УДК 004.052

В.Г. Миронова, А.А. Шелупанов, М.А. Сопов

Сети Петри–Маркова как инструмент создания аналитических моделей для основных видов несанкционированного доступа в информационной системе

Предложен инструмент для создания аналитических моделей для основных видов несанкционированного доступа в информационной системе.
Ключевые слова: сеть Петри–Маркова, угрозы безопасности, несанкционированный доступ.

В настоящее время уровень развития информационных технологий, появление новых угроз информационной безопасности (УИБ) и стремление компаний снизить риски от возможных потерь конфиденциальных данных обуславливают высокую потребность в создании систем защиты конфиденциальной информации (СЗКИ).

Защита информационных ресурсов невозможна без определения и детальной классификации УИБ, которая облегчает выявление и задачу противодействия этим угрозам.

Из всех возможных угроз безопасности конфиденциальной информации выявляются угрозы безопасности информации для информационной системы (ИС) в процессах ее создания и эксплуатации. Полный перечень угроз безопасности информации фиксируется в модели угроз безопасности ИС.

Модель угроз безопасности информации в ИС содержит данные об угрозах:

– перехват (съем) конфиденциальной информации (КИ) по техническим каналам с целью копирования или неправомерного ее распространения;

– несанкционированный, в том числе случайный доступ в ИС для изменения, копирования, неправомерного распространения КИ или деструктивных воздействий на элементы ИС и обрабатываемую КИ с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования информации [1].

Согласно [2] угрозы безопасности КИ в ИС можно характеризовать посредством таких взаимосвязанных понятий, как источник угрозы, способ (метод) реализации угрозы, используемая уязвимость и ресурс (актив), подвергаемый угрозе.

Таким образом, угроза безопасности КИ (УБКИ) реализуется в результате образования канала реализации УБКИ между источником угрозы и носителем (источником) КИ, что создает достаточные условия для нарушения безопасности КИ (несанкционированный или случайный доступ).

К элементам канала реализации УБКИ относятся множества:

A = $\{a_1, a_2, \ldots, a_i\}$ – множество источников УБКИ – персонал ИС (пользователи ИС, администраторы сегментов ИС, системные администраторы, администраторы безопасности), технический персонал ИС, разработчики ИС, программные, программно-аппаратные и аппаратные средства, функционирующие в составе ИС либо совместно с ИС, отказы, неисправности, сбои, которые могут привести к нарушению безопасности информации ИС, а также посторонние программные, программно-аппаратные и аппаратные средства, не входящие в состав ОО, i – количество возможных внутренних и внешних нарушителей КИ в ИС;

B = $\{b_1, b_2, \ldots, b_j\}$ – множество сред (путей) распространения КИ или воздействий, в которых физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) КИ, j – количество возможных сред (путей) распространения КИ или воздействий;

C = $\{c_1, c_2, \ldots, c_k\}$ – множество носителей КИ – физических лиц или материальных объектов, в том числе физических полей, в котором КИ находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин, k – количество возможных носителей КИ.

Соответственно элемент множества **D** = $\{d_1, d_2, \ldots, d_l\}$ – каналов реализации УБКИ, где l – количество возможных каналов, представляет собой кортеж, состоящий из трех элементов:

$$d_l \in \mathbf{D},\ \mathbf{D} = (a_i, b_j, c_k),\ l = \overline{1,3},\ a_i \in \mathbf{A},\ b_j \in \mathbf{B},\ c_k \in \mathbf{C}.$$

Следовательно, множество каналов реализации УБКИ является подмножеством декартового произведения множества источников УБКИ, множества сред распространения КИ или воздействий и множества носителей КИ:

$$\mathbf{D} \subset \mathbf{A} \times \mathbf{B} \times \mathbf{C}. \quad (1)$$

Применительно к конкретному виду ИС угрозы классифицируются согласно [3] в соответствии со следующими признаками:

1) по природе возникновения;
2) по степени преднамеренности проявления;
3) по непосредственному источнику угроз;
4) по положению источника угроз;
5) по степени зависимости от активности ИС;
6) по степени воздействия на ИС;
7) по этапам доступа пользователей или программ к ресурсам ИС;
8) по способу доступа к ресурсам ИС;
9) по текущему месту расположения информации, хранимой и обрабатываемой в ИС [3].

Составление полного перечня угроз в ИС производится для угроз безопасности информации нарушения конфиденциальной информации (УНКИ), связанных с:

1) непреднамеренными действиями человека по отношению к информации и ИС;
2) умышленными (преднамеренными) действиями человека;
3) преднамеренными действиями вероятностных нарушителей.

Применительно к конкретному виду ИС угрозы бывают следующих типов:

1) внешние угрозы, которые исходят от природных явлений, стихийных бедствий и катастроф, внешних нарушителей, специальных разведывательных служб;

2) внутренние угрозы – исходят от администраторов, пользователей и обслуживающего персонала системы. Угрозы, связанные с деятельностью человека как пользователя системы, делятся на преднамеренные и непреднамеренные;

3) угрозы типа отказа в обслуживании.

Исходя из вышесказанного, выделяют следующие группы угроз:

1. Угрозы, вызванные природными факторами и явлениями. $\mathbf{E} = \{e_1, e_2, \ldots, e_q\}$, $e_q \in \mathbf{E}$, q – количество угроз, вызванных природными факторами и явлениями.

2. Угрозы утечки информации по техническим каналам. $\mathbf{F} = \{\mathbf{FA}, \mathbf{FV}, \mathbf{FP}\}$.

2.1 Угрозы утечки акустической (речевой) информации. $\mathbf{FA} = \{fa_1, fa_2, \ldots, fa_r\}$, $fa_r \in \mathbf{FA}$, r – количество угроз утечки акустической (речевой) информации.

2.2 Угрозы утечки видовой информации. $\mathbf{FV} = \{fv_1, fv_2, \ldots, fv_s\}$, $fv_s \in \mathbf{FV}$, s – количество угроз утечки видовой информации.

2.3 Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН). $\mathbf{FP} = \{fp_1, p_2, \ldots, fp_t\}$, $fp_t \in \mathbf{FP}$, t – количество угроз утечки информации по каналам ПЭМИН.

3. Угрозы возникновения несанкционированного доступа к КИ. $\mathbf{G} = \{\mathbf{GV}, \mathbf{GP}\}$.

3.1. Угрозы, реализуемые в ходе загрузки операционной системы. $\mathbf{GV} = \{gv_1, gv_2, \ldots, gv_u\}$, $gv_u \in \mathbf{GV}$, u – количество угроз, реализуемых в ходе загрузки операционной системы.

3.2. Угрозы, реализуемые после загрузки операционной системы. $\mathbf{GP} = \{gp_1, gp_2, \ldots, gp_v\}$, $gp_v \in \mathbf{GP}$, v – количество угроз, реализуемых после загрузки операционной системы.

4. Угрозы отказа в обслуживании. $\mathbf{H} = \{h_1, h_2, \ldots, h_w\}$, $h_w \in \mathbf{H}$, w – количество угроз отказа в обслуживании.

5. Угрозы внедрения вредоносных программ. $\mathbf{M} = \{m_1, m_2, \ldots, m_x\}$, $m_x \in \mathbf{M}$, x – количество угроз внедрения вредоносных программ.

6. Угрозы сетевой безопасности. $\mathbf{N} = \{n_1, n_2, \ldots, n_y\}$, $n_y \in \mathbf{N}$, y – количество угроз сетевой безопасности.

7. Угрозы криптографической безопасности. $\mathbf{O} = \{o_1, o_2, \ldots, o_z\}$, $o_z \in \mathbf{O}$, z – количество угроз нарушения криптографической защиты.

8. Угрозы внедрения аппаратной закладки. $\mathbf{P} = \{p_1, p_2, \ldots, p_k\}$, $p_k \in \mathbf{P}$, k – количество угроз внедрения аппаратной закладки.

Угрозы утечки КИ по техническим каналам однозначно описываются характеристиками источника угрозы (приемника информативного сигнала), носителя КИ (источника информации) и среды (пути) распространения, т.е. определяются характеристиками канала реализации УБКИ, в данном случае технического канала утечки КИ, и описываются в соответствии с [2].

Угрозы, связанные с несанкционированным доступом (НСД), представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИС, способов реализации угроз, объектов воздействия и возможных деструктивных действий (видов несанкционированного доступа) [2].

С целью управления вероятностью успешной реализации НСД по времени (с использованием статических данных) построим аналитические модели НСД в ИС на основе сетей Петри–Маркова.

Построение аналитических моделей для основных видов НСД в ИС предлагается осуществлять в следующей последовательности:

1. Сценарий атаки делится на множества событий $\mathbf{S} = (s_1, s_2, \ldots, s_n)$, $s_n \in \mathbf{S}$ и условий $\mathbf{T} = (t_1, t_2, \ldots, t_n)$, $t_n \in \mathbf{T}$.

2. На основе множеств событий и условий строится граф сети Петри–Маркова.

3. Записываются основные элементы матрицы, определяющие логические функции срабатывания сети.

4. Сеть Петри–Маркова описывается системой интегродифференциальных уравнений.

5. Находится среднее время перемещения по сети Петри–Маркова из начальной позиции до конечного перехода на основе пуассоновского приближения.

6. Определяется вероятность успеха проведения атаки.

На рис. 1 представлена схема воздействия УБКИ на защищаемый объект.

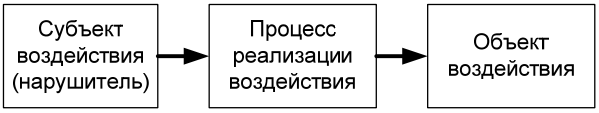

Рис. 1. Схема воздействия УБКИ на защищаемый объект

Под субъектами воздействия будем понимать нарушителей ИБ, типы которых рассмотрены в [4].

Процесс реализации воздействия – способ осуществления атаки на ИС.

Объектом воздействия будет являться ИС.

Например, угроза перехвата чужих паролей легальным пользователем операционной системы (ОС). Все компьютеры работают под управлением ОС Windows NT или Windows 2000.

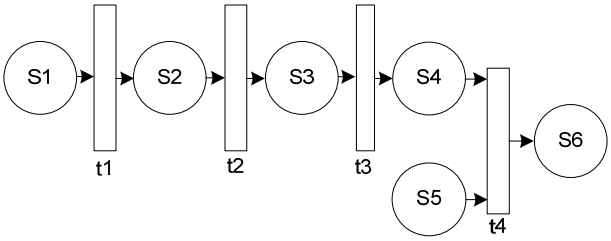

Рис. 2. Сеть Петри–Маркова для угрозы перехвата чужих паролей легальным пользователем ОС: s_1 – нарушитель (легальный пользователь ИС) имеет возможность легального доступа в ОС; s_2 – нарушитель (легальный пользователь ИС) запустил программу слежения и перехвата паролей на компьютере; s_3 – программа перехвата пароля была запущена; s_4 – нарушитель установил первоначальное окно запроса пароля и идентификатора учетной записи пользователя; s_5 – пользователь ИС готов войти в ИС; s_6 – пароль перехвачен; t_1 – нарушитель (легальный пользователь ИС) входит под своей учетной записью в систему; t_2 – нарушитель (легальный пользователь ИС) запускает программу слежения и перехвата паролей на компьютере; t_3 – используя быстрое переключение пользователей («Пуск» / «Выход из системы»/ «Смена пользователя»), нарушитель возвращается к окну с учетными записями пользователей; t_4 – пользователь системы вводит свой идентификатор и пароль

Полагаем, что плотности распределения вероятностей являются экспоненциальными зависимыми и имеют вид

$$f_{s_i t_j} = \lambda_{ij} e^{-\lambda_{ij}\tau}, \qquad (2)$$

$$\tau_{ср} = \tau_{11} + \tau_{22} + \tau_{33} + \frac{\tau_{46}^2 + \tau_{46}\tau_{56} + \tau_{56}^2}{\tau_{46} + \tau_{56}}, \quad (3)$$

где τ_{11} – среднее время входа нарушителя под своей учетной записью в систему; τ_{22} – среднее время запуска программы слежения и перехвата паролей на компьютере; τ_{33} – среднее время использования быстрого переключения пользователей («Пуск» / «Выход из системы»/ «Смена пользователя»); τ_{46} – среднее время программного перехвата пароля; τ_{56} – среднее время ввода идентификационных данных в ИС; $\tau_{ср}$ – среднее время для всей цепочки событий.

Матрица срабатывания сети Петри–Маркова

	s_1	s_2	s_3	s_4	s_5	s_6
t_1	1	1	0	0	0	0
t_2	0	1	1	0	0	0
t_3	0	0	1	1	0	0
t_4	0	0	0	1	1	$s_4t_4 \cap s_5t_4$

Вероятность успешной реализации атаки рассчитывается по формуле (4). Вероятность успешной реализации атаки типа «Копирование информации из ИС, компоненты которой располагаются в защищенной зоне»:

$$p(t) = 1 - e^{-\lambda t} = 1 - exp(-\frac{t}{t_{ср}}) = 1 - \exp(-\frac{1}{\tau_{ср}}). \quad (4)$$

Аналогично можно определить вероятность реализации других атак.

Таким образом, следует подвести краткие выводы.

Во-первых, показано, что для управления вероятностью успешной реализации НСД по времени (с использованием статических данных) можно построить аналитическую модель НСД в ИС.

Во-вторых, показана эффективность использования математического аппарата на основе сетей Петри–Маркова на примере построения модели угрозы перехвата чужих паролей легальным пользователем операционной системы (таблица).

В-третьих, предложен подход к определению вероятности успешной реализации атаки.

Работа выполнена в рамках проекта 7.701.2011 (проект 1/12) при поддержке Министерства образования и науки Российской Федерации.

Литература

1. Сабанов А.Г. Защита персональных данных в организациях здравоохранения / А.Г. Сабанов, В.Д. Зыков, Р.В. Мещеряков, С.П. Рылов, А.А. Шелупанов // М.: Горячая линия-Телеком, 2012. – С. 206.

2. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» // Утверждена заместителем директора ФСТЭК России, 15 февраля 2008 г.

3. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. [Электронный ресурс]. – Режим доступа: http://altell.ru/assets/images/laws/standard/51275-2006.pdf, свободный (дата обращения: 31 апреля 2012).

4. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1(31). – С. 28–35.

5. Миронова В.Г. Сети Петри как инструмент анализа системы защиты конфиденциальной информации. / В.Г. Миронова, А.А. Шелупанов // Известия ЮФУ. Технические науки. – 2011. – №12 (125). – С. 64–70.

6. Шелупанов А.А., Миронова В.Г. и др. Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» // Докл. Том. гос. ун-та систем управления и радиоэлектроники. – 2010. – №1(21), ч. 1. – С. 14–22.

7. Миронова В.Г. Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности / В.Г. Миронова, А.А. Шелупанов // Докл. Том. гос. ун-та систем управления и радиоэлектроники. – 2010. – №2(22), ч. 1. – С. 257–259.

8. Миронова В.Г. Анализ этапов предпроектного обследования информационной системы персональных данных / В.Г. Миронова, А.А. Шелупанов // Вестник СибГАУ им. М.Ф. Решетнева. 2011. – №2(35). С. 45–48.

9. Миронова В.Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях. / В.Г. Миронова, А.А. Шелупанов, Т.Н. Югов // Докл. Том. гос. ун-та систем управления и радиоэлектроники. – 2011. – №2(24), ч. 3. – С. 206–211.

Миронова Валентина Григорьевна
Инженер каф. КИБЭВС ТУСУРа
Тел.: 8-923-415-16-08
Эл. почта: mvg@security.tomsk.ru

Шелупанов Александр Александрович
Д-р техн. наук, проф., проректор по научной работе ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: saa@tusur.ru

Сопов Максим Алексеевич
Ст. преподаватель каф. КИБЭВС ТУСУР
Тел: 8 (382-2)413426
Эл. почта: sma@keva.tusur.ru

Mironova V.G., Shelupanov A.A., Sopov M.A.
Petri nets, Markov as a tool for creating analytical models for the main types of unauthorized access to the information system

This paper proposes a tool for creating analytical models for the main types of unauthorized access to the information system.
Keywords: Petri nets, Markov, security threats, unauthorized access.
