перечень угроз информации системы, а также способов их реализации.

Каждый элемент перечня должен содержать информацию о категориях злоумышленников, которые могут реализовать указанную угрозу.

Кроме того, должны быть указаны свойства информации, которые будут нарушены в случае успешной реализации угрозы.

После получения указанного перечня, необходимо выполнять построение модели оценки потерь. Для этого нужно для каждой угрозы из перечня провести подсчет оценки возможных потерь, которые может понести система.

Исходными данными для построения такой модели является технология функционирования системы, схема использования ресурсов, а также перечень угроз информации системы. Результатами моделирования выступает перечень возможных потерь.

Вывод. После завершения всех перечисленных выше этапов, выполняется решение задачи выбора средств защиты информации. Результатом является бинарный вектор применения известных средств защиты информации [3].

Итогом, изложенного выше, есть алгоритм решения задачи выбора средств защиты информации.

При построении указанного алгоритма необходимо учесть следующее обстоятельство: ввиду высокой значимости каждого из этапов моделирования, а также высокой цены принятия неверного решения необходимо предусмотреть возможность повторения некоторых этапов моделирования в случае необходимости.

Література

1. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика [Текст] / Г.Ф. Конахович, А.Ю. Пузыренко; – К.: «МК-Пресс», 2006. – 288 с.

2. Конахович, Г. Ф., Защита информации в телекоммуникационных системах [Текст] / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов; – К.: "МК-Пресс", 2005. – 288 с.

3. Дорошко, В.О. Основи комп'ютерної стеганографії. Навчальний посібник для студентів і аспірантів [Текст] / О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчик; – Вінниця: ВДТУ, 2003. – 143с.

4. Горбунов, В.А. Математические методы в теории защиты информации [Текст] / В.А. Горбунов; Московский государственный горный университет. – М.: АМГК, 2004. – 82с.