Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

Доклад на тему:

ПОСТРОЕНИЕ ЛОГИЧЕСКИХ МОДЕЛЕЙ ОПАСНЫХ СОСТОЯНИЙ КОМПЛЕКСОВ СРЕДСТВ АВТОМАТИЗАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Докладчик: преподаватель 33 кафедры Сидельников О.В

АКТУАЛЬНОСТЬ ИССЛЕДОВАНИЯ

Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»	обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры (КИИ) РФ, в мирное время, в период непосредственной угрозы агрессии и в военное время»
Федеральный закон РФ № 187-ФЗ от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации»	недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта КИИ
Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы	обеспечить комплексную защиту информационной инфраструктуры РФ, в том числе с использованием системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА) на информационные ресурсы и системы критической информационной инфраструктуры; проводить непрерывный мониторинг и анализ угроз, возникающих в связи с внедрением новых информационных технологий, для своевременного реагирования на них
ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения	Критически важная система информационной инфраструктуры – информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление или информационное обеспечение критическим объектом или процессом, или используется для официального информирования общества и граждан, нарушение или прерывание функционирования которой (в результате деструктивных информационных воздействий, а также сбоев или отказов) может привести к чрезвычайной ситуации со значительными негативными последствиями

ОПАСНЫЕ СОСТОЯНИЯ КСА АС

Под безопасностью КСА АС понимается способность системы функционировать, не переходя в опасное состояние.

Опасное состояние (по ГОСТ 27.002-2015) – состояние объекта, в котором возникает недопустимый риск причинения вреда людям, или окружающей среде, или существенных материальных потерь, или других неприемлемых последствий.

Несвоевременность обнаружения опасных состояний КСА АС, выхода контролируемых параметров за пределы допустимых значений, выхода из строя одного или нескольких элементов системы может повлечь отказ всей системы.

Рис.1

Отказ – событие, заключающееся в нарушении работоспособного состояния объекта (система утрачивает способность выполнять заданное назначение т. е. теряет свою работоспособность).

Компьютерный инцидент (КИ) – это факт нарушения или прекращения функционирования объектов КСА АС, в том числе вызванных компьютерной атакой (КА).

Целью обеспечения мониторинга объектов КСА АС является поддержание установленного уровня надежности, обеспечение требований безопасности и эффективности использования объекта.

Проблемы анализа состояния надежности и безопасности, своевременность выявления перехода в опасное состояние АС рассмотрены в трудах Дружинина Г.В., Ушакова И.А., Можаева С.А., Рябинина И.А., Острейковского В.А., Швыряева Ю.В. и др.

Построение логических моделей опасного состояния КСА

В логико-вероятностной теории безопасности **сценарий опасных состояний (СОС)** осуществляется с помощью логической функции опасности системы (ФОС), аргументами которой выступают **инициирующие события (ИС)** и условия, в качестве которых могут быть короткие замыкания в электросети, разряды молнии, искрение электрооборудования, сварочные работы, диверсионные акты, отказы, нарушения правил эксплуатации, ошибки операторов, деструктивные воздействия, в том числе, заключительная фаза компьютерной атаки, различные повреждающие воздействия и иные причины, приводящие к чрезвычайной ситуации.

Кратчайший путь опасного функционирования (КПОФ) – это конъюнкция инициирующего события (y_i), ни одну из компонент которой нельзя изъять, не нарушив опасного функционирования системы. **Функция алгебры логики (ФАЛ)** этой конъюнкции имеет вид:

$$\Phi_i = \bigwedge_{i \in K_{\Phi_i}} y_i \qquad (1)$$

где K_{Φ_i} – множество номеров ИС, соответствующих данному *i*- му КПОФ.

КПОФ описывает один из возможных вариантов попадания системы в опасное состояние с помощью минимального набора ИС, абсолютно необходимых для его осуществления, т.е. данного варианта опасного состояния системы.

Аналитические и графические формы представления опасного состояния системы, СОС, структурные модели систем в виде схем подробно рассмотрены в работах:

1. Рябинин И.А. Надежность и безопасность структурно-сложных систем.– СПб.: Политехника, 2000.– 248 с.: ил. – С.98.
2. Острейковский В.А., Швыряев Ю.В. Безопасность атомных станций. Вероятностный анализ – М: ФИЗМАТЛИТ, 2008.– 352 с.

Способ построения логических моделей опасного состояния КСА

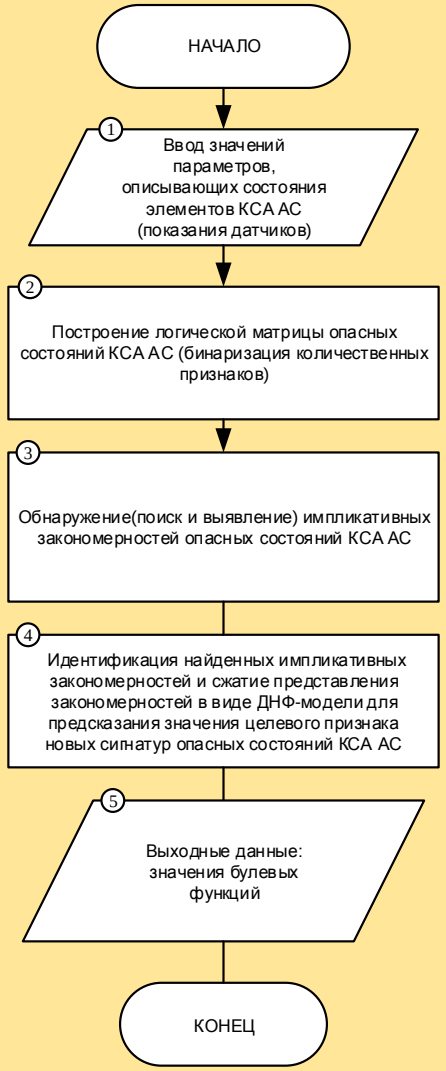

Рис. 2

Шаг 1. Формирование пространства признаков

Для мониторинга опасных состояний КСА АС строится матрица информативности признаков опасных состояний. Логические переменные описывают параметрами инициирующего состояния (значение «1» соответствует появлению инициирующего события; значение «0» соответствует отсутствию инициирующего события).

Таблица 1 – Формирование пространства признаков

	x_1	x_2	x_3	x_4	x_5	x_6
Объект X_1	0	0	1	1	1	1
Объект X_2	1	1	0	0	0	0
…….	.	.	.	.	.	.
Объект X_{64}	1	0	0	0	1	1

Шаг 2. Построение модели исследуемого класса в алгебраической форме *(в виде ДНФ запрета, если признаков минимально или в виде БФ запрета).*

Представим каждую элементарную конъюнкцию рассматриваемой ДНФ троичным вектором, компоненты которой получают значения «–», «0», «1».
Символ «–» является символом неопределенности.

$$x_1\ x_2\ x_3\ x_4\ x_5\ x_6$$

$$T = \begin{bmatrix} 1 & - & 1 & - & - & 0 \\ - & 1 & - & - & 0 & 1 \\ 0 & - & - & 0 & 1 & - \\ - & 0 & - & 1 & - & 1 \\ - & 0 & 0 & 0 & - & - \end{bmatrix} \quad (2)$$

Шаг 3. Выбор целевого признака из системы закономерностей и упрощение

Пусть в данном примере роль целевого признака играет признак опасного состояния – x_6. При $x_2 = 0$ становится излишней строка 2, так как задаваемая ею область запрета не содержит элементов с таким значением признака x_2 ($x_2 = 1$ во второй строке), и следовательно, не пересекается с интервалом возможного существования объекта, не обладающего признаком x_2. Удалив ее вместе со столбцом x_2, получим остаток (формула 3).

$$T = \begin{bmatrix} 1 & 1 & - & - & 0 \\ 0 & - & 0 & 1 & 1 \\ - & - & 1 & - & 1 \\ - & 0 & 0 & - & 1 \end{bmatrix} \quad (3)$$

Если $x_2 = 1$ следует анализировать остаток матрицы *T* (выпадают строки 4 и 5, где x_2 соответствует $\overline{0;1}$ -формула (4).

$$T = \begin{bmatrix} 1 & 1 & - & - & 0 \\ - & - & - & 0 & 1 \\ 0 & - & 0 & 1 & 1 \end{bmatrix} \quad (4)$$

Таким образом, из остатка матрицы *T* можно записать в алгебраической форме представление признака x_6 через другие признаки (формула 5).

$$x_6 = \overline{x_5} \vee \overline{x_1} \wedge \overline{x_4} \wedge x_5 \quad (5)$$

Вывод: Обнаружение (поиск и выявление) импликативных закономерностей опасных состояний КСА АС основано на выборе целевого признака из системы закономерностей и снижении размерности векторов образов сигнатур опасных состояний.

Список литературы

1. Рябинин И.А. Надежность и безопасность структурно-сложных систем.– СПб.: Политехника, 2000.– 248 с.: ил. – С.98.
2. Острейковский В.А., Швыряев Ю.В. Безопасность атомных станций. Вероятностный анализ – М: ФИЗМАТЛИТ, 2008.– 352 с.
3. Сидельников, О.В. Применение метода индуктивного прогнозирования состояний для обнаружения компьютерных атак в информационно-телекоммуникационных системах / О.В. Сидельников, В.Н. Лаптев, В.А. Шарай // Научный журнал КубГАУ [Электронный ресурс]. – Краснодар: КубГАУ, 2011. – № 72(08). – 10 с. – Режим доступа : http://ej.kubagro.ru/2011/08/pdf/37.pdf.
4. Закревский, А.Д. Логика распознавания / Изд.2-е, доп. – М.: Едиториал УРСС, 2003. – 144 с.

Спасибо за внимание