ОБ ОДНОМ ПОДХОДЕ К ПОСТРОЕНИЮ МОДЕЛИ ДЛЯ ОЦЕНКИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

А.С. Артамонов, кандидат физико-математических наук, профессор.
Санкт-Петербургский университет ГПС МЧС России

Рассмотрены формализованное представление и математическая постановка задачи оценки ущерба от проникновения нарушителя в автоматизированную систему. Представлены основные направления определения входных параметров для использования такой модели.

Ключевые слова: автоматизированная система, несанкционированный доступ, модель, транзакт

ABOUT ONE APPROACH TO THE CONSTRUCTION OF MODEL FOR THE EVALUATION OF UNAUTHORIZED ACCESS TO THE INFORMATION RESOURCES OF AUTOMATED SYSTEMS

A.S. Artamonov. Saint-Petersburg university of State fire service of EMERCOM of Russia

The article describes the formalized representation and the mathematical statement the problem of evaluating the damage from the tresspassing in the automated system. The main directions of defining the input parameters to use such a model are presented.

Keywords: automated system, unauthorized access, model, transaction

В периоды необходимости выбора комплекса решений по обеспечению безопасности в качестве ограничений учитываются следующие требования к способам организации защиты информации [1]:

– существование сертификатов по вопросам безопасности информации в соответствии с грифом обрабатываемой информации и порядком функционирования автоматизированных систем (АС);

– неизменность функционирования средств защиты;

– предоставление режима защиты охраняемых сведений, в том числе сохранения таких свойств защищенности информации, как конфиденциальность, доступность, целостность и подлинность;

– гарантированное сохранение целевых функций защищаемой автоматизированной системы – отсутствия ограничений, связанных с применением средств защиты, препятствующих реализации технологического цикла обработки информации.

В целях простого понимания и удобства описания разрабатываемых формализмов в рамках данного исследования введем следующее определение: транзактом называется любая попытка несанкционированного доступа (НСД), а также санкционированного доступа (СД) к ресурсам системы, в результате которого считывание или запись информации произошла с нарушением установленных правил.

Предположим, что успешная попытка СД с нарушением установленных правил (транзакт СД) приводит к искажению информации в базе данных.

В отличие от обычных заявок на обслуживание транзакт НСД имеет набор динамически изменяющихся особых свойств и параметров. Попытка несанкционированного доступа к информационным ресурсам (транзакт НСД) может привести к следующим результатам:

– копированию (считыванию) информации из базы данных;

– изменению (искажению) информации в базе данных;

– помехам в работоспособности (отказу в обслуживании) системы – полному прекращению или существенному замедлению исполнения функций по обслуживанию запросов.

Определение последствий транзактов НСД и их оценка осуществляется с учетом следующей системы допущений доступа к информационным ресурсам АС:

– необнаруженное поступление транзакта НСД в соответствующий элемент АС будем называть отказом определенного ресурса;

– данный отказ элемента АС влечет за собой ущерб, пропорциональный времени пребывания транзакта в системе;

– выявление транзакта НСД требует некоторого времени (зависящего от типа элемента АС, подвергшегося успешной атаке) для ликвидации последствий искажения информации (восстановление);

– прошедшему систему защиты транзакту НСД, становится доступным любой элемент (ресурс) АС;

– все потоки переходов предполагаются простейшими, то есть стационарными, ординарными и без последействия.

Возьмем за основу то, что в системе защиты информации используются следующие организационные и технические решения:

1) решения S_1, обеспечивающие аутентификацию и идентификацию персонала;

2) решения S_2 по управлению доступом пользователей к защищаемым ресурсам;

3) решения S_3, обеспечивающие регистрацию действий пользователей;

4) решения S_4 по дистанционной диагностике элементов защиты;

5) решения S_5, сориентированные на обеспечение целостности информационных ресурсов с использованием средств защиты информации;

6) решения S_6, устремленные на обеспечение в предельно возможной степени повышение достоверности и точности защищаемой информации;

7) решения S_7, способные обеспечить защиту от вредоносных программ;

8) решения S_8, позволяющие обеспечить противодействие нештатному созданию копий массивов информации;

9) решения S_9, ориентированные на предотвращение полной утраты накапливаемой информации;

10) решения S_{10}, устанавливающие регламенты обеспечения непрерывной работоспособности и восстановления системы.

Необходимо ввести следующие условные обозначения, которые будут применены при формализованном процессе несанкционированного доступа к информационным ресурсам АС:

λ – интенсивность поступления потока транзактов в АС. В силу выработанных предположений, поток транзактов будет пуассоновским, поэтому его можно охарактеризовать с помощью единственного параметра – интенсивности, при этом $\lambda \cdot \Delta t$ – вероятность поступления транзактов от момента времени *t* до момента времени $t + \Delta t$;

γ – интенсивность преодоления транзактом системы защиты; $\gamma \cdot \Delta t$ – вероятность преодоления системы защиты от момента времени *t* до момента времени $t + \Delta t$;

μ – интенсивность обнаружения транзактов в системе защиты; $\mu \cdot \Delta t$ – вероятность обнаружения транзактов от момента времени *t* до момента времени $t + \Delta t$;

P_{ki} – вероятность поступления транзакта в определенный элемент АС;

ρ – интенсивность восстановления данного элемента АС;

$1/\rho$ – среднее время устранения последствий (восстановления), предполагается, что весь этот интервал времени системе наносится определенный ущерб;

x – математическое ожидание количества транзактов в системе;

z – математическое ожидание количества транзактов, прошедших систему защиты;

u – вероятность того, что данный элемент АС не подвергся успешной информационной атаке (транзакт не попал в данный элемент, либо последствия предыдущих успешных атак на данный элемент уже устранены);

v – вероятность события, содержащегося в том, что данный элемент АС подвергся успешному нападению и эти последствия либо не обнаружены, либо еще не устранены (отказ элемента).

На рис. 1 изображен процесс поступления транзактов НСД в АС.

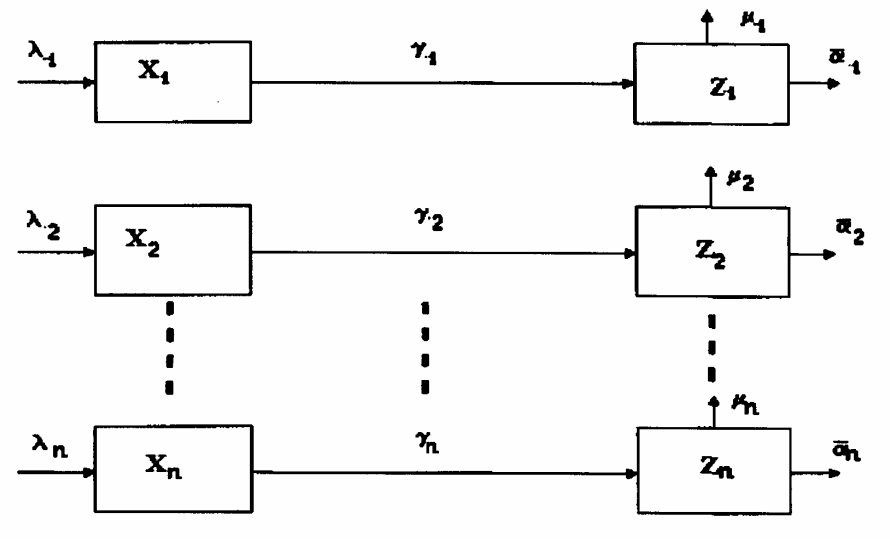

Рис. 1. **Графическое представление процесса поступления транзактов в АС**

Первый уровень контроля транзакт проходит в первом состоянии (идентификацию и аутентификацию персонала S_1), а контроль доступа пользователей к защищаемым ресурсам осуществляется во втором состоянии S_2. И только после этого проводится регистрация действий пользователей S_3 и т.д.

Окончательный выход из каждого состояния по результатам контроля происходит двумя путями:

– транзакт окончательно отрицается;

– транзакт допускается на вход АС для дальнейшей проверки.

С учетом принятой практики, транзакт, не прошедший контроля первой ступени, может поступать на вход системы неопределенное количество раз.

Интенсивность γ_k определяется по формуле:

$$\gamma = \frac{P_{nk}}{T_{nk}},$$

где P_{nk} – вероятность пропуска транзакта системой защиты; T_{nk} – среднее время «прорыва» транзакта через систему защиты.

В свою очередь:

$$\mu_k = \frac{P_{ok}}{T_{ok}}, \quad \overline{\alpha_k} = \frac{1 - P_{ok}}{T_{ok}},$$

где P_{ok} – вероятность правильного анализа транзакта; T_{ok} – среднее время анализа транзакта в системе защиты

Прошедшие систему защиты все транзакты поступают в АС. В общем случае, каждый транзакт *k*-го типа может поступить на обработку в любой из *m* элементов системы с вероятностью P_{ki} (*k* – тип транзакта; *i* – тип элемента). Для всех P_{ki} должно соблюдаться условие нормировки (полная группа событий):

$$\sum_{k=1}^{m} P_{ki} = 1.$$

Введем обобщенное понятие отказа элемента, заключающееся в том, что проведена успешная атака на АС, последствия которой либо не обнаружены, либо еще не устранены. При этом последствия атаки могут быть различными, однако все они приводят к нанесению определенного ущерба.

Отказы и сбои в работе вследствие поступления транзактов, не обнаруженных системой защиты, описываются графом, изображенным на рис. 2.

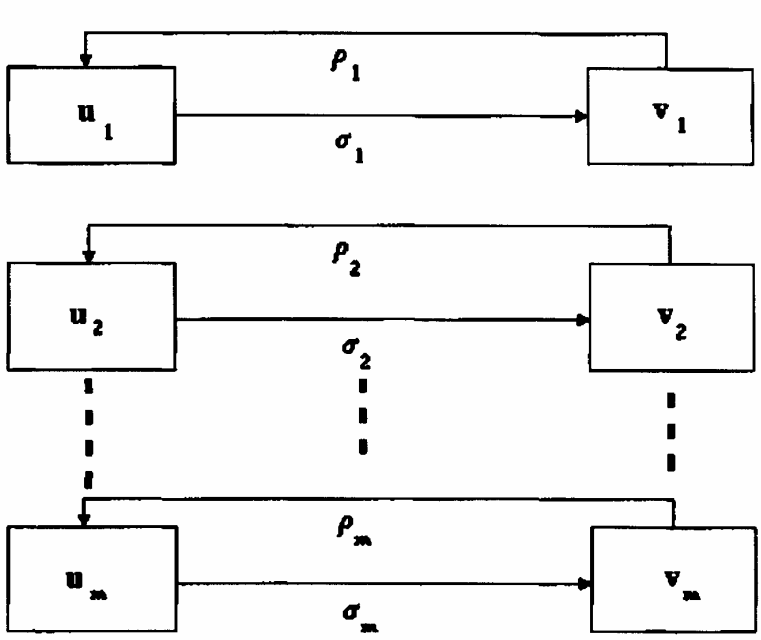

Рис. 2. **Графическое представление процесса отказов АС вследствие прохождения транзактов**

В графическом описании процесса используются следующие условные обозначения:

ρ_j – интенсивность обнаружения и восстановления отказа *j*-го элемента АС;

σ_j – интенсивность отказов *j*-го элемента АС вследствие поступления необнаруженных транзактов.

Указанные выше интенсивности вычисляются по формулам:

$$\rho_j = \frac{P_{oj}}{P_{oj} T_{bj} + (1 - P_{oj}) T_{oj}},$$

где T_{oj} – среднее время обнаружения транзакта системой защиты в *j*-м элементе АС; P_{oj} – вероятность обнаружения транзакта системой защиты в *j*-м элементе АС; t_{bj} – среднее время восстановления *j*-го элемента АС.

$$\sigma_j = \sum_{k=1}^{n} \overline{\alpha_k} P_{kj} z_k,$$

где P_{kj} – вероятность поступления транзакта *k*-го типа в элемент *j*-го типа.

Учитывая взаимосвязь обоих графов, а также простейший характер потоков перехода из состояния в состояние, можно получить следующую систему дифференциальных уравнений (2*n*+*m*):

$$\left.\begin{aligned} x_k' &= \lambda_k - \gamma_k x_k, \\ z_k' &= \gamma_k x_k - \left(\mu_k + \overline{\alpha_k}\right) z_k, \\ u_j' &= \rho_j v_j - \sigma_j u_j, \\ u_j + v_j &= 1, \\ k &= \overline{1,n}, \\ j &= \overline{1,m}. \end{aligned}\right\}$$

Решение этой системы уравнений необходимо проводить при следующих начальных условиях:

$$\left.\begin{aligned} x_k(0) &= 0, \\ z_k(0) &= 0, \\ u_j(0) &= 1, \\ v_j(0) &= 0. \\ k &= \overline{1,n}, \\ j &= \overline{1,m}. \end{aligned}\right\}$$

Проинтегрировав данную систему уравнений на промежутке времени от 0 до *T*, можно получить математическое ожидание ущерба от проникновения в систему нарушителей различных типов по следующей формуле:

$$\left.\begin{aligned} B(T_2 - T_1) &= \int_{T_1}^{T_2} \sum_{j=1}^{m} \beta_j v_j(t), \\ 0 \le T_1 &\le T_2 \le T. \end{aligned}\right\}$$

где β_j – ущерб, наносимый системе при искажении соответствующего информационного ресурса в единицу времени.

Для того чтобы обеспечить работоспособность приведенной выше базовой модели, нужна разработка комплекса методов и методик вычисления параметров, являющихся

входными для данной модели [2]. Проведение исследования и разработки должны проводиться в следующих основных направлениях:

– исследование потока транзактов НСД по типам и объемам;

– разработка методик для оценки эффективности систем защиты информации, прошедших определенные уровни защиты информации;

– разработка методов и методик восстановления работоспособности подсистем и элементов АС при их отказе, обусловленном поступлением в них транзактов НСД, прошедших основные виды контроля со стороны систем защиты;

– исследование и разработка методик оценки ущербов.

Нужно отметить, что в общем случае все эти исследования должны проводиться применительно к каждой конкретной АС как существующей, так и разрабатываемой.

Граф состояний для такой модели представлен на рис. 3:

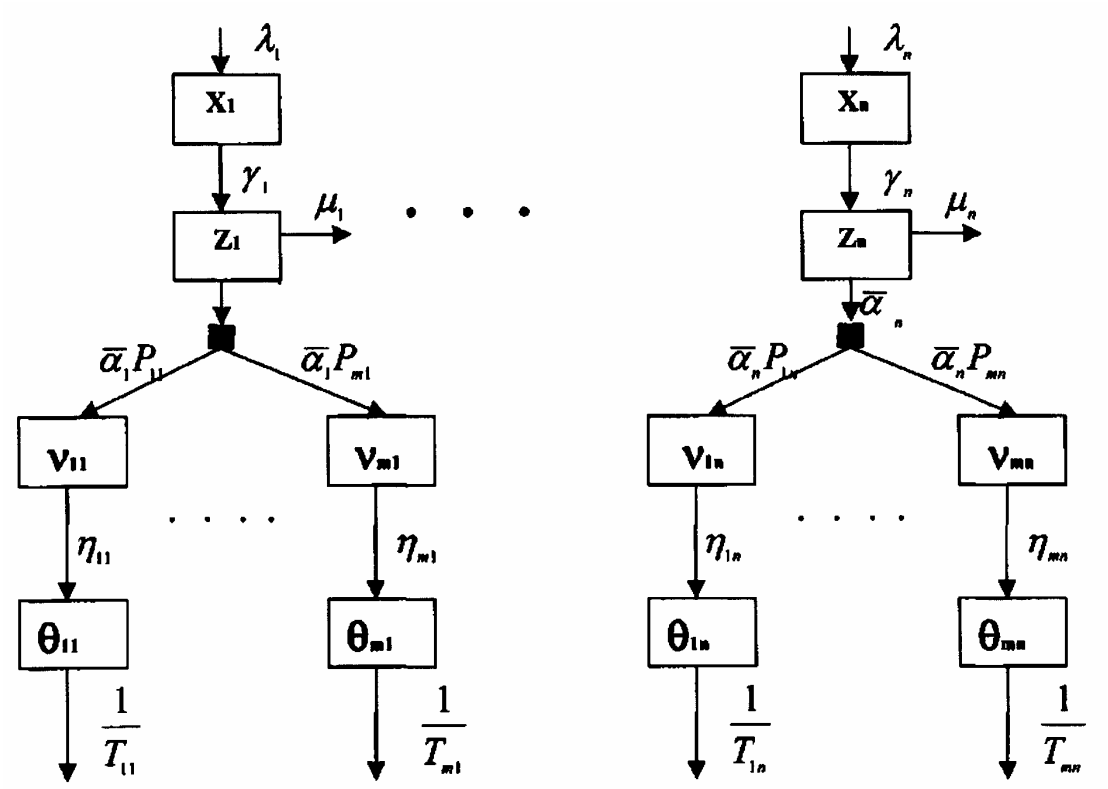

Рис. 3. **Графическое представление модели воздействия транзактов на различные элементы АС**

Предлагаемая система обыкновенных дифференциальных уравнений является математической моделью функционирования АС общего вида в условиях постоянного внешнего влияния, конечной целью которого является нанесение ущерба ее нормальной деятельности. Достижение этой цели реализовывается путем искажения информации о состоянии и деятельности подсистем и элементов данной социально-экономической системы за счет получения несанкционированного доступа к вычислительным ресурсам и базам данных обслуживающих ее АС.

Однако предположение о том, что «атакованный» элемент АС не подвергается новой информационной атаке до тех пор, пока не будут устранены последствия предыдущей атаки, является одним из предположений данной модели, существенно ограничивающим ее возможности. Введение этого предположения в случае, если среднее время между атаками превосходит суммарное среднее время обнаружения и восстановления последствий

информационных атак влияет (незначительно) на итоговые оценки и в то же время снижает размерность системы дифференциальных уравнений. В противном случае, при формулировании математической модели необходимо строить описание, опираясь не на состояния АС, а на состояния, в которых может находиться транзакт. Данный подход может существенно увеличить размерность соответствующей системы уравнений, однако решение о выборе модели должно приниматься с учетом конкретной ситуации. Различие такой модели от предшествующего случая содержится в соответствующем изменении графов состояний, при этом система концепций и допущений практически не изменяется.

Литература

1. Зима В.М., Молдавян А.А., Молдавян Н.А. Безопасность глобальных сетевых технологий. 2-е изд. СПб.: БХВ-Петербург, 2003. 368 с.

2. Системный анализ и принятие решений / В.И. Антюхов [и др.]; под ред. В.С. Артамонова. СПб.: С.-Петерб. ун-т ГПС МЧС России, 2009. 389 с.