XXV научно-практическая конференция «Комплексная защита информации»
Дорохово, Московская область, 15 – 17 сентября 2020 г.

Гефнер И.С., Текунов В.В., Язов Ю.К.

ФУНКЦИОНАЛЬНЫЕ МОДЕЛИ ПРОЦЕССОВ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ БАЗОВОЙ СИСТЕМЫ ВВОДА-ВЫВОДА

Докладчик:
доктор техн. наук, проф. Язов Юрий Константинович,
ФАУ «ГНИИИ ПТЗИ ФСТЭК России», г. Воронеж

Место процедуры оценки возможностей реализации угроз в общем алгоритме их анализа

Составляющие алгоритма анализа угроз

- Выявление источников угроз
- Выявление уязвимостей
- Выявление способов реализации угроз
- Выявление возможных объектов воздействия
- Выявление содержания несанкционированных действий
- Оценка последствий реализации угроз

Оценка возможностей реализации угроз

- Релевантные характеристики ИС
- Системотехнический уровень, на котором реализуется угроза
  - Сетевой
  - Системный
  - Прикладной
  - Микропрограммный
- Фактор времени
- Осведомленность нарушителя

Истоки функционального моделирования

Программа автоматизации промышленных предприятий ICAM (*Integrated Computer Aided Manufacturing*)

SADT (Structured Analysis and Design Technique) - Графический язык описания функциональных систем

Стандарт NIST IDEF0 (Icam DEFinition) – Методология функционального моделирования (1981 – 1993 гг.)

Публикации отдельных авторов и отчеты о НИР с материалами по функциональному моделированию угроз на сетевом, системном и прикладном уровнях

Понятие функциональной модели

Под **функциональной моделью на сетевом, системном и прикладном уровнях** понимается ориентированный граф, вершинами которого являются именованные программные или программно-аппаратные элементы ИС, задействованные в ходе реализации рассматриваемой угрозы, а дугами – действия (в том числе команды, процедуры, функции), выполняемые в ходе реализации угрозы

Формальное представление функциональной модели

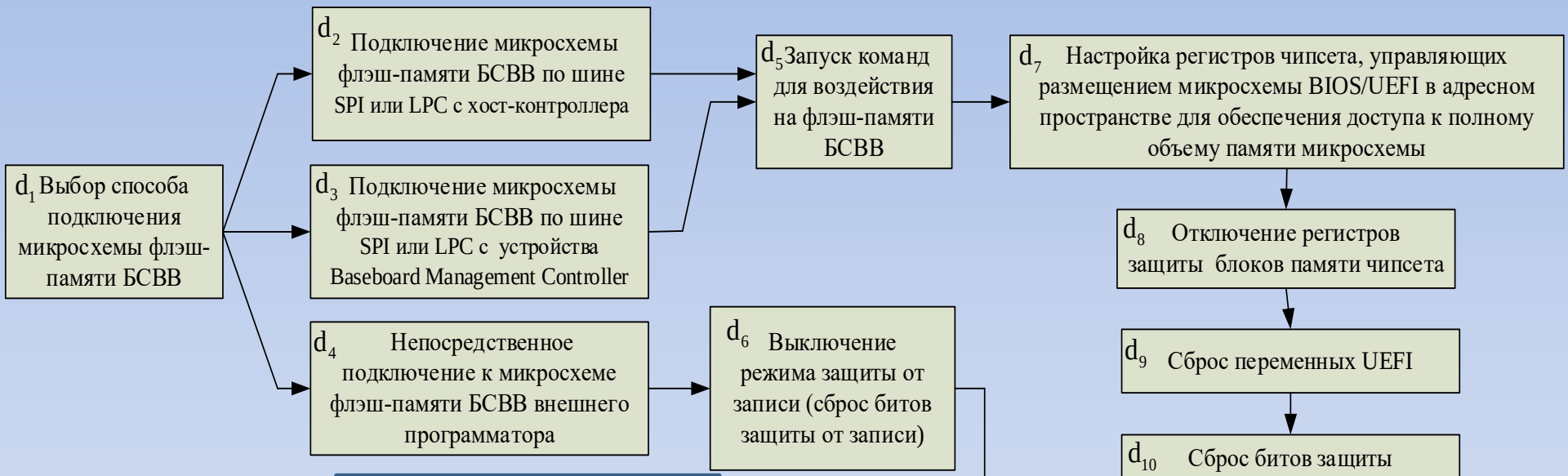
$$\Phi_u = \{D_u,\ L(D_u), M(D_u)\},\ u = \overline{1, U}$$

D_u - Множество функций (действий), $d_u^{(k)} \in D_u,\ k = \overline{1, K(D_u)}$ которые нужно выполнить при реализации u –й угрозы;

$L(D_u)$ - Совокупность условий успешного выполнения функций (действий);

$M(D_u)$ - Матрица взаимосвязей функций (действий), отражающая порядок их выполнения

Граф функциональной модели угрозы нарушения загрузки операционной системы путем модификации содержимого флэш-памяти БСВВ

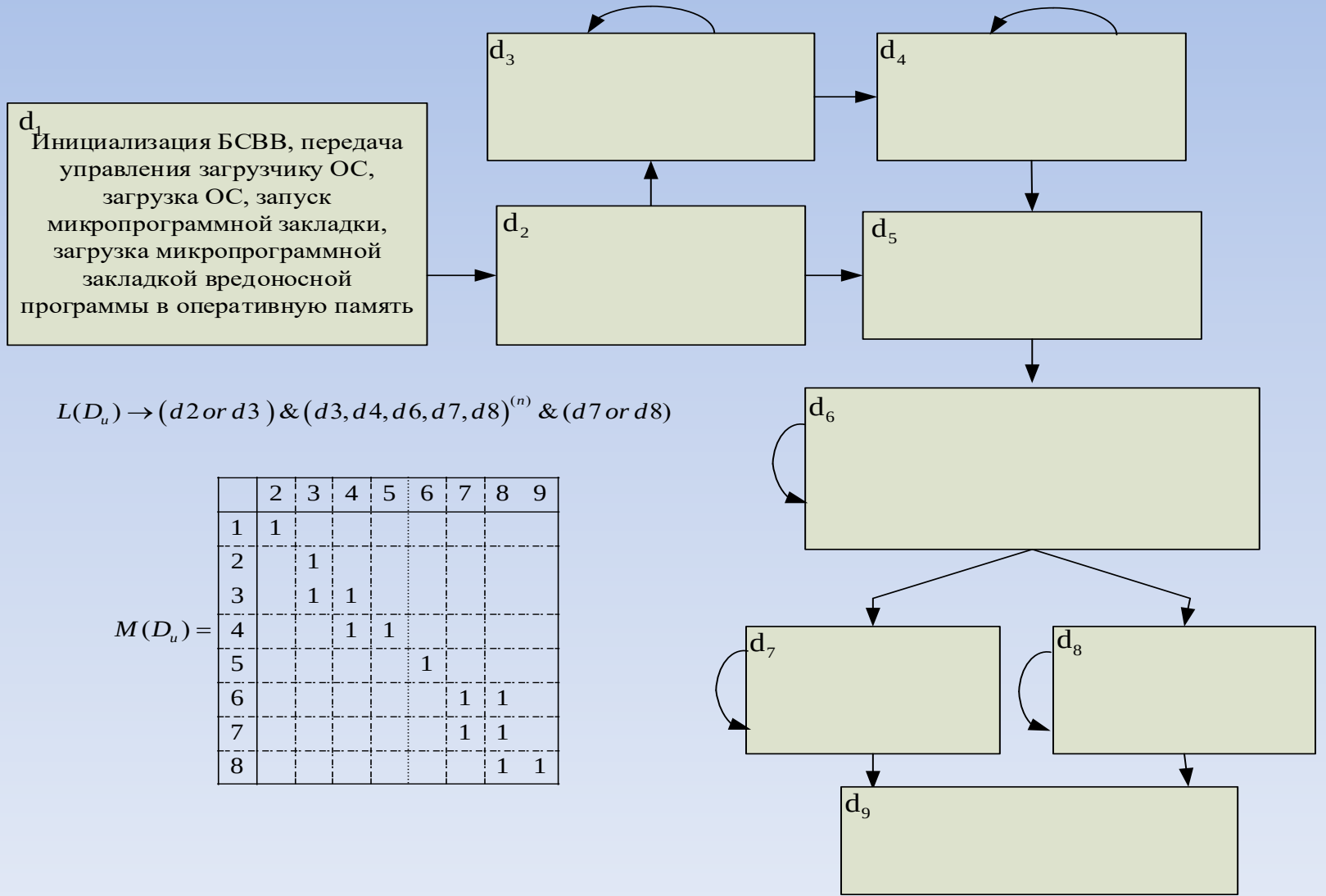


$M(D_u) =$

	2	3	4	5	6	7	8	9	10	11
1	1	1	1							
2				1						
3				1						
4					1					
5						1				
6										1
7							1			
8								1		
9									1	
10										1

$$L(D_u) \rightarrow d_2 \; or \; d_3 \; or \; d_4$$

Граф функциональной модели угрозы уничтожения или модификации системных файлов с использованием микропрограммной закладки в БСВВ



$$L(D_u) \rightarrow (d2 \, or \, d3) \& (d3, d4, d6, d7, d8)^{(n)} \& (d7 \, or \, d8)$$

$M(D_u) =$

	2	3	4	5	6	7	8	9
1	1							
2		1						
3		1	1					
4			1	1				
5					1			
6						1	1	
7						1	1	
8							1	1

Спасибо за внимание!

Язов Юрий Константинович