В.А. Минаев, А.Г. Остапенко

МОДЕЛЬ ВЗАИМОДЕЙСТВИЙ В РЕГИОНАЛЬНОЙ СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассмотрим основные параметры математической модели региональной системы информационной безопасности (РСИБ). Введем следующие обозначения:

- R - общий региональный ресурс;
- R_T - ресурсные потери из-за реализованных информационных угроз;
- R_S - часть регионального ресурса, затрачиваемая на создание и функционирование РСИБ;
- T - множество информационных угроз региональному ресурсу;
- O - множество объектов уязвимостей регионального ресурса;
- F_R, F_O, F_T - факторы внешней среды, определяющие, соответственно, состояние и динамику регионального ресурса, его уязвимостей и информационных угроз.

В общем виде система уравнений, описывающих взаимодействия [1], представляется как:

$$\begin{gathered} R = R\,(R_T,\ R_S,\ F_R), \\ R_S = R_S\,(R_T), \\ R_T = R_T\,(T), \\ T = T\,(O,\ R,\ F_T), \\ O = O\,(R_S,\ F_O). \end{gathered} \qquad (1)$$

Уравнений, описывающих сферу информационной безопасности, подобных (1), до настоящего времени предлагалось немало, но они, как правило, носили теоретический характер, не имея прямого практического применения к региональному аспекту. Однако очевидно, что их смысл должен заключаться в возможности практического анализа и прогнозирования информационной безопасности регионального ресурса, а самое главное – эффективного управления процессом её обеспечения.

Последнее обуславливает необходимость перехода к динамической форме представления взаимодействий в виде следующих разностных уравнений [1]:

$$\begin{gathered} R(t+1) = R(t) - R_T(t) - R_S(t) + a_1(t)\,F_R(t), \\ R_S(t) = a_2(t)\,R_T(t), \\ R_T(t) = a_3(t)\,T(t), \\ T(t+1) = a_4(t)\,O(t) + a_5(t)\,R(t) + a_6(t)\,F_T(t), \\ O(t+1) = O(t) - a_7(t)\,R_S(t) + a_8(t)\,F_O(t). \end{gathered} \qquad (2)$$

Система уравнений (2) включает описание механизмов [1]:

- эволюции регионального ресурса, включающего как информационную политику региона, так и внешние факторы – компонента $a_1(t)\,F_R(t)$;
- политики региона в сфере обеспечения его информационной безопасности – компонента $a_2(t)\,R_T(t)$, зависящей от потерь вследствие реализации информационных угроз – компонента $a_3(t)\,T(t)$;
- проявления информационных угроз, обусловленных тремя факторами:
  - из-за существования уязвимостей в системе информационной защиты - $a_4(t)\,O(t)$;
  - по причине "притягательности" регионального ресурса для компьютерной и иной разведки - $a_5(t)\,R(t)$;

- вследствие влияния внешней среды, в частности из-за информационно-психологического воздействия - $a_6(t)\ F_T(t)$;
- нейтрализации существующих информационных уязвимостей за счёт целенаправленных организационно-технических и других мероприятий по совершенствованию системы защиты ресурсов - $a_7(t)\ R_S(t)$;
- образования новых информационных уязвимостей - $a_8(t)\ F_O(t)$.

Использование рассматриваемой модели открывает перспективу построения сбалансированной системы информационной безопасности с возможностью текущей оценки оптимального уровня риска на основе заданных критериев. Это, в свою очередь, дает возможность:

- избежать излишних мер безопасности, как правило, возникающие при субъективной оценке рисков;
- спланировать и реализовать эффективную защиту на всех стадиях жизненного цикла информационных систем;
- оценить эффективность реализации различных вариантов контрмер.

Очевидно, что после соответствующих подстановок в (2) модель представляет систему из трех динамических уравнений, позволяющих системно управлять информационной безопасностью региона. Эта система отражает взаимообусловленную эволюцию развития регионального ресурса, множеств информационных угроз и объектов уязвимостей с учётом факторов внешней среды:

$$\begin{aligned} R(t+1) &= R(t) - A_1(t)\ T(t) + A_2(t)\ F_R(t), \\ T(t+1) &= A_3(t)\ O(t) - A_4(t)\ R(t) + A_5(t)\ F_T(t), \\ O(t+1) &= O\ t) - A_7(t)\ T(t) + A_8(t)\ F_O(t), \end{aligned} \qquad (3)$$

с начальными условиями $R(0) = R_0,\ T(0) = T_0,\ O(0) = O_0,$
где $A_1(t) = a_3(t)\ [1+a_2(t)],\ A_2(t) = a_1(t),\ A_3(t) = a_4(t),\ A_4(t) = a_5(t),\ A_5(t) = a_6(t),\ A_7(t) = a_2(t)\ a_3(t)\ a_7(t),\ A_8(t) = a_8(t)$.

Привязка предлагаемой модели к конкретному региону требует достаточно глубоких исследований не только использующихся информационных технологий, структуры организации региональной системы информационной безопасности, но и состояния текущих процессов, а также прогноза их развития.

Система (3) представляет модель, отражающую взаимовлияние объективных внутренних и внешних факторов, в конечном итоге сказывающихся на состоянии информационной безопасности регионального ресурса (совокупность материальной, финансовой, кадровой, информационной и иных компонентов региона, формирующих его потенциал как субъекта РФ).

Приведя (3) к дифференциальной форме уравнений и полагая, для упрощения, что их коэффициенты постоянны и начальные условия – нулевые, имеем:

$$\begin{aligned} dR/dt &= b_1\ T(t) + F_1(t), \\ dT/dt &= b_2\ O(t) + b_3\ R(t) + F_2(t), \\ dO/dt &= b_4\ T(t) + F_3(t), \end{aligned} \qquad (4)$$

где $R(0) = T(0) = O(0) = 0,\ b_1 = -a_3\ [1+a_2],\ b_3 = a_4,\ b_4 = -a_2\ a_3\ a_7$ и временные функции $F_1(t) = A_2(t)\ F_R(t),\ F_2(t) = A_5(t)\ F_T(t),\ F_3(t) = A_8(t)\ F_O(t)$. По определению, все a_i – положительны и, согласно допущениям, на некотором временном интервале постоянны.

Кроме того, исходя из выявленных зависимостей [1] динамики множества информационных угроз и уязвимостей от времени, примем:

$$F_2(t) = c_1\ exp(\beta_1\ t),$$

$$F_3(t) = c_2\, exp(\beta_2\, t), \qquad (5)$$

где c_1, c_2, β_1, β_2 - положительные коэффициенты.

Временную зависимость приращения регионального ресурса представим [1] в виде степенной функции:

$$F_1(t) = c_0\ t^n, \qquad (6)$$

где c_0 и n неотрицательны.

Далее авторами получены, выражения, которые могут использоваться для установления аналитических зависимостей изменения регионального ресурса от динамики множеств угроз и уязвимостей, равно как и для соответствующих численных оценок в процессе управления региональной системой информационной безопасности.

Рассмотренная математическая модель позволяет найти чувствительность основных параметров *R, O, T* к воздействию разнообразных дестабилизирующих факторов на РСИБ.

Литература

1. Минаев В.А. Информационная безопасность: российские парадоксы. – Системы безопасности, №2, 2003. - С.12-15.

2. Остапенко А.Г. Анализ и синтез линейных радиоэлектронных цепей с помощью графов. – М.: Радио и связь, 1985. – 280 с.

3. Гехер К. Теория чувствительности и допусков электронных цепей. – М.: Советское радио,1973. - С. 39-50.