УДК 004.056

МОДЕЛЬ ОБНАРУЖЕНИЯ НАРУШИТЕЛЯ В УПРАВЛЕНЧЕСКОЙ СТРУКТУРЕ

П. В. Черняков, А. И. Зотов

Донской государственный технический университет, Ростов-на-Дону, Российская Федерация

letronas@mail.ru
zotovai@mail.ru

Цель данной работы заключается в создании алгоритма нахождения нарушителя в управленческой структуре. В работе описана модель обнаружения нарушителя, исследована возможность улучшения этой модели.

Ключевые слова: Информационная безопасность, модель обнаружения нарушителя, управленческая структура, нарушитель.

UDC 004.056

INTRUDER DETECTION MODEL IN THE MANAGEMENT STRUCTURE

P. V. Chernyakov, A. I. Zotov

Don State Technical University, Rostov-on-Don, Russian Federation

letronas@mail.ru
zotovai@mail.ru

The aim of this work is to create an algorithm for finding an intruder in the management structure. The paper describes the model of intruder detection in the management structure. The authors have conducted the research on the possibilities of improvement of this model.

Keywords: Information security, model of intruder detection, management structure, intruder.

Введение. В настоящее время во все сферы деятельности человека активно внедряются информационно-коммуникационные технологии, направленные на улучшение жизни общества. При этом число угроз информационной безопасности с каждым днём растет, требуя повышения защищенности предприятий, организаций, учреждений, фирм. Так как управленческие структуры активно используются в оборонной промышленности, других важных областях и отраслях нашей жизни, то, безусловно, особо важным можно считать вопрос об обнаружении нарушителя в такой управленческой структуре [1]. Из-за действий нарушителя может произойти срыв выполнения операции, производственной задачи и других мероприятий, основой функционирования которых является управленческая структура.

Основная часть. Управленческая структура предназначена для выполнения функций промежуточного звена между объектами, принимающими управленческие решения (командные звенья), и исполнительными звеньями (ИЗ), предназначенными для выполнения этих команд [2].

Командное звено формирует команды, приказы, распоряжения, указания, предписания и другие информационные посылки, которые чаще всего требуют определенных действий по приведению их к форме, понятной исполнительным звеньям и удобной для восприятия на входах.

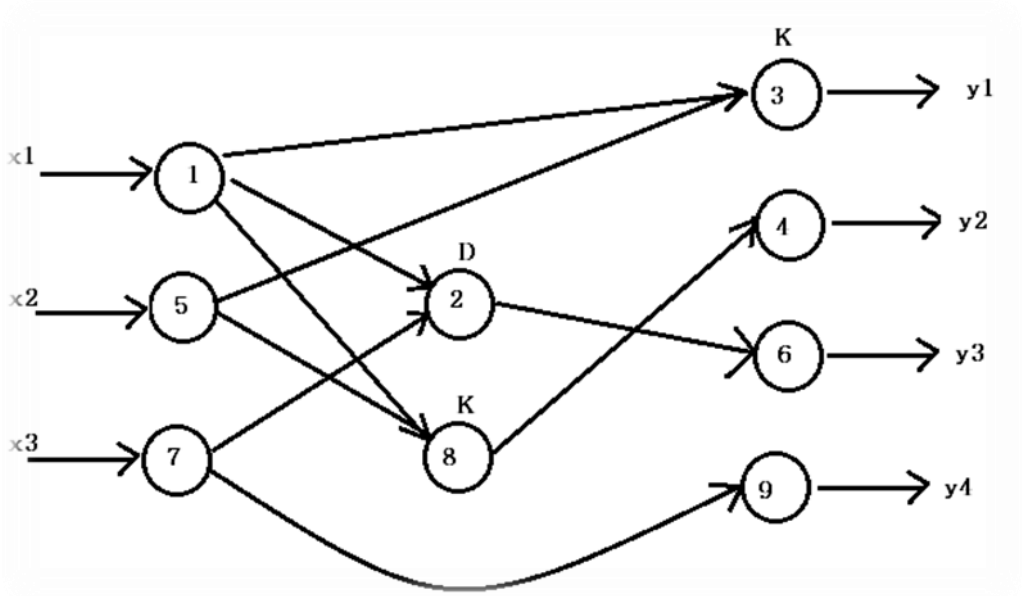

Рис. 1. Пример простейшей управленческой структуры

Ячейки, по которым передаётся информация — это операторы и узлы. При этом узел — оператор, принимающий более одной информационной посылки. Узнать, что оператор (или узел) ненадежен, можно по инверсии сигнала — при подаче определенной комбинации значений на выходе фиксируется неверный результат. При передаче сигнала от отправителя к получателю существует несколько этапов: шифрование, дополнение, алгоритмизация и пр. По функциональным признакам узлы могут быть охарактеризованы выполнением либо функции дизъюнкции (*D*-узлы), либо — конъюнкции (*K*-узлы).

Пример такой системы можно привести, моделируя обычную ситуацию в университете. Опишем задачу организации поездки студентов ДГТУ в г. Таганрог. На операторы *X*1, *X*2, *X*3 подаются распоряжения:

*X*1 – Точка сбора;

*X*2 – Обеспечение питания студентов;

*X*3 – Разделение на группы.

Все команды проходят через ячейки, которые могут быть конъюнктивными (*K*) и дизъюнктивными (*D*). При попадании в одну конъюнктивную ячейку двух сигналов, на выходе получаем единицу только в том случае, если оба сигнала будут равны единицы. Выход из дизъюнктивной ячейки будет равен единице в случае, если хотя бы один сигнал равен единице. Единица соответствует правильному прохождению оператора, если на входе такого оператора поступает единица или комбинация, соответствующая единице (для узлов). Таким образом на выходе операторы получают указания и могут приступать к их выполнению.

Авторы рассмотрели наиболее простой пример работы подобной системы. В реальности система может быть гораздо сложнее, но обязательным условием всегда является то, что указания, приказы, поступающие на *X*1, *X*2, *X*3 не связаны между собой.

Основная цель настоящей работы — это нахождение нарушителя в управленческой структуре. На первом этапе для реализации данной цели моделируется работа без нарушителя. В результате получаем таблицу работы схемы, которая называется таблицей взаимосвязи входов и вы-

ходов. Далее составляются таблицы, которые однозначно определят место нарушителя в структуре. Данная задача называется задачей тестовой локализации.

Таблица 1

Комбинация входных параметров (без нарушителя)

*X*1	*X*2	*X*3
0	0	0
0	0	1
…	…	…
1	1	1

Таблица 2

Комбинация выходных параметров (без нарушителя)

*Y*1	*Y*2	*Y*3	*Y*4
0	0	0	0
0	0	1	1
…	…	…	…
1	1	1	1

На следующем этапе составляются аналогичные таблицы в предположении, что нарушитель находится в каком-то определенном узле. В итоге получаем комбинации на входе и выходе, которые однозначно определят местонахождение нарушителя в системе, если таковой имеется.

Таблица 3

Комбинация входных параметров (нарушитель в узле y1)

*X*1	*X*2	*X*3
0	0	0
0	0	1
…	…	…
1	1	1

Таблица 4

Комбинация выходных параметров (нарушитель в узле y1)

*Y*1	*Y*2	*Y*3	*Y*4
0	0	0	0
0	0	1	1
…	…	…	…
0	0	1	1

Таким образом, составив таблицы до девятого узла, можно получить набор комбинаций, которые помогут локализовать нарушителя в системе.

Заключение. Рассмотрен достаточно простой пример локализации нарушителя в управленческой структуре — это случай с детерминированным исходом. Описан алгоритм, позволяющий обнаружить нарушителя с помощью тестовой локализации. Отмечено, что в реальности действия операторов носят вероятностный характер и математическая модель должна носить вероятностный (стохастический) характер. Авторами принято решение продолжить разработки в указанном направлении.

Библиографический список.

1. Давидов, П. С. Техническая диагностика радиоэлектронных устройств и систем / П. С. Давидов. — Москва : Радио и связь, 1988. — 256 с.
2. Шибанов, Г. П. Контроль функционирования больших систем / М. В. Шибанов. — Москва : Радио и связь, 1977. — 360 с.