УДК 004.056

К.А. Чехонин, Л.А. Шивдяков, Ю.Г. Крат, О.В. Рыбкина

Моделирование информационной безопасности критически важных объектов

Рассмотрена актуальность обеспечения информационной безопасности критически важных объектов в Дальневосточном Федеральном округе, связанная прежде всего с тем, что они оказывают существенное влияние на безопасность восточных рубежей страны и экономику региона. В составе таких объектов функционирует информационно-телекомунникационная система. Деструктивные воздействия на нее могут привести к значительным негативным последствиям.

В процессе работы с информационными ресурсами в ключевых системах информационной инфраструктуры рассматриваемых объектов, а также при их передаче и хранении возникают проблемы надежной защиты информации от угроз несанкционированного распространения, несанкционированных и непреднамеренных воздействий, которые могут привести к уничтожению, искажению или блокированию доступа к информации для законных пользователей. Наибольшую опасность такие угрозы представляют для технических средств обработки и передачи информации, содержащих средства обработки изображений (видеозаписи, передачи и приема телевизионных сигналов) и знаковой информации (телеграфной и факсимильной связи), вычислительной техники, изготовления и размножения документов, обработки речевой информации.

В работе рассматривается моделирование информационной безопасности критически важной системы информационной инфраструктуры объекта – информационно-управляющей или информационно-телекоммуникационная системы, которая осуществляет управление критически важным объектом или информационное обеспечение управления таким объектом и в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями. Моделирование производим путем создания интеллектуальной системы поддержки принятия решения посредством теории информации, математической статистики и адаптивных нейронечетких сетей. На этапе проектирования данные приводим к форме, пригодной для применения нейротехнологий с четким выделением набора параметров, позволяющих решать стоящую задачу ИБ с последующим их табличным представлением, где каждая запись является отдельным объектом, а каждое поле – признаком всех исследуемых объектов. В дальнейшем, применяя методы нейронечетких технологий, определяем структуру интеллектуальной системы, производим ее обучение и верификацию.

Рассматриваются алгоритмы нормировки данных и выделения информативных признаков. Для этого осуществляется преобразование множества

$$X = [x_1, x_2, \ldots, x_p] \tag{1}$$

во множество:

$$Z = [z_1, z_2, \ldots, z_p] \tag{2}$$

с диапазоном изменения (–1, 1) и равномерным законом распределения по следующим шагам:

Шаг 1. Задается $K = 1$ и определяется среднее значение и стандартное отклонение для множества (1):

$$\bar{x} = \frac{1}{p}\sum_{i=1}^{p} x_i\ , \tag{3}$$

$$\sigma = \frac{1}{p}\sum_{i=1}^{p} (x_i - \bar{x})^2\ , \tag{4}$$

где p – количество данных; x_i – входная переменная, при $i = \overline{1\ldots p}$; $\bar{x}$ – среднее значение; σ – стандартное отклонение входной переменной.

Шаг 2. Определяется множество (2) по функции

$$z_i = \frac{2}{1 + \exp[-K(x_i - \bar{x})]} - 1, \tag{5}$$

где K – настраиваемый коэффициент; z – преобразованная переменная.

Шаг 3. Определяется энтропия полученного множества по функционалу

$$H(Z) = -\sum_{j=1}^{h} P_j(z) \log P_j(z)\ , \tag{6}$$

где h – количество вариантов в вариационном ряде; $P_j(z) = a_j / a$ – частота встречаемости множества Z в варианте a_j (a_j – количество данных в варианте; a – общее количество данных).

Шаг 4. Наращивается значение коэффициента $K := K + 0{,}01$ и пересчитываются шаги 2 и 3 до тех пор, пока функционал (6) растет.

Принадлежность преобразованного множества диапазону (–1, 1) гарантируется функцией (5), а равномерность закона распределения обеспечивается поиском коэффициента K по функционалу (6).

Работа алгоритма построения каскадной нейронечеткой сети реализуется в виде следующих шагов:

Шаг 1. Определяется показатель эффективного размера адаптивной нейронечеткой сети для определенного размера данных:

$$p \approx [2^d (4d+1)]^2 / d, \tag{7}$$

где p – количество обучающих примеров; d – размер вектора, подаваемого на вход адаптивной нейронечеткой сети.

Шаг 2. Определяется структура каскадной нейронечеткой сети, состоящая из узлов и слоев, по системе (8) до момента, пока $t_k \le 0$ и $m_k = 1$:

$$\begin{cases} m_1 = (m_0 - t_1) / d, \\ m_2 = (m_1 + t_1 - t_2) / d, \\ m_3 = (m_2 + t_2 - t_3) / d, \\ \vdots \\ m_k = (m_{k-1} + t_{k-1} - t_k) / d. \end{cases} \tag{8}$$

$$M = [m_1, m_2, \ldots, m_k],$$

где k – количество слоев в сети; m_k – округленное до меньшего целое число от деления m_{k-1} / d, определяющее количество узлов в k-слое; $t = m_{k-1} - d \cdot m_k$ – остаток от деления, определяющий количество незадействованных признаков в k-слое, переходящих на следующий слой; $m_0 = n$.

Таким образом, создается сходящая каскадная структура, состоящая из входного (нулевого) слоя с внешними n-признаками и последующих k-слоев, каждый слой имеет m-узлов. Выходы узлов слоя образуют внутренние признаки для следующего слоя. В качестве узла выступает адаптивная нейро-нечеткая сеть с заданным количеством входов d.

Шаг 3. Для j узла l – слоя формируется обучающая группа:

$$y_i = [x_1, x_2, \ldots, x_d]_{l,j,i}, l = \overline{1 \ldots k}, j = \overline{1 \ldots m_1}, i = \overline{1 \ldots p}. \tag{9}$$

При формировании групп соблюдаются правила:

1) признаки (внешние или внутренние) объединяются в группы по правилу минимума кросс-энтропии, которая считается по формуле

$$I(x) = \log(N_{x_1} \cdot N_{x_2} \cdot \ldots \cdot N_{x_d} / N_{x_1, x_2, \ldots, x_d}), \tag{10}$$

где $N_{x_1} \cdot N_{x_2} \cdot \ldots \cdot N_{x_d}$ – количество промежутков, где присутствуют $x_1, x_2, \ldots$ или x_d соответственно; $N_{x_1, x_2, \ldots, x_d}$ – количество клеток, в которых содержатся точки с координатами $x_1, x_2, \ldots, x_d$;

2) каждый признак (внешний или внутренний) используется только в одной группе и только один раз;

3) признаки (внешние или внутренние), не вошедшие в группу в верхнем слое, участвуют в соревновании на образование группы на нижних слоях.

Шаг 4. j узел l – слоя обучается на обучающей группе при помощи алгоритма обратного распространения ошибки.

Шаг 5. Аналогично шагам 3 и 4 формируются последующие слои, учитывая, что выходы узлов предыдущего слоя являются внутренними признаками и участвуют в формировании обучающих групп для последующих слоев.

Шаг 6. Из полученных узлов и слоев строим модель каскадной нейронечеткой сети. Работа полученной сети оценивается по выходу последнего слоя.

Для решения задач информационной безопасности критически важных объектов в структуре ПО имеется три модуля: модуль принятия решения, осуществляющий расчет в рамках поставленной задачи, модуль выработки решения, модуль статистических исследований, осуществляющий подтверждение или опровержение гипотез, выдвигаемых экспертом при помощи статистических критериев.

Чехонин Константин Александрович
Д-р физ.-мат. наук, профессор, зав. каф. информационных технологий и систем Дальневосточного государственного университета путей сообщения
Эл. почта: director@festu.khv.ru.

Шевдяков Леонид Алексеевич
Руководитель Управления федеральной службы по техническому и экспортному контролю по Дальневосточному федеральному округу

Крат Юлия Георгиевна
Аспирант каф. информационных технологий и систем

Рыбкина Олеся Викторовна
Аспирант каф. информационных технологий и систем

K.A. Chehonin, L.A. Shivdyakov, U.G. Krat, O.V. Ryibkina

Information safety modeling crucial objects

The maintenance urgency of information safety modeling crucial objects in Far East Federal district is connected first of all by that they render essential influence on safety of east boundaries of the country and economy of region. In structure of such objects functions it is information-telecommunication system. Destructive influences on it can lead to significant negative consequences.