УДК 004.04

ИНСТРУМЕНТАРИЙ МИНИМИЗАЦИИ РИСКА ЗАЩИЩЕННОСТИ В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ (РКС)

В.Е. МУХИН

Разработана структура средств минимизации риска защищенности распределенных компьютерных систем, выполнена формализация функционирования основных блоков предложенной структуры. Предложена оценка уровня угроз безопасности, интегральная оценка ущерба вследствие атак на уязвимости, а также оценка степени риска реализации угроз безопасности в компьютерных системах. Также предложен подход к анализу риска на основе оценок степени опасности факторов угроз безопасности и вероятности реализации угроз безопасности с разделением их на соответствующие группы, а также на основе построения специальной матрицы рисков защищенности для минимизации риска защищенности.

ВВЕДЕНИЕ

Широкое внедрение и использование информационных технологий в настоящее время стало неотъемлемым фактором развития современного общества. РКС значительно повышают эффективность информационной составляющей в деятельности организаций, но в то же время, становятся одним из наиболее уязвимых компонентов, притягивая к себе внимание злоумышленников.

Актуальность проблемы обеспечения безопасности компьютерных систем возрастает в связи с рядом объективных причин. В частности, по отношению к распределенным компьютерным системам должен быть обеспечен высокий уровень доверия, т.к. в них хранится и обрабатывается ценная и конфиденциальная информация, которая представляет собой реальную ценность для ее владельца [1, 2]. Несанкционированный доступ к данной информации, в частности, ее разрушение или модификация, может привести к серьезному ущербу. Таким образом, обеспечение информационной безопасности РКС является чрезвычайно важной проблемой.

Современные РКС имеют сложную структуру. Увеличение количества используемых системно-технических платформ и широкий набор сетевых сервисов приводит к расширению списка уязвимостей и повышает требования к средствам защиты. Использование стандартных средств защиты, такие как межсетевые экраны и средства защиты от несанкционированного доступа, является необходимым, но уже не достаточным условием построения надежной и эффективной системы информационной безопасности.

В результате, для снижения уровня уязвимости РКС от внутренних и внешних атак и, в конечном счете, для избежания потерь важной информации, необходимо применение дополнительных механизмов защиты информации [3].

Одним из таких механизмов являются средства анализа риска защищенности в РКС. Анализ риска защищенности позволяет всесторонне исследовать информационную систему исследуемого объекта, оценить текущий уровень его информационной безопасности, выявить уязвимые места в системе защиты, создать модели возможных угроз РКС, проверить правильность подбора и настройки средств защиты [4].

Под риском понимается вероятность наступления нежелательного события, ведущего к потерям, в данном случае потерям информации, а также величина ущерба ввиду несанкционированного доступа к ней. Анализ риска защищенности подразумевает выполнение оценки степени риска и величины ущерба в случае осуществления того или иного варианта несанкционированных действий (НСД), выполняемых по специальным методикам [5].

В процессе проведения анализа риска защищенности РКС анализируются технологические потоки как электронной, так и бумажной информации, топология связей между узлами в системе, выявляются незащищенные или некорректные соединения, проводится анализ настроек межсетевых экранов и других средств защиты. Результатом данного анализа является ряд организационных документов, которые в дальнейшем могут явиться основой для построения надежной РКС [1].

Также в процессе анализа риска изучаются компоненты РКС, которые могут подвергнуться угрозам, определяются уязвимые места системы, оцениваются вероятность реализации каждой конкретной угрозы и возможные размеры потерь, выбираются возможные методы защиты и оцениваются их стоимость. На заключительном этапе оценивается эффективность применения предлагаемых средств защиты [6].

В результате, на основе анализа риска защищенности, принимается решение о целесообразности тех или иных мер и средств защиты, которые представляются в специальном документе, определяющем политику безопасности в данной РКС.

СРЕДСТВА МИНИМИЗАЦИИ РИСКА ЗАЩИЩЕННОСТИ

Рассмотрим общую структуру средств минимизации риска защищенности. Данная структура состоит из восьми основных блоков: задания целей, оценки угроз безопасности, оценки уязвимостей, анализа риска защищенности, выбора вариантов реакции (на потенциальные атаки), принятия решения, реакции и мониторинга состояния РКС.

Блоки задания целей, оценки угроз безопасности и оценки уязвимостей выполняют предварительный сбор информации о состоянии безопасности РКС и обеспечивают данные для следующих стадий процесса оценки риска защищенности. Блок анализа риска защищенности является фактически ключевым, поскольку он определяет текущий уровень риска, его критичность, а также факторы, позволяющие снизить риск защищенности. Следующие четыре блока определяют возможные варианты реакции на потенциальные вторжения, принимают решение и непосредственно реагируют на атаки, а также осуществляют модификацию параметров средств защиты РКС и мониторинг их состояния.

Рассмотрим особенности реализации блоков данной структуры.

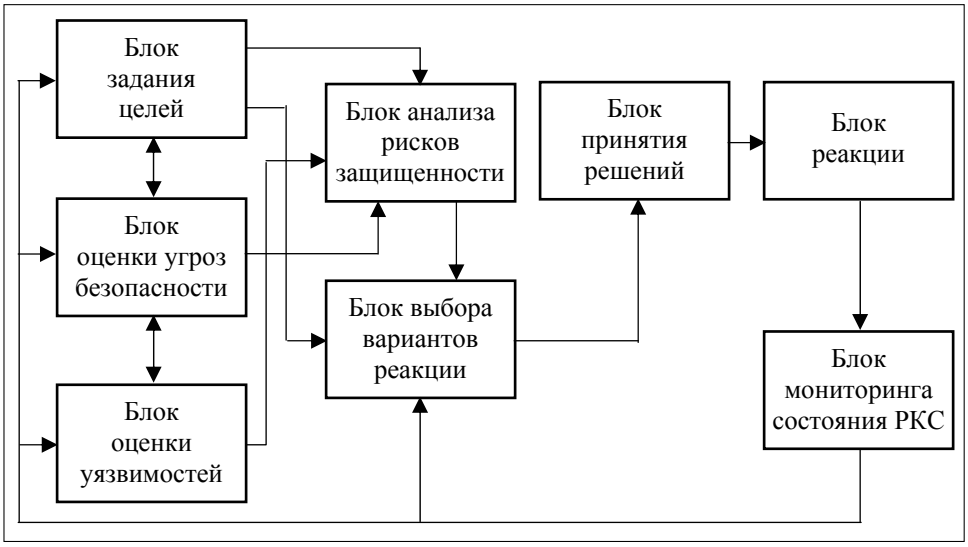

Рис. 1. Структура средств, реализующих минимизацию риска защищенности РКС

Блок задания целей

В данном блоке определяются параметры, по которым будет проводиться анализ и минимизация риска защищенности РКС. В большинстве случаев эти параметры задаются администратором безопасности, который должен постоянно выявлять потенциальные угрозы, уязвимости и оценивать риски.

Блока анализа целей представляется целевой функцией f :

$$f = f(s_i, a_i, g_i), \tag{1}$$

где s_i — субъект-инициатор события, a_i — параметры действий субъекта, g_i — возможные цели. В свою очередь, параметры действий субъекта a_i представляются в виде кортежа данных:

$$a_i = f'\left(\{t_1,\ldots,t_c\},\{l_1,\ldots,l_d\},\{r_1,\ldots,r_e\},\{\gamma_1,\ldots,\gamma_f\}\right), \tag{2}$$

где t_i — время события, l_i — место события, r_i — используемые средства, γ_i — степень опасности события.

Определенные в данном блоке параметры используются в других блоках системы минимизации риска защищенности.

Блок оценки угроз безопасности

Под угрозой безопасности понимается возможность (вероятность) того, что злоумышленник может совершить несанкционированный доступ к ресурсам РКС. В целом, все угрозы безопасности подразделяются на угрозы модификации или кражи критичных данных, угрозы нарушения функционирования системного программного обеспечения РКС, а также угрозы, косвенно ведущие к реализации несанкционированного доступа [7].

Блок оценки угроз безопасности выполняет общий анализ возможных угроз РКС, сгруппированных по классам. Для повышения корректности

реализации данной процедуры часто требуются значительные затраты [8]. Следует отметить, что оценка угроз не позволяет непосредственно оценить уровень риска защищенности РКС, но в данном блоке формируются данные и решения, которые используются при анализе риска.

Оценка угроз безопасности включает две составляющие: ситуационный анализ и выявление угроз.

Ситуационный анализ представляет собой детальный анализ параметров функционирования аппаратно-программного обеспечения РКС, в том числе параметров применяемых средств обеспечения безопасности. При проведении данного анализа целесообразно сгруппировать однотипные данные и оценивать их отдельно по каждой группе.

Выявление угроз предусматривает комплексный и детальный анализ всех факторов, которые могут оказывать влияние на безопасность функционирования РКС. Угрозы разделяются на три базовые группы: «потенциальные» — действия, которые теоретически могут представлять опасность; «реальные» — действия злоумышленников по НСД; «направленные» — те, которые направлены на реализацию конкретных уязвимостей в аппаратно-программном обеспечении РКС.

Эффективный уровень TL_j угрозы безопасности от *j*-того нарушителя предлагается рассчитывать как:

$$TL_j = \omega_1 * LP_j + \omega_2 \frac{1}{n} \sum_{i=1}^{n} F_{ij} , \qquad (3)$$

где LP_j — потенциальный уровень угрозы нарушителя; F_{ij} — корректирующие факторы из спецификации модели нарушителя; n — количество исследуемых факторов; ω_1, ω_2 — весовые коэффициенты, регулирующие удельный вес обеих составляющих в TL_j, причем $\omega_1 + \omega_2 = 1$. В том случае, если отдельный фактор для некоторой исследуемой категории нарушителя имеет несколько значений, для вычислений используется среднее значение этого фактора. Под потенциальным уровнем угрозы нарушителя LP_j понимаются его общие возможности в целом, в отличие от конкретных возможностей TL_j для конкретной РКС.

Для расчета и корректировки параметров ω_1, ω_2, F_{ij}, LP_j используются данные блока задания целей.

Блок оценки уязвимостей

В данном блоке выявляются уязвимости, т.е. потенциальные возможности для злоумышленника получить несанкционированный доступ к системе, который приводит к определенному ущербу аппаратно-программного обеспечения РКС и обрабатываемых в ней данных.

Оценка уязвимостей включает две составляющие: выявление уязвимостей и определение факторов, снижающих риск реализации уязвимостей в системе безопасности РКС.

Выявление уязвимостей. Уязвимость рассматривается как потенциальный канал реализации угрозы, т.е. это слабые места (т.н. «дыры») в существующих средствах безопасности РКС. В качестве факторов, способствую-

щих появлению уязвимостей могут, в частности, выступать: незащищенные ресурсы или ресурсы с низким уровнем защищенности, неэффективные средства защиты, некорректные действия по предотвращению угроз, низкая квалификация администраторов безопасности, потенциальные ошибки в системном программном обеспечении и т.д.

Определение факторов, снижающих риск реализации уязвимостей. К их числу относятся те факторы, которые могут уменьшить вероятность реализации уязвимостей РКС. Например, в качестве таких факторов выступают: эффективная система защиты РКС; высокая квалификация администраторов безопасности; средства мониторинга, которые упреждают опасные действия; система адаптивного управления безопасностью и т.д.

Анализ уязвимостей РКС предусматривает необходимость участия администратора безопасности, поскольку он может влиять на многие факторы, связанные с уязвимостью системы.

Существует шесть основных факторов, которые влияют на уязвимости РКС: местонахождение уязвимости, степень открытости РКС, ценность обрабатываемой информации, влияние особенностей РКС, применение адекватных мер и средств защиты, квалификация администраторов безопасности.

Введем понятие уязвимости I и II типа. К I-му типу относятся такие уязвимости, которые потенциально предотвращаются реализованными в системе средствами защиты, а ко II-му — те, которые не предотвращаются даже потенциально. Сформируем интегральную оценку C, характеризующую потенциальный суммарный ущерб вследствие реализации атаки на уязвимости РКС:

$$C = \sum_{i=1}^{N} \frac{UI_i}{U} + \sum_{j=1}^{M} K_j * \frac{UII_i}{U}, \qquad (4)$$

где UI — количество пользователей, скомпрометированных в результате атаки на уязвимость типа I; N — количество уязвимостей типа I; UII — количество пользователей, скомпрометированных в результате атаки на уязвимость типа II; M — количество уязвимостей типа II; U — общее количество пользователей в системе; K_j — коэффициент, характеризующий уязвимость типа II.

Для получения данной оценки необходимо для каждой обнаруженной уязвимости:

- определить тип уязвимости;
- если уязвимость имеет тип II, то с помощью экспертных оценок определить последствия данной уязвимости и рассчитать коэффициент K_j;
- оценить количество пользователей, на которых могут быть произведены атаки по использованию уязвимостей типа I и II, по отношению к общему количеству пользователей в системе.

Блок анализа риска защищенности

Анализ риска защищенности представляет собой оценку вероятности реализации несанкционированных действий путем использования уязвимостей в системе безопасности. Данный анализ требует комплексного учета всех факторов, связанных с угрозами безопасности РКС. При этом следует отме-

тить, что, в том случае, если существующая угроза безопасности является серьезной, но вероятность ее реализации является низкой (т.е. ее влияние на безопасность РКС оценивается как незначительное), то уровень риска защищенности также считается низким.

Анализ риска защищенности включает две составляющие: вероятность реализации угроз безопасности и оценку степени ущерба вследствие реализации угроз безопасности.

Для *оценки степени ущерба вследствие реализации угроз безопасности* факторы разделяются по группам, которые отражают степень их опасности по отношению к ресурсам РКС. При этом факторы с низким уровнем опасности рассматриваются как неопасные, а факторы с высокой степенью опасности обязательно должны быть нейтрализованы.

Группы факторов угроз безопасности по степени их опасности распределяются таким образом: критичная, высокая, средняя, низкая и незначительная.

Отнесение факторов угроз безопасности к определенной группе степени риска проводится на основе экспертных оценок и предыдущей статистической информации по функционированию РКС.

Вероятность реализации угроз безопасности также находится в одной из групп, которые отражают степень возможности реализации угроз безопасности.

Возможности реализации угроз безопасности группируются на основании предварительной статистической информации по функционированию системы безопасности РКС. Выделяются следующие степени возможности реализации угроз безопасности: практические невозможно, маловероятно, вероятно, высоковероятно, практически неизбежно.

Для оценки риска реализации угрозы от нарушителей предлагается использовать функцию TR, характеризующую возможность реализации этой угрозы:

$$TR = \frac{1}{m} * \sum_{i=1}^{m} \sum_{j=1}^{n} K_{ij} PE_j = \frac{1}{m} * \sum_{i=1}^{m} \sum_{j=1}^{n} K_{ij} PB_j TL_j \ , \ m \le n \, , \qquad (5)$$

где $K_{ij} = 0$, если на *i*-м месте в перечне субъектов угрозы не представлен *j*-й злоумышленник (неопасный фактор), $K_{ij} = 1$, если на *i*-м месте в перечне субъектов угрозы представлен *j*-й злоумышленник (опасный фактор), m — количество опасных субъектов, n — общее количество всех субъектов, PE_j — эффективная вероятность реализации угрозы, PB_j — базовая вероятность реализации угрозы, т.е. общеизвестная или общепринятая вероятность конкретной угрозы.

Величина возможного ущерба от реализации угрозы определяется таким образом:

$$PL_j = c_j \sum_{k=1}^{3} K_{ki} A_k \ , \qquad (6)$$

где A_k — априорные требования по обеспечению трех основных свойств защищенной информации: конфиденциальность, целостность и доступность. Эти требования могут быть выражены по относительной шкале, при

этом $K_{ki} = 0$, если данная угроза не влияет на *k*-е свойство информации, $K_{ki} = 1$, если данная угроза влияет на *k*-тое свойство информации, а c_i — нормирующий коэффициент.

Таким образом, величина риска реализации угрозы безопасности R в РКС рассчитывается как:

$$R = \left(\frac{1}{m} * \sum_{i=1}^{m} \sum_{j=1}^{n} K_{ij} PB_j TL_j \right) \left(c_i \sum_{k=1}^{3} K_{ki} A_k \right). \qquad (7)$$

Представленный подход позволяет оценить влияние различных факторов на формирование количественных значений эффективного уровня риска и сформулировать требования к мерам и средствам защиты.

Матрица рисков защищенности. Завершающая стадия анализа риска защищенности состоит в построении матрицы рисков. Данная матрица строится по двум основным параметрам, описывающим риски защищенности: степени опасности факторов угроз безопасности и вероятности реализации угроз безопасности (рис. 2).

Существующие риски защищенности располагаются в данной матрице рисков и им назначаются приоритеты, т.е. степени опасности как вероятности реализации угроз безопасности, при этом используются экспертные оценки. Всего выделяют четыре категории рисков защищенности: низкий, средний, высокий и сверхвысокий. Так, те риски, располагающиеся в правом верхнем квадранте матрицы рисков (рис. 2), рассматриваются как самые опасные риски. Важно отметить, что назначение категории рискам зависит от условий функционирования конкретной РКС. Конечной целью является перемещение всех возможных угроз безопасности РКС в левый нижний угол матрицы рисков защищенности.

Регулярное обновление матрицы рисков позволяет выявлять тенденции в среде защиты информации, а также позволяет оценить факт снижения или повышения риска защищенности РКС. Матрица рисков может использоваться как основа для разработки стратегий минимизации риска защищенности и для планирования возможных путей снижения вероятности реализации угроз безопасности РКС.

Блок выбора вариантов реакции (на потенциальную атаку)

На этом этапе администратор безопасности определяет комплекс механизмов для обеспечения безопасности и защищенности РКС. Выбор механизмов защиты должен основываться на анализе в реальном режиме времени критичных параметров безопасности и на анализе риска защищенности РКС. Возможными вариантами реакции на атаки злоумышленников являются: использование существующих средств защиты в неизменном виде; перенастройка параметров существующих средств защиты; добавление и изменение конфигурации существующих средств защиты; приостановка функционирования или отключение тех средств защиты, которые не являются необходимыми в данный момент.

Некоторые из перечисленных выше вариантов реакции на атаки могут вызвать существенное увеличение аппаратно-программных затрат, что, в свою очередь, может снизить производительность РКС [8]. Данный фактор

необходимо учитывать при выборе того или иного варианта реакции. Также следует учитывать, что обеспечение требуемого уровня безопасности обработки критичной информации всегда имеет наивысший приоритет при выборе вариантов реакции на потенциальные атаки.

Рис. 2. Матрица рисков защищенности РКС

Блок принятия решения

Данный блок реализует две основные функции.

Во-первых, здесь принимаются решения по приоритетным направлениям выявления угроз безопасности и уязвимостей РКС. Часто оказывается, что спектр угроз безопасности является весьма широким, поэтому сложно обеспечить оперативную реакцию на все актуальные угрозы. Прежде всего, необходимо выявить наиболее опасные угрозы и нейтрализовать их за минимальный промежуток времени. В том случае, если критичные угрозы не удается нейтрализовать оперативно, возможно, требуется принять решение о временной приостановке функционирования РКС или ее отдельных сегментов.

Во-вторых, на данном этапе необходимо определить требуемые аппаратно-программные ресурсы и оценить соответствующие затраты на реализацию противодействия угрозам безопасности РКС для выбора эффектив-

ных средств защиты информации, в частности, по критерию цена/качество. Качество средств защиты информации определяется, прежде всего, такими параметрами, как обеспечиваемая ими степень защиты и аппаратно-программные затраты на их реализацию.

Для эффективного поиска решений используется алгоритм случайного поиска с предысторией [10].

Данный алгоритм представляется в виде следующих рекуррентных выражений:

$$\overline{X}_{i+1} = \overline{X}_i + \Delta\overline{X}_{i+1};$$

$$\overline{X}_i = \overline{X}_{i-h} \text{ при } [f(\overline{X}_{i-1}) < f(\overline{X}_i)] \vee [f(\overline{X}_i) < 0], \qquad (8)$$

где $\overline{X}_i$ — вектор параметров целевой функции (таких, например, как длины ключей шифрования, которые во многом определяют уровень защищенности информации и т.д.) на i-том шаге поиска; h — число последовательно неудачных шагов поиска; $\Delta\overline{X}_{i+1}$ — вектор приращений на i+1-м шаге поиска, который определяется как:

$$\Delta\overline{X}_{i+1} = \begin{cases} a\overline{R}_{i+1} & \text{при } (i=0) \vee (|\Delta\overline{X}_i| = |\Delta\overline{X}_{i-1}|) \wedge (h>1), \\ \Delta\overline{X}_i & \text{при } [f(\overline{X}_{i-1}) \geq f(\overline{X}_i)] \wedge [f(\overline{X}_i) \geq 0], \\ -\Delta\overline{X}_i & \text{при } (|\Delta\overline{X}_i| \neq |\Delta\overline{X}_{i-1}|) \wedge (h \geq 1), \end{cases} \qquad (9)$$

где a — максимальная величина рабочего шага поиска, $\overline{R}_{i+1}$ — вектор случайных чисел, определяется как:

$$\overline{R}_{i+1} = (0, ..., 0, R_k^{i+1}, R_{k+1}^{i+1}, ..., R_L^{i+1}, 0, ..., 0),$$

$$R_k^{i+1} = R_{k+1}^{i+1} = ... = R_L^{i+1} = \psi, \qquad (10)$$

где ψ — случайно равномерно распределенные числа, выбираемые из интервала $[-1,1]$; k и L — случайные целые числа, распределенные на отрезке $[1,h]$ и упорядоченные соотношением $k \leq L$, $f(\overline{X}_{i-1})$, $f(\overline{X}_i)$, $f(\overline{X}_{i+1})$ — значения параметров целевой функции после осуществления $(i-1)$-, i-, $(i+1)$-го шагов поиска.

Специфика предлагаемого алгоритма состоит в том, что в нем вводится окно истории, т.е. запоминается величина такого последнего шага по каждой переменной, который привел к требуемому изменению целевой функции. В данном алгоритме вначале используется сохраненное значение шага поиска и лишь в том случае, если оно не дает требуемого результата, выполняется расчет величины шага в соответствии с алгоритмом случайного поиска.

Эффективные решения по минимизации риска защищенности должны базироваться на учете требования постоянного снижения уровня существующих рисков защищенности ввиду возможных серьезных последствий при функционировании РКС в условиях высокого уровня риска их защищенности [1].

Блок реакции (на угрозы безопасности)

Данный блок реализовывает реакцию средств защиты на угрозы безопасности и предотвращает несанкционированный доступ к РКС. Эффективная реакция на угрозы безопасности является результатом комплексного функционирования всех предыдущих и данного блока.

Блок мониторинга состояния РКС

Для эффективного предотвращения угроз безопасности РКС необходимо проведение постоянного мониторинга существующих угроз, уязвимостей. Блок мониторинга состояния РКС является завершающим в предложенной структуре средств минимизации риска защищенности и координирует функционирование ряда структурных блоков. Общая схема системы мониторинга состояния РКС представлена на рис. 3 и включает в себя следующие модули: модуль сбора информации и проверки состояния системы; модуль формирования событий безопасности; модуль обнаружения вторжений; модуль реакции системы; модуль обновления шаблонов и классов.

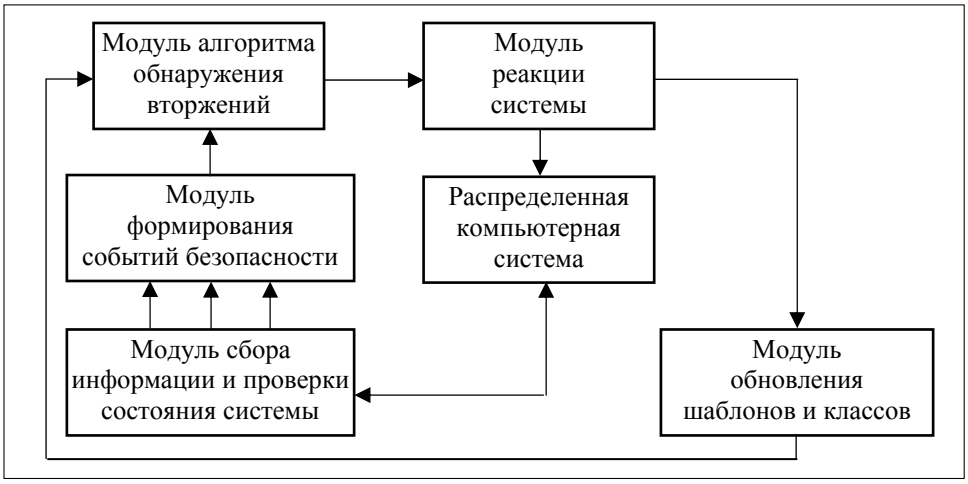

Рис. 3. Общая структура комплексной системы мониторинга состояния РКС

Модуль сбора информации и проверки состояния системы, в качестве которых системы выступают классические системы обнаружения вторжений, средства защиты (антивирусы, межсетевые экраны, аппаратные средства защиты и контроля доступа) и средства анализа защищенности РКС. Системы анализа защищенности проводят всесторонние исследования контролируемых ресурсов с целью обнаружения уязвимостей, которые способны привести к нарушению политики безопасности РКС.

Модуль формирования событий безопасности получает информацию от средств сбора информации и проверки состояний системы, выступающих в качестве агентов-приложений по специальному протоколу получения данных, в соответствии с которым выполняется преобразование журналов регистрации событий агентов-приложений во внутренний формат данных, использующийся в системе мониторинга безопасности.

Модуль обнаружения вторжений на первом этапе анализирует существующие причинно-следственные связи, указывающие на взаимосвязь между вторжениями, дифференцированными по времени, месту, способу атаки и задействованным средствам, а также формирует вероятностную зависимость между событиями, инициатор которых выявлен не был, и анализируемыми событиями.

Далее проводится автоматическое ранжирование по уровням опасности угроз действий нарушителя, на основе анализа возможного ущерба компьютерной системе. Основной задачей данного блока является формирование вероятностей вторжений злоумышленников в РКС и определение потенциальных целей нарушителей, а также прогнозирование их дальнейших действий.

Если воздействие на систему критично, то *Модуль реакции системы* производит автоматическую нейтрализацию действий злоумышленника. Если же степень угрозы не превышает пороговый уровень, то продолжается штатное функционирование системы.

Модуль обновления шаблонов и классов на основании информации о совершенных вторжениях и методах действия злоумышленника обеспечивает своевременное обновление шаблонов и сигнатур.

ЗАКЛЮЧЕНИЕ

Обеспечение безопасности РКС представляет собой комплекс мероприятий, включающий в себя, в частности, механизмы защиты аппаратно-программных средств и действия администратора безопасности по их применению. Известно, что абсолютную безопасность РКС обеспечить в принципе невозможно, однако возможно существенно снизить уровень угроз безопасности и риска защищенности системы. Для реализации данной задачи необходим формализованный процесс и соответствующие средства минимизации риска защищенности, рассмотренные в данной статье.

Предложенные средства минимизации риска защищенности имеют практическую направленность, учитывают требования к современным методам минимизации риска защищенности и позволяют эффективно выявлять, классифицировать и анализировать угрозы безопасности РКС, что обеспечивает повышение эффективности применения средств защиты информации.

ЛИТЕРАТУРА

1. *Медведовский И.Д., Петренко С.А., Нестеров С.А.* Руководство по управлению информационными рисками корпоративных информационных систем Internet/Intranet. — М.: «Domina Security», 2002. — 184 с.
2. *Maiwald E.* Fundamentals of network security. — New York: «McGraw-Hill. Technology Education», 2004. — 648 p.
3. *Hentea M.* Information security management. Encyclopedia of multimedia technology and networking. IDEA Group Reference. — Pennsylvania: «Hershey», 2005. — P. 390–395.
4. *Hentea M.* Enhancing information security risk management with a fuzzy model // Proceedings of 19th International Conference on Computer Application in Industry and Engineering. — Las Vegas, USA, 2006. — P. 132–139.
5. *Симонов С.В.* Технологии и инструментарий для управления рисками // Информационный бюллетень «Jet Info». — 2003. — № 2. — 32 с.
6. *Tassabehji R.* Information security threats. Encyclopedia of multimedia technology and networking. IDEA Group ReferencePennsylvania: «Hershey», 2005. — P. 404–410.
7. *Cardoso R.C., Friere M.M.* Security vulnerabilities and exposures in internet systems and services. Encyclopedia of multimedia technology and networking. IDEA Group Reference, Pennsylvania: «Hershey», 2005. — P. 910–916.
8. *Петренко С.А., Попов Ю.И.* Оценка затрат на информационную безопасность // Конфидент. Защита информации. — 2003. — № 1. — С. 45–52.
9. *Wang F.Y.* Agent-based control for networked traffic management systems // IEEE Intelligent Systems. — 2005. — № 5(19). — P. 92–96.
10. *Мухин В.Е., Павленко Е.Н.* Адаптивное управление безопасностью компьютерных систем на основе семиотических СППР с интеллектуальным агентом // Искусственный интеллект. — 2004. — № 4. — С. 785–793.

Поступила 26.11.2009