УДК 004.492.2

АНАЛИЗ И СОВЕРШЕНСТВОВАНИЕ МОДЕЛИ РАСПРЕДЕЛЕНИЯ И ИСПОЛЬЗОВАНИЯ РЕСУРСОВ С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цымбалова А.А, Губенко Н.Е.
Донецкий национальный технический университет

Рассмотрена модель распределения и использования ресурсов, выделяемых на защиту информации, сделан ее анализ. Предложена усовершенствованная модель.

Постановка проблемы

С распространением информационных технологий организации становятся все более зависимыми от информационных систем и услуг, а, следовательно, все более уязвимыми по отношению к угрозам безопасности. Поэтому главной целью любой системы информационной безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, недопущение хищения финансовых средств, утечки, искажения и уничтожения служебной информации. Однако обеспечение необходимого уровня защиты информации задача весьма сложная, требующая для своего решения создания целостной системы организационных мероприятий и применения специфических средств и методов по защите информации [1].

Модели процессов защиты информации являются одними из основных элементов научно-методологического базиса защиты. Основой для их построения являются общие цели (задачи) защиты информации и условия, в которых осуществляется защита. Одним из вопросов, который возникает при решении задачи построения модели системы защиты, является оценка объема ресурсов, необходимых для обеспечения требуемого уровня защиты, и оптимальное их распределение, и именно эти процессы должны быть определяющими [2].

В данной статье для подробного рассмотрения и анализа была выбрана модель распределения и использования ресурсов, выделяемых на защиту информации, предложенная Грездовым Г.Г., так как методы математического моделирования, используемые при построении данной модели, оказывают большую помощь в построении эффективной системы информационной безопасности.

Модель распределения и использования ресурсов, выделяемых на защиту информации

Процесс защиты информации – это процесс взаимодействия угроз, воздействующих на информацию, и средств защиты информации, которые препятствуют их воздействию [4].

На рисунке 1 представлен поэтапный процесс построения модели распределения ресурсов, выделяемых на защиту информации.

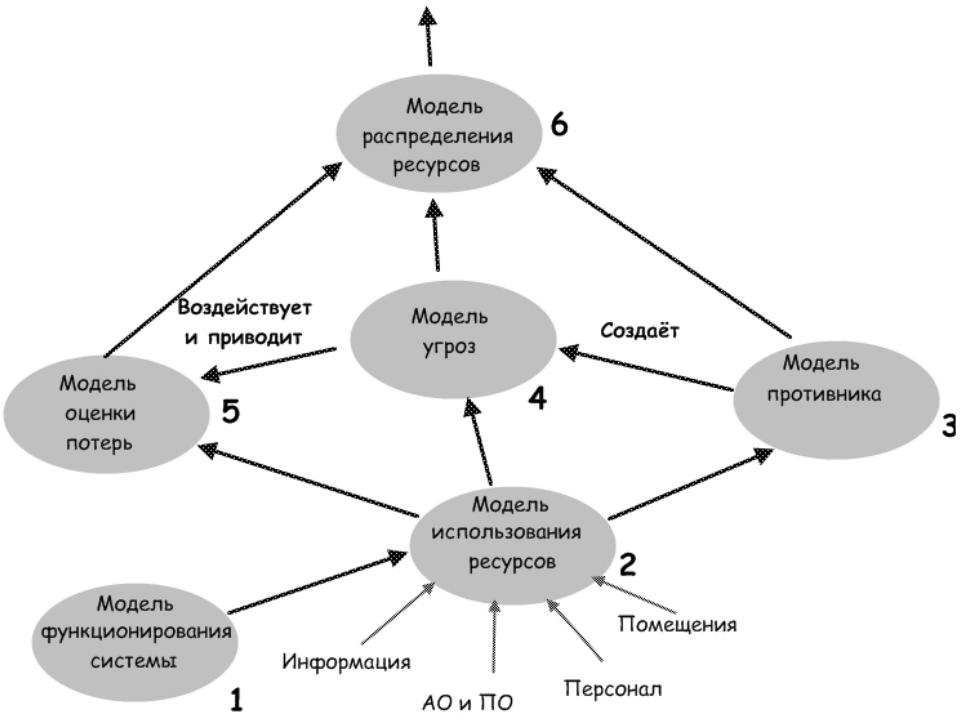

Рисунок 1– Модель распределения и использования ресурсов, выделяемых на защиту информации

Модель распределения и использования ресурсов строится исходя из возможностей противника и защищающейся стороны, на основании модели угроз, а также модели оценки потерь, так как исходя из экономической целесообразности, расходы на средства защиты не должны превышать предполагаемый ущерб от нарушения информационной безопасности [3].

Решение задачи выбора средств защиты информации

Для формирования эффективной комплексной системы защиты информации нужно минимизировать функцию

$$f(y) = \sum_{i=1}^{N} L_i (R_i - \sum_{j=1}^{M} GM_{ij} \cdot \gamma_j) \qquad (1),$$

при следующих ограничениях:

$$\sum_{j=1}^{M} r_j \cdot (C_j + X_j) \le C_d \qquad (2),$$

где N – число угроз информации, L – оценка стоимости потерь в случае реализации каждой из угроз, R – максимальные возможности атакующей стороны по реализации угроз, M – число существующих средств защиты, GM – набор показателей эффективности средств защиты информации, r – вектор применения средств защиты информации защищающейся стороной (r_j=0, если i-тое средство защиты информации не используется; в противном случае коэффициент равен 1), C_d – финансовые средства, которые могут выделены защищающейся стороной для осуществления защиты информации, X_j – потери, связанные со снижением производительности системы, в случае использования средства защиты информации.

В данной формуле рассматривается суммарный риск, который характеризует опасность, которой может подвергаться система и зависит от показателей ценности ресурсов и вероятностей нанесения ущерба ресурсам (выражаемых через вероятности реализации угроз для ресурсов (информация, аппаратное и программное обеспечение, персонал, помещения)). Поэтому вычисляется сумма потерь, которые понесет система в случае реализации каждой из угроз.

Методика определения суммы потерь состоит в определении размера потерь, которые понесет система в случае реализации отдельной угрозы и умножения полученного значения на вероятность проявления угрозы.

При определении вероятности проявления дестабилизирующих факторов необходимо учесть следующие обстоятельства:

1) Неизвестно, какие средства, которыми располагает противник, могут быть использованы для нанесения ущерба системе.

2) Необходимо определить состав средств, используемых для защиты информации в системе.

Решение задачи состоит в отыскании значений вектора r.

Построение вектора r заключается в следующем: $r_i = 1$, если финансовые возможности противника превышают стоимость хотя бы одного из средств нападения, способного вызвать дестабилизирующий фактор. В противном случае элемент вектора будет равен 0 [3].

Анализ методики выбора средств защиты информации

1) Методика не рассматривает вопрос противодействия системы защиты информации распределенным атакам. Распределенная атака представляет собой действие или последовательность связанных между собой действий противника, которые используют уязвимости объекта защиты.

2) Методика не учитывает тот факт, что потери, связанные со снижением производительности, вызванные использованием средств защиты информации, зависят от распределения средств защиты информации. Таким образом, финансовые средства, которые могут быть выделены защищающейся стороной для осуществления защиты информации, также зависят от распределения средств защиты информации и могут быть получены после проведения специальных вычислений.

3) Методика не дает возможность выбора между разными вариантами построения комплексной системы защиты информации.

4) Методика не обеспечивает единый подход формирования для защиты информации, которая составляет государственную, военную или коммерческую тайну.

Совершенствование модели распределения и использования ресурсов, выделяемых на защиту информации

Таким образом, как показывает анализ, для построения эффективной комплексной системы защиты информации предполагается внести следующие изменения:

1) Выявить противодействие системы защиты распределенной атаке, то есть при формировании модели угроз предварительно построить *модель распределенной атаки*;

2) Определить уязвимость объекта защиты, так как для оценки рисков информационной системы защищенность каждого ценного ресурса определяется не только при помощи анализа угроз, действующих на конкретный ресурс, а при помощи уязвимостей, через которые данные угрозы могут быть реализованы, то есть при формировании модели распределенной атаки предварительно построить *модель уязвимостей.*

На рисунке 2 представлена усовершенствованная модель формирования комплексной системы защиты информации.

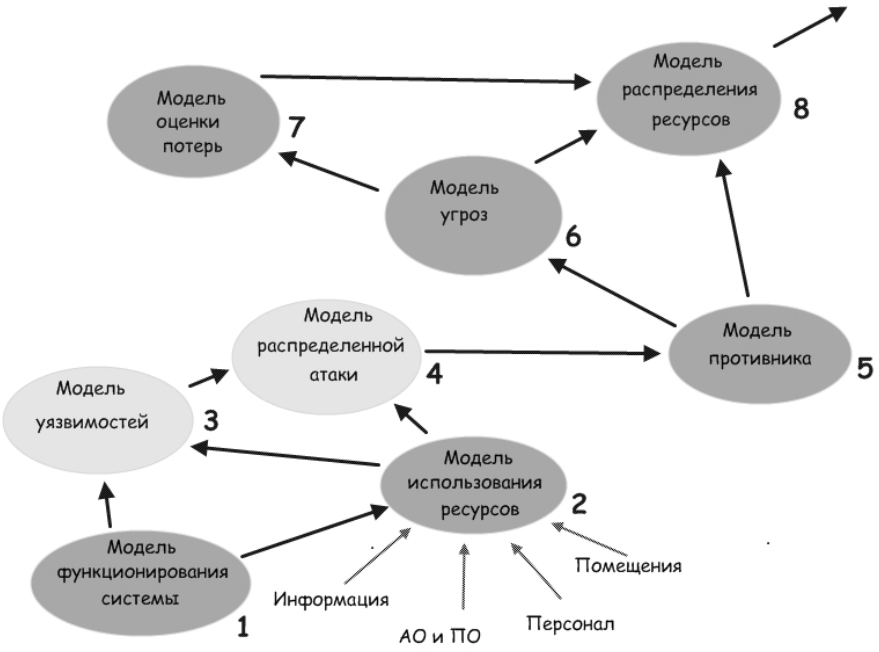

Рисунок 2 – Усовершенствованная модель распределения и использования ресурсов

Выводі

Предлагаемые изменения позволяют усовершенствовать модель и снизить вероятность реализации угроз конфиденциальности, целостности и доступности данных.

Список литературы

1. Цымбалова А.А, Губенко Н.Е. Анализ модели использования ресурсов с точки зрения информационной безопасности. Информационные управляющие системы и компьютерный мониторинг — 2011 / Материали II всеукраинской научно-технической конференции студентов, аспирантов и молодых учёных. — Донецк, ДонНТУ — 2011, с. 292-295.

2. Корнеев Д.В. Обобщенная модель системы защиты ресурсов распределения вычислительной сети [Электронный ресурс] — Режим доступа к статье: http://admin.smolensk.ru/virtual/expo/html/tesis.htm

3. Грездов Г. Г. Способ решения задачи формирования комплексной системы защиты информации для автоматизированных систем 1 и 2 класса [Текст] / Г. Г. Грездов // (Препринт/ НАН Украины. Отделение гибридных управляющих систем в энергетике ИПМЭ им. Г. П. Пухова НАН Украины; № 01/2005) – Киев : ЧП Нестреровой, 2005. – С. 66.

4. Грездов Г. Г. Модифицированный способ решения задачи формирования эффективной комплексной системы защиты информации автоматизированной системы / Г. Г. Грездов; монография. – К.: ДУІКТ, 2009. – 32 с.

Получено 12.09.2011