ЗАЩИТА ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.001.57

В.А. Минаев[1]
В.С. Журавлев[2]

МОДЕЛИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ОБЪЕКТОВ ОТ УГРОЗ НЕПОСРЕДСТВЕННОГО И УДАЛЕННОГО ДОСТУПА

Рассматривается возможность интегрирования моделей защиты информационно-телекоммуникационных объектов от угроз непосредственного и удаленного доступа, входные потоки которых в первом случае описываются линейно, с заданием определенных параметров, и записаны в виде системы линейных уравнений с моделью, в которой входные потоки описываются нелинейными функциями, что обуславливает создание модели защиты в наиболее реальных условиях. При интеграции обоих примеров получим совершенно новую модель на основе идеи профессора Минаева В.А. с описанием входных потоков нелинейными функциями.

***Ключевые слова**: информационно-телекоммуникационная система (ИТКС), субъект атаки, реализация атаки, математическое моделирование, закон распределения, интенсивность атаки.*

V.A. Minaev
V.S. Zhuravlev

MODELLING SYSTEM PROTECTION OF INFORMATION AND TELECOMMUNICATION FACILITIES FROM THREATS OF DIRECT AND REMOTE ACCESS

The possibility of integrating the model for protecting information and telecommunication facilities from the threat of direct and remote access, input streams, which in the first case described by linear, with the assignment of certain parameters, and recorded in the form of a system of linear equations with a model in which the input streams are described by nonlinear functions that causes the creation of a model of protection in the most realistic conditions. With the integration of the two examples, we get quite new model, based on the ideas of Professor Minaev V.A., with a description of nonlinear functions of the input streams.

***Keywords**: Information and Telecommunications System (ITCS), the subject of attack, the implementation of the attack, mathematical modeling, distribution law, the intensity of the attack.*

Постановка задачи. Исследование и разработка модели защиты от угроз в сфере информационных технологий, которая необходима для анализа вероятности реализации атаки на информационно-телекоммуникационный объект. Модель защиты от угроз непосредственного и удаленного доступа будет рассмотрена нами в условиях реальных событий.

Для эффективной реализации безопасности передаваемых информационных сведений по конкретным (описанным и предложенным заранее) каналам связи необходимо создание совершенной модели, основанной на ранних разработках предыдущих специалистов.

[1] Доктор технических наук, профессор, проректор НОУ ВПО «Российский новый университет».

[2] Аспирант НОУ ВПО «Российский новый университет».

Предложенный, ниже в работе, проект модели основывается на идеях профессора Минаева Владимира Александровича

На основе полученных знаний предлагаю проект модели, разработанной мной в рамках подготовки первой главы диссертационной работы. Для создания модели защиты мной были изучены диссертационная работа Остапенко Г.А. «Топологические модели информационных операций в социотехнических системах: аспект региональной безопасности» и диссертационная работа Радько Н.М. «Методология риск-анализа несанкционированного доступа и управления эффективностью информационно-телекоммуникационных систем критических приложений в условиях конфликта». Основная работа будет основываться на интеграции в модель защиты, описанную в диссертационной работе Остапенко Г.А., модели, описанной в диссертационной работе Радько Н.М.

Г.А. Остапенко описывает модель защиты и параметры в системе обеспечения информационной безопасности региона. Данная модель имеет аналитический подход.

Рассмотрев актуальность предложенной темы, можем составить аналитический подход к рассматриваемой проблеме. Модель описывает процессы информационных операций (в конкретном региональном аспекте). В общем виде взаимодействия описываются системой уравнений:

$$R = R \times (R_T, R_S, F_R)$$
$$R_S = R_S \times (R_T)$$
$$R_T = R_T \times (T)$$
$$T = T \times (O, R, F_T)$$
$$O = O \times (R_S, F_O), \quad (1.1)$$

где R – общий региональный ресурс;

R_T – ресурсные потери из-за реализованных информационных угроз;

R_S – часть регионального ресурса, затрачиваемая на создание и функционирование систем информационной безопасности;

T – множество информационных угроз региональному ресурсу;

O – множество объектов уязвимостей регионального ресурса;

F_R, F_O, F_T – факторы внешней среды, определяющие состояние и динамику регионального ресурса, его уязвимости информационных угроз [1, с. 26].

После подстановки значимых параметров модель представляет систему из трех динамических уравнений

$$R_{(t+1)} = R(t) - A_1(t) \times T(t) + A_2(t) \times F_R(t)$$
$$T_{(t+1)} = A_3(t) \times O(t) + A_4(t) \times R(t) + A_5(t) \times F_T(t)$$
$$O_{(t+1)} = O(t) - A_7(t) \times T(t) + A_8(t) \times F_O(t) \quad (1.2)$$

с начальными условиями $R(0) = R_O, T(0) = T_O, O(0) = O_O$,

где $A_1(t) = a_3(t) \times [1 + a_2(t)]$; $A_2(t) = a_1(t)$; $A_3(t) = a_4(t)$; $A_4(t) = a_5(t)$;

$A_5(t) = a_6(t)$; $A_7(t) = a_2(t) \times a_3(t) \times a_7(t)$;

$A_8(t) = a_8(t)$.

Приведя к дифференциальной форме уравнений (коэффициенты постоянны, начальные условия нулевые):

$$\frac{dR}{dt} = b_1 \times T(t) + F_1(t),$$
$$\frac{dT}{dt} = b_2 \times O(t) + b_3 \times R(t) + F_2(t),$$
$$\frac{dO}{dt} = b_4 \times T(t) + F_3(t), \quad (1.3)$$

где $R(0) = T(0) = O(0) = 0$; $b_1 = -a_3[1 + a_2]$; $b_3 = a_4$; $b_4 = -a_2 \times a_3 \times a_7$;

временные функции $F(t) = A_2(t) \times F_2(t)$; $F_2(t) = A_5(t) \times F_t(t)$; $F_3(t) = A_8(t) \times F_O(t)$.

По определению, все коэффициенты a_i – положительны и на некотором временном интервале постоянны.

Перейдем к дифференциальным уравнениям с постоянными коэффициентами, имеем начальное уравнение:

$$\begin{cases} \dot{R} = a_1 \times N + F_1(t) \\ \dot{V} = a_2 \times V + a_3 \times R + F_3(t) \\ \dot{V} = a_4 \times N + F_3(t) \end{cases} \quad (1.4)$$

$$a_1 = -A_1(t)$$
$$a_2 = -A_3(t)$$
$$a_3 = -A_4(t)$$
$$a_4 = -A_7(t)$$
$$F_1(t) = -A_2(t) \times F_R(t)$$
$$F_2(t) = -A_5(t) \times F_N(t)$$
$$F_3(t) = -A_8(t) \times F_V(t)$$
$$\dot{R} = \dot{x}_1$$
$$\dot{N} = \dot{x}_2$$
$$\dot{V} = \dot{x}_3$$
$$\dot{x}_1 = a_1 \times x_2 + F_1(t)$$
$$\dot{x}_2 = a_2 \times x_3 + a_3 \times x_1 + F_2(t)$$
$$\dot{x}_3 = a_4 \times x_2 + F_3(t)$$
$$x_1(0) = x_{10}$$
$$x_2(0) = x_{20}$$
$$x_3(0) = x_{30}.$$

В работе Радько Н.М. описание потоков в модели основывается на законе Пуассона, так как, согласно этому закону, вероятностное распределение дискретного типа моделирует случайную величину, представляющую собой число собы-

тий, произошедших за фиксированное время, при условии, что данные события происходят с некоторой фиксированной средней интенсивностью и независимо друг от друга. А при рассмотрении процессов, протекающих в системе, целесообразно связать с количеством атак различных типов, реализованных на исследуемом интервале времени.

Для формирования модели защиты информации рассмотрим представление схемы предполагаемой атаки на информационно-телекоммуникационную систему:

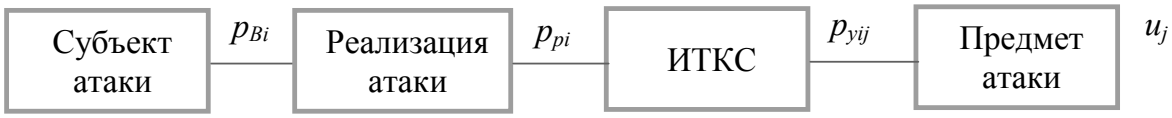

Рис. 1. Схема атаки на ИТКС и ее составляющие параметры,
где p_{Bi} – вероятность появления *i*-ой атаки;
p_{pi} – вероятность реализации *i*-ой атаки;
p_{yij} – вероятность нанесения ущерба вида *j* в результате реализации *i*-ой атаки;
u_j – величина нанесенного ущерба вида *j*

Предлагается рассмотреть вероятность реализации некоторого количества атак, которые распределяются по закону Пуассона:

$$p_k = \frac{(\lambda_0 T)^k}{k!} e^{-\lambda_0 T}, \quad (1.5)$$

где λ_0 – среднее число атак, возникающее в единицу времени (интенсивность);

T – временной интервал, на котором исследуется функционирование системы.

Задаем T, получаем среднее количество возникающих атак на этом интервале $\lambda = \lambda_0 T$:

$$p_k = \frac{\lambda^k}{k!} e^{\lambda}. \quad (1.6)$$

При реализации атаки имеется несколько независимых источников атак с интенсивностью λ_i, тогда получим суммарную интенсивность $\lambda = \sum_i \lambda_i$:

$$p_k = \frac{\sum_i \lambda_i^k}{k!} e^{-\sum_i \lambda_i}. \quad (1.7)$$

Если допустить, что интенсивность на интервале T выражается функцией $\lambda_0(t)$, $t \in T$, тогда средняя интенсивность на интервале:

$$\lambda(T) = \int_0^T \lambda_0(t)\, dt. \quad (1.8)$$

Тогда закон распределения вероятностей имеет вид:

$$p_k(T) = \frac{(\lambda(T))^k}{k!} e^{-\lambda(T)}. \quad (1.9)$$

Рассмотрим закон распределения вероятности реализации атаки.

При $p'_I = 1$ распределение вероятностей атак есть распределение вероятностей возникновения атак с интенсивностью λ_{i0}. При $k \le m$, где m – число возникших атак, вероятность появления будет иметь вид:

$$p_m = \frac{\lambda_{i0}^m}{m!} e^{-\lambda_{i0}}. \quad (1.10)$$

Таким образом, для получения модели защиты информационно-телекоммуникационных объектов от угроз удаленного и непосредственного доступа, рассмотрев две модели, можно поставить задачу моделирования системы защиты от угроз в более вероятных и реальных условиях. Предыдущие разработки дают возможность совместить, провести интеграцию двух представленных моделей, что позволит исследовать уже новую модель защиты с новыми параметрами.

Это делается для усовершенствования процесса управления, позволит увидеть процессы реализации атак и предупредить их, что делает интегрированную модель более защищенной по сравнению с предыдущими разработками.

Литература

1. Остапенко Г.А. Топологические модели информационных операций в социотехнических системах: аспект региональной безопасности : дис. … канд. техн. наук. – М., 2005.

2. Радько Н.М. Методология риск-анализа несанкционированного доступа и управления эффективностью информационно-телекоммуникационных систем критических приложений в условиях конфликта : дис. … канд. техн. наук. – М., 2012.

3. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. – М. : РадиоСофт, 2010. – 232 с.