УДК 004.492.2

МОДЕЛЬ РАСПРЕДЕЛЕНИЯ И ИСПОЛЬЗОВАНИЯ РЕСУРСОВ, ВЫДЕЛЯЕМЫХ НА ЗАЩИТУ ИНФОРМАЦИИ

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

Рассматривается модель распределения и использования ресурсов, выделяемых на защиту информации, а также постановка задачи выбора средств защиты информации. Сделан анализ рассмотренной модели. 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.

Модели процессов защиты информации являются одними из основных элементов научно-методологического базиса защиты. 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 [1].

В данной статье для подробного рассмотрения и анализа была выбрана модель распределения и использования ресурсов, выделяемых на защиту информации, основанная на методах математического моделирования, которые оказывают большую помощь в построении эффективной системы информационной безопасности. Во-первых, именно с их помощью можно доказать, что вложение средств в систему защиты информации действительно экономит деньги предприятия, а во-вторых, в условиях ограниченности ресурсов, с помощью этих методов можно выбрать наиболее оптимальный комплекс средств защиты, а также смоделировать, насколько созданная система защиты окажется эффективной в борьбе против наиболее распространенных угроз.

Модели процессов защиты информации

Общие модели процессов защиты – модели, которые позволяют определять общие характеристики указанных систем и процессов в отличии от моделей локальных и частных, которые обеспечивают определение некоторых локальных или частных характеристик систем.

Общая модель процесса защиты информации

Данная модель отображает процесс защиты информации как процесс взаимодействия угроз, воздействующих на информацию, и средств защиты информации, которые препятствуют их воздействию

Обобщенная модель системы защиты информации

Эта модель системы защиты отображает основные процессы, осуществляемые в системе с целью рационализации процессов защиты. Указанные процессы в самом общем виде могут быть представлены как процессы распределения и использования ресурсов, выделяемых на защиту информации.

Модель общей оценки угроз информации

Эта модель оценивает не просто угрозы, а еще и потери, которые могут иметь место при появлении различных угроз. Данные модели важны еще и тем, что именно на них в наибольшей степени были выявлены те условия, при которых такие оценки могут быть адекватны реальным процессам защиты информации

Модели анализа систем разграничения доступа к ресурсам информационной системы

Модели этого класса предназначены для обеспечения решения задач анализа и синтеза систем разграничения доступа к различным видам ресурсов и прежде всего к массивам данных или полям. Выделение этих моделей в отдельный класс обусловлено тем, что механизмы разграничения доступа относятся к числу наиболее существенных компонентов системы защиты информации, от эффективности функционирования которых, в значительной мере зависит общая эффективности информации [2].

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 [3].

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

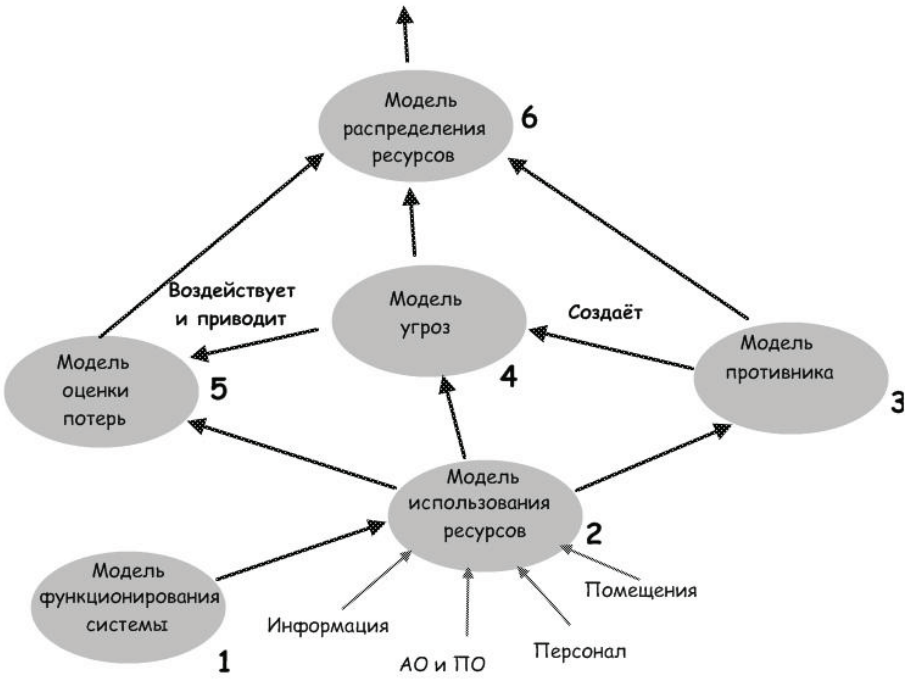

Рисунок 1. Модель распределения и использования ресурсов, выделяемых на защиту информации

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 [4].

Методика выбора средств защиты информации

Для формирования эффективной комплексной системы защиты информации нужно минимизировать функцию (1) при ограничениях (2):

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

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

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_{ij} – 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_j =0 , если финансовые возможности противника превышают стоимость хотя бы одного из средств нападения, способного вызвать дестабилизирующий фактор. В противном случае элемент вектора будет равен 0 [5].

6

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

На основе проведенного анализа, для построения эффективной комплексной системы защиты информации предполагается внести следующие изменения:

1. 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. Алгоритм оценки показателя уязвимости обычно реализует перебор каким-либо образом всех возможных маршрутов нарушителей, расчет значений показателя для каждого маршрута, определение наиболее уязвимых маршрутов, точек перехватов нарушителей. Результатом этапа станет множество уязвимостей компонентов.
2. Выявить противодействие системы защиты распределенной атаке, то есть при формировании модели угроз предварительно построить модель распределенной атаки. Результатом моделирования станет полный перечень возможных атак.

Распределенная атака состоит из четырех этапов:

1. *Стадия рекогносцировки*. На этой стадии нарушитель старается получить как можно больше информации об объекте атаки, на основе которой планируется дальнейшие этапы атаки. Он включает такие действия как определение сетевой топологии, типа и версии операционной системы атакуемого узла, а также доступных сетевых и иных сервисов и т.п. Эти действия реализуются различными методами.
2. *Стадия вторжения в ИС.* На этом этапе нарушитель получает несанкционированный доступ к ресурсам тех хостов, на которые совершается атака.
3. *Стадия атакующего воздействия на ИС.* Данная стадия атаки направлена на достижение нарушителем тех целей, для которых и предпринималась атака. При этом атакующий может также осуществлять действия, которые могут быть направлены на удаление следов его присутствия в ИС. Обычно это реализуется путем удаления соответствующих записей из журналов регистрации узла и других действий, возвращающих атакованную систему в исходное, «предатакованное» состояние.
4. *Стадия дальнейшего развития атаки*. На этом этапе выполняются действия, которые необходимы для продолжения атаки на другие объекты ИС [5].

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

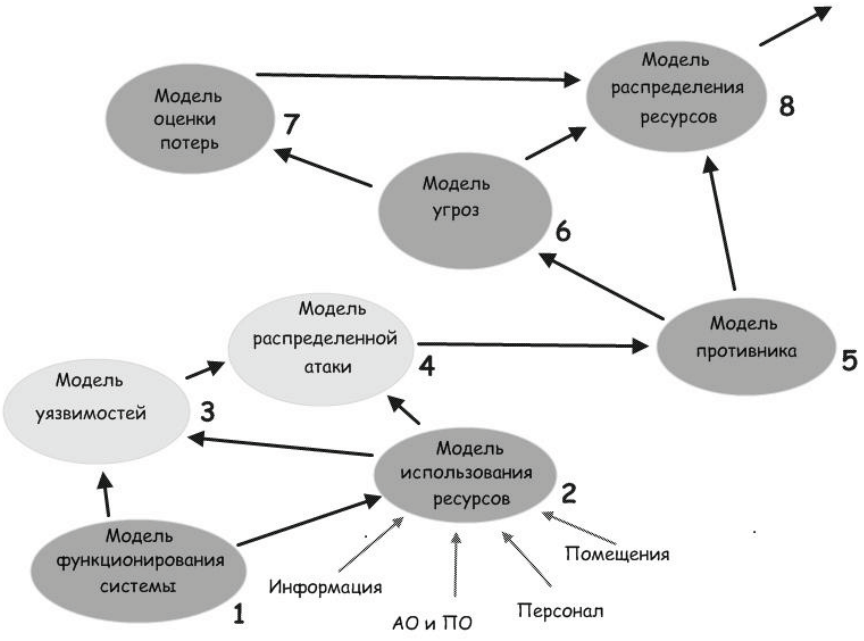

Рисунок 2. Усовершенствованная модель распределения и использования ресурсов

Вывод

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

Литература

[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] Домарев В.В. Безопасность информационных технологий. – :ТИД Диа Софт, 2002 - с. 688

[3] Гроздов Г. Г. Способ решения задачи формирования комплексной системы защиты информации для автоматизированных систем 1 и 2 класса [Текст] / Г.Г. Гроздов // (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] Гроздов Г. Г. Модифицированный способ решения задачи формирования эффективной комплексной системы защиты информации автоматизированной системы / Г. Г. Гроздов; монография. – К.: ДУІКТ, 2009. – 32 с.

[5] Колесников Д.Г. Компьютерные атаки и технологии их обнаружения. [Электронный ресурс] – Режим доступа к статье: http://web-protect.net/attack.htm