Ученые записки Таврического национального университета имени В.И. Вернадского
Серия «Экономика и управление». Том 27 (66). 2014 г. № 4. С. 32-38.

УДК 004.056.5

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ВЫБОРА ОПТИМАЛЬНОГО ЧИСЛА ЗАЩИЩЕННЫХ БЛОКОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ

Бойченко О.В., Ермоленко Я.О.

Таврический национальный университет имени В.И. Вернадского, Симферополь, Республика Крым
E-mail: ***bolek61@mail.ru***

В статье рассматриваются современные проблемы защиты программного обеспечения информационных систем управления предприятием. Предложена математическая модель создания условий для нахождения оптимального числа защищенных блоков программного обеспечения, при которых достигается наибольший эффект от защиты.
Ключевые слова: защита информации, структура программного обеспечения, информационные системы управления предприятием, математическая модель глубины установки паролей.

ВВЕДЕНИЕ

Практика функционирования информационных систем управления предприятием (ИСУП) указывает на наличие существенного ряда проблем, связанных с недостатками в подсистеме защиты информационных ресурсов ИСУП. Это, прежде всего, несоответствие требований технической защиты информации [1], а также недостаточность реализации в полной мере методов защиты информационных ресурсов подсистемой контроля доступа и защиты информации ИСУП.

Указанные недостатки позволяют нарушителю получать доступ к данным с нарушением установленных правил разграничения доступа; считывать данные с устройств памяти после выполнения санкционированных запросов; копировать носители информации; маскироваться под зарегистрированного пользователя, выдавать собственные несанкционированные запросы за запросы операционной системы; получать защищенные данные с помощью специально организованной серии санкционированных запросов; модифицировать программные средства (ПС), преднамеренно включая в его состав специальные блоки для нарушения безопасности данных; фальсифицировать факты формирования, выдачи и получения данных; подтверждать получение от пользователя данных, сформированных самим нарушителем, передачу пользователю данных, которые не передавались; изучать права доступа других пользователей; незаконно расширять свои права и изменять полномочия других пользователей [2].

Следует отметить, что ни одна система защиты данных не может считаться надежной на все 100 процентов. Поэтому, в частности в имени пароля, нельзя использовать очевидные фразы, которые легко угадать. Взлом системы защиты преступники могут осуществлять, в частности, путем подделки открытых ключей, анализа удаленных (не до конца) файлов, а также файлов подкачивания (виртуальная память), создания компьютерных вирусов или программных закладок.

Кроме того, нарушение режима физического доступа может позволить постороннему лицу захватить файлы с исходным текстом. Методы криптографии защищают данные, только до тех пор, пока они зашифрованы, и не могут помешать нарушению режима физической безопасности, когда раскрытой может стать текстовая или звуковая информация (этот вид атак проще и дешевле криптоанализа).

Таким образом, проблема защиты данных современных ИСУП является достаточно актуальной, что требует необходимости применения комплекса организационно-правовых, аппаратно-программных и инженерно-технических мероприятий.

Отдельные вопросы проблематики защиты блоков программного обеспечения (ПО) ИСУП в части анализа особенностей процесса начальной обработки данных, предусматривающего рассмотрение множественного числа всех признаков, касающихся искомой зависимости на основе статистических методов, корреляционного анализа и линейных регрессий, рассматриваются в работах таких ученых как Р.В. Бараненко, В.Н. Козел, Е.А. Дроздова, А.О. Плотников и других [3].

Однако, невзирая на достаточно мощный ресурсный потенциал системы информационной безопасности ИСУП, указанные проблемы заостряются ввиду существенного увеличения объемов данных современных ИСУП, неопределенностью их форматов по объему и времени, а также применением разнообразных систем безопасности для защиты блоков ПО ИСУП [4], что требует проведения дальнейших научных исследований.

Цель исследования состоит в разработке математической модели рационального выбора блоков программного обеспечения ИСУП, при которых достигается максимальный эффект от защиты с использованием парольной защиты структуры ПО ИСУП.

ИЗЛОЖЕНИЕ ОСНОВНОГО МАТЕРИАЛА

Формула для выбора рационального размера блоков, которые подлежат защите, может быть получена из таких рассуждений.

Пусть

b_i - число команд в блоке, который защищен паролем;

α - вероятность сбоя при выполнении команды (с учетом циклов);

l - число машинных команд для реализации одного пароля;

L - дополнительная память, которая нужна для реализации метода паролей:

$$L = nl,$$

где - число паролей;

B - память, которая защищена паролями:

$$B = \sum_{i=1}^{n} b_i,$$

q_i - условная вероятность неопределения сбоя при передаче управления системой при условии, что сбой был в блоке;

q - безусловная вероятность неопределение сбоя системой паролей (безотносительно к тому или другого блока);

C - объем памяти, не защищенной системой паролей (защищенной другими системами);

V - общий объем памяти:

$$V = B + C + L.$$

Очевидно, что

$$q_i = \frac{(b_i + L + C)}{B + L + C} + p_i \frac{(b_i + L + C)}{B + L + C} + ... + p_i^n \frac{(b_i + L + C)}{B + L + C} = \frac{b_i + L + C}{V(1 - p_i)}. \qquad (1)$$

Здесь p_i - совместимая вероятность того, что при случайном сбое в блоке управления передается другому блоку, но сбой не будет обнаружен паролем, который отвечает дежурному (после сбоя) блоку (к которому попало управление) через возникновение дежурного сбоя в указанном блоке.

$$p_i = \sum_{k \neq i} \frac{b_k}{V} \left(\frac{1}{b_k} \bullet \sum_{r=0}^{b_k} \left[1 - (1 - \alpha)^r \right] \right) = \frac{1}{V} \sum_{k \neq i} \left[(b_k + 1) - \frac{1 - (1 - \alpha)^{b_k + 1}}{\alpha} \right]. \qquad (2)$$

Формулы можно упростить при предположениях, непротиворечащих практике. При $\alpha \to 0$ получим

$$q_i = \frac{b_i + L + C}{V - \sum_{k \neq i} \left(b_k + 1 - \frac{1 - \ell^{-\alpha(b_k + 1)}}{\alpha} \right)}. \qquad (3)$$

При малых размерах блоков $(\alpha b_k \to o)$ после определенных превращений получим

$$q_i = \frac{b_i + L + C}{V - \frac{\alpha}{2}\sum_{k \neq i}(b_k + 1)^2}. \tag{4}$$

Найдем минимум q_i при фиксированном значении b_i. Очевидно, что задача нахождения оптимальных величин объемов блоков $b_{k,k\neq i}$ при фиксированном b_i может быть сведена к задаче нахождения оптимальных величин $b_{k,k\neq i}$, которые минимизируют функцию

$$f(b_1,...,b_{k-1}) = \sum_{k=1}^{n-1}\left(b_{k+1} - \frac{1-\ell^{-\alpha(b_k+1)}}{\alpha}\right). \tag{5}$$

При ограничениях

$$\sum_{k=1}^{n-1} b_k = B - b_i; b_k \geq 0. \tag{6}$$

Применив замену $y_k = b_k + 1$ с необходимыми превращениями, получим систему

$$y_k = B - b_i + (n-1) - (y_1 + y_2 + ... + y_{n-2}); k = \overline{1, n-2}, \tag{7}$$

Откуда следует

$$y_1 = y_2 = ...y_{n-2} \tag{8}$$

и окончательно

$$b_{1_1} = b_2 = ...b_{n-2}. \tag{9}$$

Таким образом, мы показали, что при фиксированных n и b_i минимум q_i достигается, если объемы защищенных блоков будут ровными между собой.

Допуская, что

$$b_i = B/n, \overline{i, n}. \tag{10}$$

Получим при $\alpha \to 0$

$$q_i = \frac{\frac{B}{n} + L + C}{V - (n-1)\left(\frac{B}{n} + 1 - \frac{1 - \ell^{-\alpha(\frac{B}{n}+1)}}{\alpha}\right)}. \qquad (11)$$

При $\frac{\alpha B}{n} \to o$

$$q_i = \frac{\frac{B}{n} + L + C}{V - \frac{\alpha}{2}(n-1)(\frac{B}{n}+1)^2}. \qquad (12)$$

Безусловная вероятность того, что случайный сбой не будет обнаружен системой паролей $\{П_i\}$, равняется

$$q = \frac{b_i}{B}\sum_{i=1}^{n} q_i.$$

Действительно, поскольку отказы с вероятностью α являют собой редкие события $(\alpha \to 0)$, мы можем утверждать (с ссылкой на теорему Пуассона и особенности экспотенциального закона распределения), что момент появления сбоя имеет равномерное распределение, то есть вероятность появления случайного сбоя в модуле M_i при условии, что сбой состоялся) равняется $\frac{b_i}{B}$.

Принимая во внимание (10), получим

$$q = \frac{1}{n}\sum_{i=1}^{n} q_i = q_i. \qquad (13)$$

Найдем оптимальное число защищенных блоков, при котором достигается наибольший эффект от защиты, то есть $q_i = q_{i\min}$.

Подставляя $L = nl$ в (12), получим

$$q_i = \frac{\frac{B}{n} + nl + C}{B + nl + C - \frac{\alpha}{2}(n-1)\left(\frac{B}{n}+1\right)^2} = \frac{an^3 + bn^2 + cn}{dn^3 + en^2 + fn + g},$$

где

$$a = 2l, b = 2C, c = 2B, d = 2l - \alpha, e = 2B + 2C + 2\alpha B + \alpha, f = 2\alpha B - \alpha B^2, g = \alpha B^2.$$

Отсюда оптимальное n находится из уравнения

$$a_4 n^4 + a_3 n^3 + a_2 n^2 + a_1 n + a_0 = 0, \tag{14}$$

где

$$a_4 = 2l(2B + 4l + \alpha(2B + 1)) - 2\alpha C,$$
$$a_3 = 4B(\alpha(l(2 - B) + 1) - 2l),$$
$$a_2 = 2B(\alpha(B(3l - C - 2) + 2C) - 2(B + C) - \alpha),$$
$$a_1 = 2\alpha B^2(2C - B - 2),$$
$$a_0 = 2\alpha B^2.$$

Более удобная формула получается на базе выражения (11).
При $\alpha \to 0$ имеем

$$q_i = \frac{\frac{B}{n} + nl + C}{B + C + (n - l)\left(\frac{B}{n} + 1 - \frac{1 - \ell^{-\alpha\left(\frac{B}{n}+1\right)}}{\alpha}\right)}.$$

Сделав несколько превращений, получим

$$n^* = 1 + \sqrt{1 + \frac{B + C}{l}}. \tag{15}$$

ВЫВОДЫ

Разработкой математической модели удается получить ответ на проблемный вопрос относительно вычисления необходимой глубины обустройства паролями слоев ПО ИСУП, поскольку программный код позволяет ставить их после каждой команды.

Следовательно, модель позволяет математически описать глубину установки паролей в слоях структуры ПО ИСУП и выбрать оптимальный размер защищенного блока [5].

Разработанная математическая модель позволяет создать условия для нахождения оптимального числа защищенных блоков ПО ИСУП, при которых достигается наибольший эффект от защиты. Отмеченное обеспечивает оптимизацию процесса управления защитой информации в ИСУП и повышает

качество функционирования системы для поддержки управленческих решений в деятельности предприятия.

Полученные результаты могут быть использованы во время дальнейших научных исследований в направлении разработки перспективных образцов устойчивого программного обеспечения информационной системы управления.

Список литературы

1. Хорев А.А. Организация защиты информации от утечки по техническим каналам / А.А. Хорев // Спец. техника. – М., 2006. – № 3. – С. 53 – 64.
2. Бойченко О. В. Правове регулювання міжнародної співпраці щодо забезпечення інформаційної безпеки в органах внутрішніх справ / О.В.Бойченко // Форум права. – 2008. – № 3. – С. 46-52 [Електронний ресурс]. – Режим доступу: http:www.nbuv.gov.ua / e-journals /FP/2008-3/08bovovs.pdf
3. Бараненко Р.В. Оптимизация работы корпоративных компьютерных сетей / Р.В. Бараненко, В.Н. Козел, Е.А. Дроздова, А.О. Плотников // ААЭКС. – М., 2004. – №1(13). – С. 25-29.
4. Бойченко О.В. Математична модель обробки інформації складної інформаційної системи / Бойченко О.В. // Радіоелектроніка та телекомунікації. – Львів: Львівська політехніка, 2011. – № 705. – С. 194-199.
5. Бойченко О.В. Математичне моделювання вибору раціонального розміру блоків інформаційної системи, що підлягають захисту / О.В. Бойченко, І.В. Пампуха, Н.М. Берназ // Системи озброєння та військова техніка. – Х.: ХУПС, 2012. – Вип. 3. – № 11. – С. 93-98.

Статья поступила в редакцию 10. 11. 2014 г