Федеральное агентство по образованию
ГОУ ВПО «Волгоградский государственный университет»
Факультет физики и телекоммуникаций

На правах рукописи

ШИПИЛЕВА Алла Владимировна

НЕКОТОРЫЕ ЗАДАЧИ В ТЕОРИИ ВЕТВЯЩИХСЯ ПРОЦЕССОВ И МОДЕЛИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность 01.01.05 – теория вероятностей и математическая статистика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико – математических наук

Волгоград - 2009

Работа выполнена на кафедре информационной безопасности факультета физики и телекоммуникаций Волгоградского государственного университета.

Научный руководитель: доктор физико – математических наук
профессор
Горяйнов Виктор Владимирович.

Официальные оппоненты: доктор физико – математических наук
профессор
Ватутин Владимир Алексеевич;

кандидат физико – математических наук
профессор
Смирнов Сергей Николаевич.

Ведущая организация: ***Московский государственный институт электроники и математики.***

Защита диссертации состоится 29 мая 2009 г. В 11 часов на заседании диссертационного совета Д 501.001.44 в Московском государственном университете имени М.В. Ломоносова по адресу: 119991, ГСП – 1, г. Москва, Ленинские горы, МГУ им. М.В. Ломоносова, 2–ой учебный корпус, факультет ВМиК, аудитория 685.

С диссертацией можно ознакомиться в библиотеке факультета вычислительной математики и кибернетики МГУ.

С текстом автореферата можно ознакомиться на портале ВМиК МГУ им. М.В.Ломоносова http://cs.msu.ru в разделе «Наука» – «Работа диссертационных советов» – «Д 501.001.44».

Автореферат разослан “ ” апреля 2009 г.

Ученый секретарь
диссертационного совета
профессор Н.П. Трифонов

Общая характеристика работы

Актуальность темы. Во многих случаях приходится иметь дело с системами, состояния которых характеризуются количеством определенных частиц, которые могут исчезать или превращаться в другие частицы. Превращения частиц наблюдаются в космических излучениях, в биологических системах (популяции бактерий), распространение эпидемий, в технических системах (уязвимости в корпоративных сетях). Превращения частиц носят случайный характер, поэтому изменение состояния таких систем естественно описывать с помощью определенных классов случайных процессов – ветвящихся. В начале исследований ветвящихся процессов в качестве объекта рассматривались две модели: процесс Гальтона – Ватсона (каждая частица, существующая в целочисленный момент времени, независимо от предыстории и эволюции остальных частиц производит случайное число частиц - потомков) и марковский ветвящийся процесс с непрерывным временем (обобщение процесса Гальтона – Ватсона, в котором предполагается, что превращения частиц происходят в любой момент времени). Описанию этих процессов посвящены отдельные главы в монографиях Т. Е. Харриса, Б.А. Севастьянова[1], И.И. Гихмана и А.В. Скорохода, К.В. Athreya и P.E. Ney[2].

Обобщением этих моделей является ветвящийся процесс с иммиграцией, в котором наряду с размножением и превращением частиц имеется постоянный приток частиц извне, управляемый случайным механизмом, не зависящим от числа существующих частиц (М.С. Бартлетт, Б.А. Севастьянов, S. Karlin и J. VcGregor). Для процессов Гальтона – Ватсона, марковских ветвящихся процессов и ветвящихся процессов с иммиграцией изучались различные характеристики и предельные теоремы.

---

[1] Севастьянов Б.А. Ветвящиеся процессы. – М.: Наука. – 1971. –436с.

[2] Athreya K.B., Ney P.E. Branching process. – Berlin: Springler – Verlag. – 1972 – 285p.

Недавно, В.В. Горяйнов предложил новый подход к изучению ветвящихся процессов с дискретным пространством состояний посредством полугрупп вероятностных производящих функций относительно операции композиции. В его работах[3] изучена структура полугруппы вероятностных производящих функций и решена известная задача вложения процесса Гальтона – Ватсона в однородный марковский ветвящийся процесс[4]. Также были решены и другие задачи[5].

При исследовании различных предельных теорем теории вероятностей одним из центральных является вопрос описания предельного множества. Предельные теоремы для некоторых ветвящихся процессов с иммиграцией были получены Б.А. Севастьяновым, В.А. Ватутиным, С.В. Нагаевым, Е. Сенета, К.В. Митовым, Ш.К. Формановым и Р.Х. Ибрагимовым. Известно, что докритические ветвящиеся процессы с иммиграцией сходятся к дискретной случайной величине. В работе получено описание допустимых диапазонов предельного распределения вероятностей и построен процесс, который имеет заданную предельную производящую функцию. Для прикладных задач важен вопрос построения процесса с заданным конечным набором начальных вероятностей предельного распределения, который эквивалентен задаче нахождения производящей функции, имеющей заданный набор начальных коэффициентов.

Для однородных марковских ветвящихся процессов интересным представляется нахождение оценок распределения момента вырождения. Т. Е. Харрис отмечал, что в общем случае нелегко определить распределение момента

---

[3] Горяйнов В.В. Полугруппы аналитических функций и ветвящиеся процессы//ДАН СССР 318(1991). – С.1046 – С.1049.

[4] Горяйнов В.В. Дробное итерирование вероятностных производящих функций и вложение дискретных ветвящихся процессов в непрерывные// Матем. Сб. – 1993. – т.194. – N5. – С.55 – С. 72.

[5] Горяйнов В.В. Эволюционные семейства аналитических функций и неоднородные по времени марковские ветвящиеся процессы// Докл. РАН. – 1996. – т.347. – N6. – С.729 – С.731.

вырождения явно[6]. M. Sze[7] получил оценки распределения момента вырождения для вложимого критического процесса Гальтона-Ватсона. Эти оценки можно получить в общем случае, используя подход В.В. Горяйнова.

Марковские ветвящиеся процессы находят широкое применение в различных прикладных областях. В связи с развитием автоматизированных систем, важным является обеспечение информационной безопасности этих систем. Большинство существующих моделей злоумышленника[8] построены на основе конечных автоматов и вероятностных конечных автоматов и используются для решения задач представления атак на информационную систему, оценки сложности атаки, оценке ущерба от проведенной атаки, но не предоставляют средств для автоматизированного моделирования атак с целью исследования их оптимизации. Поэтому, актуальным является построение формальных моделей злоумышленников, имеющих эти средства.

Цель диссертации.

Решение некоторых задач теории ветвящихся процессов на основе подхода, предложенного В.В. Горяйновым и построение математических моделей злоумышленника в информационной системе, предоставляющих средства автоматизированного моделирования атак.

Научная новизна. Все основные результаты диссертации являются новыми и состоят в следующем:

1. Описание допустимых диапазонов предельных распределений вероятностей и решение интерполяционных задач для докритических ветвящихся процессов с иммиграцией.

---

[6] Харрис Т.Е. теория ветвящихся случайных процессов. – М: Мир. – 1966. – 356с.

[7] Sze M. Markov processes associated with critical Galton – Watson process with application to extinction probabilities//Adv. Appl. Probab. – 1976. – v.8. – N2. –P.278 – P.295.

[8] Schneier B. Attack Trees//Dr. Dobb's Journal. – 1999;

2. Получение оценок распределения момента вырождения для однородных марковских ветвящихся процессов.

3. Построение математической модели действий злоумышленника на основе предельного распределения вероятностей докритического однородного марковского ветвящегося процесса.

4. Разработка и исследование математической модели действий злоумышлен – ника на основе марковских ветвящихся процессов, учитывающих, что процесс устранения уязвимостей может происходить как в результате доработки программного и/или аппаратного обеспечения, так и в результате проводимой политики безопасности.

Методы исследования.

В работе применяются методы теории вероятностей, теории ветвящихся процессов, теории аналитических функций, методы статистического моделирования.

Теоретическая и практическая значимость.

Работа носит теоретический и практический характер. Ее результаты могут быть полезны в теории ветвящихся процессов. Модели злоумышленника, построенные на основе марковских ветвящихся процесов могут использоваться для автоматического моделирования атак на информационную систему и определения наиболее вероятных маршрутов действий злоумышленника с целью выработки рекомендаций по закрытию уязвимых мест.

Апробация работы. Основные результаты докладывались на:

- на V, X, XIV Всероссийской школе – коллоквиуме по стохастическим методам (г. Йошкар-Ола 1998, г. Сочи 2003, г. Сочи 2007)
- IV международной конференции «Методы и средства управления

технологическими процессами» (г. Саранск 2007)

- на семинаре отдела дискретной математики МИАН им. В.А. Стеклова (г. Москва)
- на семинаре кафедры прикладной математики и информатики ВГИ «Аналитические методы и компьютерное моделирование» под рук. д. ф.-м .н. Горяйнова В.В. и к. ф.-м. н. Батхина А.Б. (г. Волжский).

Публикации. Результаты диссертации опубликованы в 6 работах, список которых приведён в конце автореферата.

Структура и объем диссертации.

Диссертация состоит из введения, двух глав, разбитых на параграфы, заключения, списка литературы. Текст изложен на 76 страницах. Список литературы включает 49 наименований.

Краткое содержание диссертации

Во введении приведен обзор по тематике работы, изложены цели исследования, а также перечислены основные полученные результаты.

Первая глава посвящена описанию допустимых диапазонов предельного распределения вероятностей докритических ветвящихся процессов с иммиграцией и нахождению оценок распределения момента вырождения однородных марковских ветвящихся процессов.

В §1.1 приводятся основные результаты В.В. Горяйнова о полугруппах вероятностных производящих функций и их структуре.

В §1.2 описывается множество предельных распределений вероятностей докритического марковского ветвящегося процесса с иммиграцией $\mu(t)\left(\mu(0)=0\right)$. Пусть $f^t(z)=\sum_{k=0}^{\infty}P_k(t)z^k$ - производящая функция этого

процесса ($P_k(t) = P(\mu_t = k)$, $P_k(t) \geq 0$, $k = 0, 1, \ldots$, $\sum_{k=0}^{\infty} P_k(t) = 1$);

$f(z) = \sum_{k=0}^{\infty} p_k z^k$ – инфинитезимальная производящая функция эволюции частиц ($p_1 < 0$, $p_k \geq 0$ при $k \neq 1$, $\sum_{k=0}^{\infty} p_k = 0$); $g(z) = \sum_{k=0}^{\infty} q_k z^k$ - инфинитезимальная производящая функция иммиграции частиц ($q_0 < 0$, $q_k \geq 0$ при $k \neq 0$, $\sum_{k=0}^{\infty} q_k = 0$).

Отправным пунктом проведенных исследований является следующая предельная теорема.

Теорема А (Севастьянов Б.А.) Если $f'(1) < 0$, $g'(1) < \infty$, *то существуют пределы* $\lim_{t\to\infty} P_k(t) = P_k$ ($P_k \geq 0$ *при* $k = 0, 1, 2, \ldots, \sum_{k=0}^{\infty} P_k = 1$) *и производящая функция* $F(z) = \sum_{k=0}^{\infty} P_k z^k$ *удовлетворяет уравнению* $F(z) = \exp\left\{\int_z^1 \frac{g(x)}{f(x)} dx\right\}$.

Если закон иммиграции $g(z)$ зафиксирован, то справедлива следующая теорема.

Теорема 1. *Пусть выполняются условия теоремы А. Для того чтобы распределение вероятностей* $P_0, P_1, P_2, \ldots$ ($\sum_{n=1}^{\infty} nP_n < \infty$) *являлось предельным, необходимо и достаточно, чтобы выполнялась следующая система неравенств:*

$$0 < P_0 < 1, \qquad 0 < P_1 < 1, \qquad \frac{1}{2}\frac{P_1^2}{P_0} + \frac{1}{2}\left(\frac{q_1}{q_0} + 1\right)P_1 < P_2 < 1,$$

$$\omega_2 = -\frac{1}{\alpha}\sum_{k=0}^{2} q_k P_{2-k} + 2P_2 - 3P_3\sigma \geq 0,$$

$$\omega_n = -\frac{1}{\alpha}\sum_{k=0}^{n} q_k P_{n-k} - (n+1)\sigma P_{n+1} + nP_n - \frac{1}{P_1}\sum_{k=2}^{n-1}(n-k+1)\omega_k P_{n-k+1} \geq 0,\ n = 3,4,\ldots,$$

$$\sum_{n=2}^{\infty} n\omega_n < P_1, \text{ где } \sigma = -\frac{q_0 P_0}{\alpha P_1},\ \alpha = \frac{1}{P_1}\left(q_0 P_1 + q_1 P_0 - \frac{2q_0 P_0 P_2}{P_1}\right).$$

В §1.3 исследуется вопрос существования инфинитезимальных произво – дящих функций $f(z)$ в предельной *теореме А* для докритических ветвящихся процессов с иммиграцией, которая имела бы заданные начальные коэффициенты. В связи с этим вводится в рассмотрение предельная интерполяционная задача, которую впервые для докритических марковских ветвящихся процессов определили В.В. Горяйнов и А.А. Полковников[9].

Определение. *Пусть заданы последовательности чисел* $\{i_k : i_k \in N, k = 0,...,n, \ i_l \neq i_m, \ l \neq m\}, \{d_k : d_k \geq 0, \ \sum_{k=0}^{n} d_k \leq 1\}$ *и инфинитезимальная производящая функция иммиграции* $g(z)$. *Будем говорить, что предельная интерполяционная задача* $\{i_0, ..., i_n, g(z); d_0, d_1, ..., d_n\}$ *непрерывно разрешима, если найдется такой докритический ветвящийся процесс* $\mu(t)$ *с инфинитезимальной производящей функцией* $f(z)$, *что* $d_k = \lim_{t\to\infty} pr(\mu(t) = i_k)$, $k = 0,1,2,...,n$.

Процесс $\mu(t)$, *удовлетворяющий этим условиям, будем называть решением поставленной предельной интерполяционной задачи.*

В работе получены необходимые и достаточные условия непрерывной разрешимости задач $\{0, 1, 2, g(z); x_0, x_1, x_2\}$ и $\{0,1,2\ldots,m, g(z); P_0, P_1,\ldots,P_m\}$.

Теорема 2. *Предельная интерполяционная задача* $\{0, 1, 2, g(z); x_0, x_1, x_2\}$ *разрешима тогда и только тогда, когда выполняется система неравенств*

$$0 < x_0 < 1, \quad 0 < x_1 < 1,$$

$$\frac{1}{2}\frac{x_1^2}{x_0} + \frac{1}{2}\left(\frac{q_1}{q_0} + 1\right)x_1 < x_2 < \frac{1}{2}\frac{x_1^2}{x_0} + \frac{1}{2}\left(\frac{q_1}{q_0} + 2\right)x_1.$$

[9] Горяйнов В.В., Полковников А.А. О предельных распределениях вероятностей докритических ветвящихся процессов//Теория вероятностей и ее применение. – 1996. – т.41. – вып.2. – С.417 – С.425.

Теорема 3. *Предельная интерполяционная задача* $\{0,1,2\ldots,m,\ g(z);\ P_0,\ P_1,\ldots,P_m\}$, $m \geq 3$, *разрешима тогда и только тогда, когда выполняется система неравенств* $0 < P_0 < 1, \quad 0 < P_1 < 1,$

$$\frac{1}{2}\frac{P_1^2}{P_0} + \frac{1}{2}\left(\frac{q_1}{q_0} + 1\right)P_1 < P_2 < \frac{1}{2}\frac{P_1^2}{P_0} + \frac{1}{2}\left(\frac{q_1}{q_0} + 2\right)P_1,$$

$$\max\{0,(n+1)b_n - a_n\} \leq \omega_n \leq b_n, \quad n = 2,\ldots,m-1,$$

где $0 < a_2 < P_1$, $b_2 = P_1(1-\sigma)$ *и* $a_n = a_2 - \sum_{k=2}^{n-1} k\omega_k$, $b_n = b_2 - \sum_{k=2}^{n-1}\omega_k$, $\quad n = 3,4,\ldots,m$,

а числа $\sigma, \omega_k, k = 2,3,\ldots,m-1$, *определяются через* $P_0, P_1,\ldots,P_m$ *так же, как и в теореме 1.*

В заключительном §1.4 первой главы приводятся найденные асимптотически точные оценки распределения момента вырождения $\tau = \inf\{t : \xi_t = 0\}$ $(\inf \phi = \infty)$ для однородных марковских ветвящихся процессов ξ_t с непрерывным временем.

Если процесс ξ_t с инфинитезимальной производящей функцией $v(z)$ докритический или критический, то справедлива следующая теорема.

Теорема 4. *Если* $v'(1) \leq 0$ *и* $v'(0) = -1$, *то*

$$e^{-t} \leq P\{\tau > t\} \leq \frac{2}{2+t}.$$

В случае надкритического процесса $P\{\tau = \infty\} = 1 - q$, где $q = \lim_{t\to\infty} P\{\xi_t = 0\}$ вероятность вырождения процесса. Поэтому в случае надкритического процесса и $0 < q < 1$ через $F_\tau(t)$ обозначим условную функцию распределения

$$F_\tau(t) = P\{\tau \leq t \mid \tau < \infty\} = \frac{1}{q}P\{\tau \leq t\}.$$

Случай $q = 0$ — тривиален, поскольку для него $P\{\tau \neq \infty\} = 0$.

Для надкритического процесса ξ_t верна следующая теорема.

Теорема 5. *Если* $v'(1) > 0$ *и* $v'(0) = -1$, *то*

$$e^{-t} \le 1 - F_\tau(t) \le \frac{1-q}{g(t,q)-q}$$

где q — наименьший неотрицательный корень уравнения $v(z) = 0$ *(0<q<1) и* $g(t,q) = \exp\{t(1-q)/(1+q)\}$.

Вторая глава посвящена построению и исследованию моделей злоумышленников, построенных на основе марковских ветвящихся процессов.

В §2.1 описываются существующие в настоящее время модели: деревья атак, улучшенные деревья атак, графы атак, специального типа высокоуровневые конечные автоматы Interacting State Mashines (ISM), позволяющие с разной степенью детализации описывать процесс сетевой атаки. Модели используют разную математическую базу, но большинство из них основаны на конечных автоматах и представляют атаку на автоматизированную систему как последовательность состояний автомата. Существующие методы моделирования атак направлены на решение задач представления атак, оценки сложности атаки, оценке ущерба от проведенной атаки, но не предоставляют средств для автоматизированного моделирования атак с целью исследования их оптимизации.

В §2.2 описана модель дерева атак на основе докритических однородных марковских ветвящихся процессов.

Злоумышленник обычно предваряет свои атаки предварительным зондированием всех компонентов корпоративной системы (КС). На этом этапе он собирает информацию, которая является недоступной для него в рамках служебных полномочий. На практике злоумышленником определяются роли компьютеров в корпоративной сети, выделяются файловые сервера и сервера баз данных, маршрутизаторы и интеллектуальные коммутаторы. На основе этой информации злоумышленником строится дерево уязвимостей КС. И, что особенно важно, им выбирается инструментарий для проведения атак,

например, подбираются эксплойты для осуществления непосредственно атак на узлы корпоративной сети.

Пусть случайные величины $Z_0, Z_1, Z_2, \ldots$ - число уязвимостей в нулевом, первом, втором, и.т.д. уровнях защиты корпоративной сети соответствует числу вершин (состояний) корневого ориентированного дерева уязвимостей (дерева угроз). Дугам дерева уязвимостей приписаны вероятности перехода из состояния i – го уровня защиты в состояние i+1 – го уровня. Длительность пребывания в каждом состоянии нулевого, первого, и.т.д. уровнях защиты равна соответственно $T_0, T_1, T_2, \ldots$.

Пусть $Z_0=1$ с вероятностью 1 и математическое ожидание количества уязвимостей на первом уровне защиты $EZ_1 < 1$. Обозначим через P вероятностную меру . Тогда закон распределения вероятностей сл.в. Z_1

$$P\{Z_1 = k\} = p_k\ ,\ k=0,1,2,\ldots \text{ и}$$

$\sum p_k = 1$, где p_k интерпретируется как вероятность того, что уязвимость, существующая на первом уровне защиты, обеспечивает доступ к уязвимостям на втором уровне.

При определении вероятностей, с которыми злоумышленник выбирает соответствующую ветвь дерева, будем использовать решение предельной интерполяционной задачи докритических однородных марковских ветвящихся процессов, которое получено В.В. Горяйновым и А.А. Полковниковым.

Отметим, что при определении вероятности того, что злоумышленник не сможет использовать уязвимости для проведения атак за заданное время, необходимо учитывать тип дерева уязвимостей. Рассматривается три основных типа: двоичное, троичное и m-арное деревья уязвимостей (могут быть использованы и смеси деревьев):

- Если дерево уязвимостей КС является двоичным, то злоумышленник выбирает для атаки уязвимость в левом узле с вероятностью $p_1=x$, а правую - с $p_2=y$. Вероятности x и y выбираются из условий:

$$0<x<1\ ,\ x\ (1-x)/2<y \le x\ (1-x).$$

- Если дерево уязвимостей КС является троичным деревом, злоумышленник выбирает для атаки уязвимость в левом узле с вероятностью $p_1=x$, а правую с вероятностью $p_3= y$. Вероятности x и y удовлетворяют системе неравенств:

$$\begin{cases} 0 < x < 1 \\ 0 < y \le x\,(1-x)^2, & \text{если } 0 < x \le ½ \\ 0 < y \le ¼\ x\,(1-x)(3-2x), & \text{если } ½ < x < 1 \\ 1 > y > 1/6\ x\,(1-x)(2-x), & \text{если } 0 < x \le 2/3 \\ 1 > y > 1/48\ x\,(12-12x-x^2), & \text{если } 2/3 < x \le 6/7 \\ 1 > y > x\,(1-x), & \text{если } 6/7 < x < 1. \end{cases}$$

- Если дерево уязвимостей КС является m - арным деревом то злоумышленник выбирает для атаки уязвимости в соответствующих узлах 1, 2, …m с вероятностями $p_1= b_1,\ p_2= b_2,\ \ldots,\ p_m= b_m$, $m \ge 3$, которые удовлетворяют следующим условиям:

$$\begin{cases} 0 < b_1 < 1,\ \dfrac{1}{2} b_1(1-b_1) < b_2 \le b_1(1-b_1) \\ \sigma = \dfrac{b_1}{b_1^2 + 2b_2},\ \lambda = b_1\sigma,\ \alpha_2 = b_1(1-\lambda),\ \beta_2 = b_1(1-\sigma) \\ \max\{0, (n+1)\beta_n - \alpha_n\} \le \nu_n \le \beta_n,\ n = 2,3,\ldots m \\ \alpha_n = \alpha_2 - \sum\limits_{k=2}^{n-1} k\nu_k,\ \beta_n = \beta_2 - \sum\limits_{k=2}^{n-1} \nu_k \beta_n,\ n = 3,4,\ldots,m. \end{cases}$$

Тогда вероятности b_k , $k=3,4,\ldots,m$ находятся из равенства:

$$\nu_k = (k-\lambda) b_k - (k+1)\sigma b_{k+1} - \frac{1}{b_1} \sum_{n=2}^{k-1} (k-n+1)\nu_n b_{k-n+1}\ .$$

Эта модель является средством автоматического моделирования атак и позволяет находить наиболее вероятный путь достижения цели злоумышленником за заданное время.

Модель злоумышленника, описанная в §2.2 не учитывает то, что уязви–

мости в корпоративной сети могут быть устранены, как путем доработки программного и/или аппаратного обеспечения, так и в результате проводимой политики безопасности.

В §2.3 разработана и исследована модель злоумышленника, учитывающая указанные ограничения.

Пусть в начальный момент времени $t = 0$ численность целей $Z(0)$ для атак злоумышленника в автоматизированной системе неслучайна, множества целей $Y(0)$ и уязвимостей $X(0)$, ведущих непосредственно к целям фиксировано. Злоумышленник при положительном воздействии на уязвимости x ($x \in X(0)$), может получить сразу доступ к множеству целей. Однако получить доступ к этим уязвимостям можно только после успешного проведения атак на уязви–мости, расположенные на нижних уровнях дерева. Этот процесс можно представить как процесс размножения уязвимостей $X(0)$ и использовать для его описания и исследования модель, разработанную в §2.2.

Будем предполагать, что воздействия злоумышленника происходят лишь в фиксированные моменты времени $t_k = kT$, $T = const > 0$, $k \in N$. Уязвимость x, существуя до момента времени t_k - 0, в момент t_k производит $\pi_x^{(k)}$ потомков, где величины $\pi_x^{(k)}$, $k \in N$, $x \in X$, независимы, одинаково распределены $\mathrm{P}\{\pi_x^{(1)} = n\} = p_n$, $n \in \mathrm{Z}_+$, $\mathbf{E}\pi_x^{(1)} = \sum_{n=0}^{\infty} np_n = m < +\infty$.

Процесс устранения x - уязвимости может происходить как в результате доработки программного и/или аппаратного обеспечения), так и в результате проводимой политики безопасности. Поэтому, момент устранения δ_x x - уязвимости определяется следующим равенством

$$\delta_x = \sigma_x + \min\{l_x, \rho_x\},$$

где σ_x - момент появления (рождения) x - уязвимости в автоматизированной системе, l_x - продолжительность жизни x - уязвимости до момента гибели вследствие модернизации программного и/или аппаратного обеспечения , а

ρ_x - продолжительность жизни x - уязвимости до момента гибели вследствие применяемой политики безопасности.

Следовательно, процесс роста числа уязвимостей достижимых из x - уязвимости за время $[0;t]$: $\xi_x(t) = \sum_{k=1}^{[t/T]} \varepsilon_x(t_k - 0)\pi_x^{(k)}, t \geq 0$ и $\varepsilon_x(t) = I\{\sigma_x \leq t < \delta_x\}$ - индикатор уязвимости x.

В дальнейшем будем предполагать, что случайные величины l_x одинаково распределены для всех (кроме существовавших первоначально) уязвимостей, независимы в совокупности и не зависят от случайных величин $\pi_x^{(k)}$, $k \in N$, $x \in X$. Обозначим через $L_0(\alpha) = \mathrm{P}\{l_x > \alpha\}$ функцию распреде – ления сл.величин l_x для первоначально существующих уязвимостей $x \in X(0)$, а через $L(\alpha) = \mathrm{P}\{l_x > \alpha\}$ – функцию распределения сл.величин l_x для остальных уязвимостей $x \notin X(0)$. Здесь и далее аргумент α будет использоваться для обозначения возраста уязвимости.

Случайная величина ρ_x имеет экспоненциальное распределение с постоянной интенсивностью $\gamma \geq 0$: $\mathrm{P}\{\rho_x > \alpha \mid \sigma_x, Z_x\} = e^{-\gamma\alpha}$ (п.н.) и не зависит от σ_x и Z_x.

В соответствии с приведенным построением, тройки $\{(l_x, \rho_x, \xi_x(\cdot))\}_{x \in X}$ независимы в совокупности и случайный процесс $Z(t)$ - ветвящийся.

Обозначим $\xi_x = \xi_x(\infty)$ — число уязвимостей - потомков, достижимых (произведенных) x – уязвимостью за все время своего существования. Справедливо следующее предложение.

Предложение. Уравнение $\mathbf{E}\xi_x = 1$ *имеет единственный действительный корень.*

Сравнение с единицей математического ожидания случайной величины ξ_x является основным условием для классификации процессов Z(t). Процесс $Z(t)$

будет докритическим при $\mathbf{E}\xi_x < 1$, критическим при $\mathbf{E}\xi_x = 1$ и надкритическим при $\mathbf{E}\xi_x > 1$.

Моделирование дерева атак предлагается проводить численно методом Монте - Карло. При разработке алгоритма моделирования считается известным распределение момента ς_s ближайшего устранения уязвимости вследствие проводимой политики безопасности, начиная от момента $t = s$. Фиксируется $s \geq 0$. В множестве уязвимостей выделяются два подмножества: $X^{-s} = \{x : \delta_x \leq s\}$ и $X^{s+} = \{x : \delta_x > s\}$. В первое подмножество входят те уязвимости, которые устранены до момента *s* включительно, а во второе — все остальные. Для всех $x \in X^{s+}$ заменяются процессы $\varepsilon_x(t)$ и $\xi_x(t)$ на $\varepsilon_x^*(t)$ и $\xi_x^*(t)$ и определяются новые случайные процессы, которые показывают динамику развития множества уязвимостей:

$$Z_s(t) = \sum_{x \in X^{s+}} \varepsilon_x^*(t) + \sum_{x \in X^{-s}} \varepsilon_x(t), t > 0$$

и $X_s(t) = \{x \in X^{s+} : \varepsilon_x^*(t) = 1\} \cup \{x \in X^{-s} : \varepsilon_x(t) = 1\}$, $t \geq 0$, если, начиная с момента $t = s$, перестанет действовать проводимая политика безопасности. Процесс $Z_s(t)$ при $t \geq s$ является ветвящимся.

Пусть $t \geq s$ и $h > 0$. Если $s \leq t < \varsigma_s$, то $\varepsilon_x(t) = \varepsilon_x^*(t)$ для всех $x \in X^{s+}$. Следовательно, $Z(t) = Z_s(t)$ и $X(t) = X_s(t)$. Поэтому,

$$\mathrm{P}\{\varsigma_s > t \mid Z_s\} = e^{-\int_s^t Z_s(u)\lambda(Z_s(u))du} \text{ (п.н.), } t \geq s,\ \lambda(Z_s(u)) = \gamma.$$

В момент ς_s процессы $Z(t)$ и $X(t)$ терпят скачок: вследствие проводимой политики безопасности устраняется одна уязвимость из X. Обозначим эту уязвимость через ψ_s. Тогда

$$Z(\varsigma_s) = Z(\varsigma_s - 0) - 1 = Z_s(\varsigma_s - 0) - 1, X(\varsigma_s) = X(\varsigma_s - 0) - \psi_s = X_s(\varsigma_s - 0) - \psi_s.$$

Доказано, что случайная величина равномерно распределена на $X(\varsigma_s - 0)$.

Отдельные реализации процесса $Z(t)$ находятся с применением

алгоритма прямого моделирования. Для моделирования случайных величин l_x использован метод обратных функций. Вычисление функций $L_0^{-1}(\cdot)$ и $L^{-1}(\cdot)$ не является слишком трудоемким.

Для моделирования величин $\pi_x^{(k)}$ промежуток $[0;1)$ разбивается на промежутки

$$\Delta_1 = [0; q_1), \Delta_2 = [q_1; q_2), \Delta_3 = [q_2; q_3),...,$$

где $q_n = p_1 + ... + p_n$, и применяется формула $\pi_x^{(k)} = n$, если $\alpha \in \Delta_n$.

На практике количество вероятностей p_n, отличных от нуля, как правило, конечно.

Для моделирования величины ς_s используется модель, аналогичная модели свободного пробега нейтрона в кусочно - постоянной среде. Для определения ς_s решается уравнение

$$e^{-\int_s^{\varsigma_s} Z_s(u)\lambda(Z_s(u))du} = \alpha.$$

Пусть $s = u_0 < u_1 < u_2 < ... < u_{m-1}$ - моменты скачков процесса Z_s. Находится максимальное *m* такое, что

$$I_m = \int_s^{u_m} Z_s(u)\lambda(Z_s(u))du = \sum_{i=0}^{m-1} Z_s(u_i)\lambda(Z_s(u_i))(u_{i+1} - u_i) \le -\ln(\alpha).$$

Тогда ς_s вычисляется по формуле:

$$\varsigma_s = u_m + \frac{-\ln(\alpha) - I_m}{Z_s(u_m)\lambda(Z_s(u_m))}$$

и полагаем $\varsigma_s = \infty$, если $Z_s(u_m)\lambda(Z_s(u_m)) = 0$. В модели моменты $u_0, u_1, u_2,...$ вычисляются последовательно как моменты скачков процесса $Z_s(t)$, то есть процесса, который описывает множество уязвимостей без проводимой политики безопасности.

Так как, случайная величина ψ_s равномерно распределена, то в качестве ψ_s можно выбрать уязвимость с номером $[\alpha Z(\zeta_s - 0)]$. По построенному дереву

атак определяются наиболее вероятные пути достижения цели злоумышленником.

В **заключении** перечислены основные результаты диссертации.

Автор выражает благодарность своему научному руководителю д. ф.-м.н. В.В. Горяйнову за постановку задач, внимание и критические замечания, к.т.н А.В. Цыбулину за консультации и обсуждение результатов.

Работы автора по теме диссертации

[1] Шипилева А.В. *Предельные распределения для ветвящихся процессов с иммиграцией.*// Обозрение прикладной и промышленной математики. - 1998. -т.5. - вып.2. - С.297-298.

[2] Шипилева А.В. *Предельные распределения для ветвящихся процессов с иммиграцией.*// Известия высших учебных заведений. Математика. - 2000. - № 1(452). - С.77 - С.83.

[3] Шипилева А.В. *Оценка распределения момента вырождения марковского ветвящегося процесса.*// Теория вероятностей и ее применение. - 2000. -т.45. - вып.4. С.776-779.

[4] Цыбулин А.М., Шипилева А.В. *Математическая модель злоумышленника в корпоративной сети.* - Сборник трудов. Управление большими системами ИПУ им. В.А.Трапезникова РАН. - 2007. - вып.19. -С.127-133.

[5] Цыбулин А.М., Шипилева А.В. *Синтез модели дерева атак на автоматизированную систему.//* Материалы IV межд. конф. Методы и средства управления технологическими процессами. - 2007. - С.191-194.

[6] Цыбулин А.М., Шипилева А.В. *Математическая модель дерева атак на автоматизированную систему.*// Обозрение прикладной и промышленной математики. - 2008. - т.15. - вып.1. - С.183-184.