УДК 003.056.5

СТРУКТУРНОЕ МОДЕЛИРОВАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Т.М. Волосатова, **И.Н. Чичварин**

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
e-mail: tamaravol@gmail.com; chichvarin.ivan@ gmail.com

Рассмотрено состояние современных средств обеспечения безопасности информационных систем. Показано, что поскольку САПР – весьма специфичная информационная система, необходима разработка и специфичных моделей угроз ее безопасности. Учтено, что САПР — открытая, непрерывно меняющаяся система, в которой применяются CALS-технологии. Обращается внимание на необходимость разработки единой методологии создания модели угроз информационной безопасности САПР (ИБ САПР), позволяющей с единых позиций подходить к разработке подсистем ИБ САПР в различных проектных организациях. Показана необходимость и возможность снабжения моделей угроз ИБ САПР экспертной компонентой, позволяющей формализовать эвристики, неизбежно сопровождающие процесс формирования модели угроз любой информационной системы.

Ключевые слова: модели угроз, информационная безопасность САПР, угроза несанкционированного доступа, вектор ложных данных, вектор утечек, комбинационная схема, вероятностный автомат, нечеткий автомат, недетерминированный автомат, детерминированный автомат, композиция автоматов.

STRUCTURAL MODELING OF THREATS TO INFORMATION SECURITY OF COMPUTER-AIDED DESIGN SYSTEMS

T.M. Volosatova, **I.N. Chichvarin**

Bauman Moscow State Technical University, Moscow, Russian Federation
e-mail: tamaravol@gmail.com; chichvarin.ivan@ gmail.com

The state of the art of aids for ensuring security of information systems is discussed. It is shown that since the Computer-Aided Design (CAD) system is a very specific information system, it is necessary also to develop specific models of its security threats. The fact that CAD is an open continuously varying system in which CALS technologies are applied is taken into account. The need is stressed for developing a unified methodology for creation of a threat model of the CAD information security (CAD IS), which allows the development of CAD IS subsystems to be approached from the common positions at different design institutions. It is shown that the CAD IS threat models must and can be equipped with an expert component enabling heuristics (that inevitably accompany the process of threat model formation for any information system) to be formalized.

Keywords: threat models, information security of CAD system, threat of unauthorized access, false data vector, data leakage vector, probabilistic automation, fuzzy automation, non-deterministic automation, deterministic automation, composition of automata.

Как показывает анализ работ [1–4], САПР занимает особое место среди информационных систем. Кроме прочих отличий для таких систем характерна ярко выраженная структурированность, проявляющаяся в следующих аспектах:

блочно-иерархическом подходе к построению системы и к процессу проектирования;

наличии четко определенной конфигурации, выраженной во взаимосвязной совокупности подсистем (видов обеспечений).

Последняя особенность обусловливает и возможность создания подсистемы, обеспечивающей информационную безопасность (ИБ) САПР. Анализ публикаций в области ИБ [1, 4–6] позволяет считать, что необходимость создания такой подсистемы актуальна и не требует каких-либо дополнительных обоснований. В работе [3] показано, что вопросы ИБ САПР имеют специфику, заставляющую рассматривать их отдельно от общих вопросов ИБ остальных автоматизированных информационных систем. При этом подчеркиваются следующие факторы:

- САПР — открытая и развивающаяся система, поэтому предъявляются специфичные требования к подсистеме ИБ САПР, а именно к ее развитию;
- выявлено, что существенной особенностью требований к ИБ САПР является применение CALS-технологий. Поскольку CALS предполагает сопровождение ОП в течение всего жизненного цикла, очевидна и специфичность обеспечения ИБ САПР, прежде всего защиты проектно-эксплуатационной документации от несанкционированного доступа (НСД) в период всего жизненного цикла.

Все перечисленное позволяет считать, что построение модели угроз ИБ САПР также сопряжено с рядом специфических особенностей.

Методы моделирования угроз безопасности информационных систем. К требованиям, предъявляемым к указанным методам, можно отнести:

- адекватность модельного представления (учет большинства существенных уязвимостей системы);
- возможность выработки средств подавления (ослабления) возможных атак при использовании моделирования реализаций угроз.

Специфика ИБ САПР предполагает следующие дополнения к перечисленным требованиям:

- учет факторов открытых (развивающихся) систем проектирования, дорабатываемых проектантами во время эксплуатации;
- возможность применения в САПР CALS-технологий.

Анализ наиболее распространенных методов аудита ИБ позволяет классифицировать их с помощью структуры, показанной на рис. 1.

Рис. 1. Классификация распространенных методов формирования моделей угроз безопасности информационных систем

Пример весьма распространенного метода описания угроз, условно названного в настоящей статье как таблично-текстовый, приведен на рис. 2 [7]. Остальные методы в дополнительных объяснениях не нуждаются.

Отметитм, что наглядность таблично-текстового описания — его единственное достоинство, если принять во внимание перечисленные требования.

Модель угроз ИБ САПР в виде таблично-текстового описания приведена на рис. 3 [4].

Рассмотрим пример типовой методологии построения модели угроз ИБ системы [8].

Этап 1. *Общая оценка угроз ИБ и последствий атак.* Перечень в некоторой степени можно отнести к области ИБ САПР. Далее в табл. 1 приведен перечень возможных последствий реализации угроз.

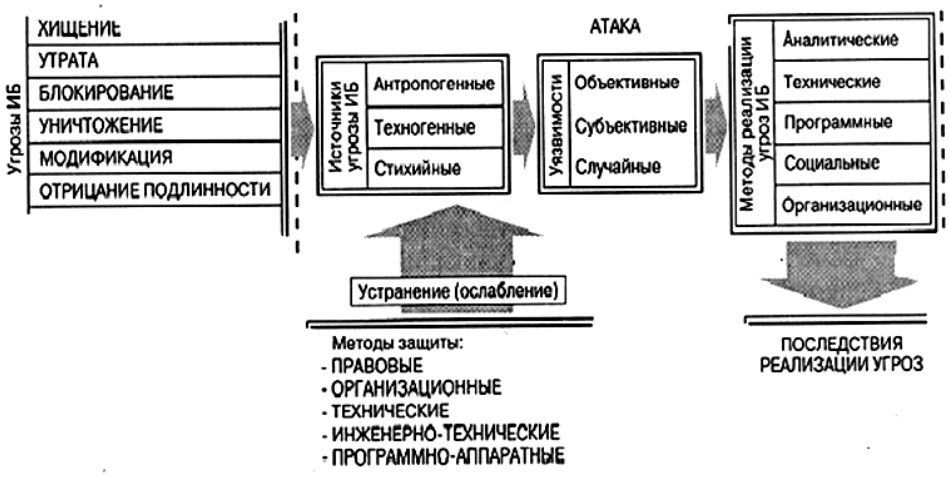

Рис. 2. Модель угроз ИБ в виде таблично-текстового описания

Рис. 3. Модель угроз ИБ САПР в виде таблично-текстового описания

Таблица 1

Перечень возможных последствий реализации угроз

Тип угрозы	Возможные последствия
Анализ сетевого трафика	Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей
Сканирование сети	Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей
Выявление пароля	Выполнение любого действия, связанного с получением несанкционированного доступа

Тип угрозы	Возможные последствия
Подмена доверенного объекта сети	Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
Навязывание ложного маршрута сети	Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений
Внедрение ложного объекта сети	Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
Отказ в обслуживании:	
частичное исчерпание ресурсов	Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений
полное исчерпание ресурсов	Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения. Отказ в предоставлении сервиса (электронной почты, файлового и т.п.)
нарушение логической связанности между атрибутами, данными, объектами	Невозможность передачи сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т.п.
использование ошибок в программах	Нарушение работоспособности сетевых устройств
Удаленный запуск приложений: путем рассылки файлов, содержащих деструктивный исполняемый код, вирусное заражение; путем переполнения буфера серверного приложения; с использованием возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами	Нарушение конфиденциальности, целостности, доступности информации Скрытое управление системой

Далее модель строится путем экспертного перечисления угрозы: утечки по техническим каналам и угрозы НСД.

Перечисленные угрозы включают в себя:

— угрозы, реализуемые в ходе загрузки операционной системы, которые направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

— угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных) с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);

— угрозы внедрения вредоносных программ;

— угрозы анализа сетевого трафика с перехватом передаваемой по сети информации;

— угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.;

— угрозы внедрения ложного объекта сети;

— угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;

— угрозы отказа в обслуживании;

— угрозы выявления паролей;

— угрозы удаленного запуска приложений;

— угрозы внедрения по сети вредоносных программ.

Этап 2. *Определение уровня исходной защищенности системы* (табл. 2). Во многих практических случаях под уровнем исходной защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик (Y1).

Исходная степень защищенности зачастую определяется экспертным путем, например:

1) $Y1 = 0$. Система имеет высокий уровень исходной защищенности, если не менее 70 % характеристик соответствуют уровню “высокий” (суммируются положительные решения но первому столбцу, соответствующему высокому уровню защищенности), а остальные — среднему уровню защищенности (положительные решения по второму столбцу);

2) $Y1 = 5$. Система имеет средний уровень исходной защищенности, если не выполняются условия по п. 1 и не менее 70 % характеристик ИСПД соответствуют уровню не ниже “средний” (берется

отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему числу решений), а остальные — низкому уровню защищенности;

3) $Y1 = 10$. Система имеет низкую степень исходной защищенности, если не выполняются условия по п. 1 и 2.

Таблица 2

Характеристики, определяющие исходный уровень защищенности системы

Технические и эксплуатационные характеристики	Уровень защищенности		
	высокий	средний	низкий
1. По встроенным (легальным) операциям с записями баз данных:			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача.	–	–	+
2. По наличию соединений с другими базами данных:			
интегрированная организация использует несколько баз, при этом организация не является владельцем всех используемых баз	–	–	+
система, в которой используется одна база, принадлежащая организации — владельцу данной системы	+	–	–

Этап 3. *Экспертное определение вероятности реализации угроз в системе*. Под вероятностью реализации угрозы поднимается определяемый экспертным путем показатель, характеризующий, насколько вероятной является реализация конкретной угрозы безопасности для данной системы в складывающихся условиях обстановки.

Зачастую вероятность (Y2) определяется по четырем вербальным градациям этого показателя:

маловероятно — отсутствуют объективные предпосылки для осуществления угрозы ($Y2 = 0$);

низкая вероятность — объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y2 = 2$);

средняя вероятность — объективные предпосылки для реализации угрозы существуют, а принятые меры обеспечения безопасности недостаточны ($Y2 = 5$);

высокая вероятность — объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности не приняты ($Y2 = 10$).

Пример экспертной оценки вероятности реализации угрозы безопасности различными категориями нарушителей (К) приведен в табл. 3.

Таблица 3

Экспертная оценка вероятности реализации угрозы безопасности различными категориями нарушителей (К)

Угроза безопасности		Вероятность реализации угрозы нарушителем категории К							Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы
		К1	К2	К3	К4	К5	К6	Итог Y2		
Утечки:	акустической (речевой) информации	0	0	0	0	0	0	0	0,25	Низкая
	видовой информации	0	0	0	2	5	2	5	0,5	Средняя
	по каналу ПЭМИН	0	0	0	0	0	0	0	0,25	Низкая
Угрозы, реализуемые:	в ходе загрузки операционной системы	0	0	0	0	0	0	0	0,25	Низкая
	после загрузки операционной системы	2	2	2	2	2	2	2	0,35	Средняя
	внедрением вредоносных программ	2	0	0	5	2	5	5	0,5	Средняя
	анализом сетевого трафика с перехватом передаваемой по сети информации	2	0	0	2	2	2	2	0,35	Средняя

Окончание таблицы 3

Угроза безопасности		Вероятность реализации угрозы нарушителем категории К							Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы
		К1	К2	К3	К4	К5	К6	Итог Y2		
Угрозы, реализуемые:	сканированием, направленным на выявление открытых портов и служб, открытых соединений и др.	2	0	0	2	2	2	2	0,35	Средняя
	внедрением ложного объекта сети	2	2	2	2	2	2	2	0,35	Средняя
	навязыванием ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	5	0	0	0	0	0	0	0,25	Низкая
	отказом в обслуживании	2	0	0	2	2	2	2	0,35	Средняя
	выявлением паролей	2	0	0	2	0	0	2	0,35	Средняя
	удаленным запуском приложений	2	0	0	2	2	2	2	0,35	Средняя
	внедрением по сети вредоносных программ	2	0	0	2	2	2	2	0,35	Средняя

Этап 4. *Определение возможности реализации угрозы в системе*. По итогам оценки уровня исходной защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) по эмпирической формуле: $Y = (Y1+Y2)/20$, и определяется возможность ее реализации (см. табл. 3).

Этап 5. *Оценка опасности угроз в системе*. Оценка опасности проводится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

- низкая опасность — если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- средняя опасность — если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность — если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Пример оценки опасности приведен в табл. 4.

Таблица 4

Оценки опасности

Угроза безопасности данным	Опасность угроз
Утечки:	
акустической (речевой) информации	Низкая
видовой информации	Средняя
по каналу передачи сообщений	Низкая
Угрозы, реализуемые:	
в ходе загрузки операционной системы	Низкая
после загрузки операционной системы	Низкая
внедрением вредоносных программ	Средняя
анализом сетевого трафика с перехватом передаваемой по сети информации	Средняя
сканированием, направленным на выявление открытых портов и служб, открытых соединений и др.	Низкая
внедрением ложного объекта сети	Низкая
навязыванием ложного маршрута путем несанкционированного изменения маршрутно-адресных данных	Средняя
отказом в обслуживании	Низкая
выявлением паролей	Низкая
удаленным запуском приложений	Низкая
внедрением по сети вредоносных программ	Низкая

Этап 6. *Составление перечня актуальных угроз безопасности данных в системе*. В соответствии с правилами отнесения угрозы безопасности к актуальной (табл. 5) для ИСПДн АС существуют следующие актуальные угрозы (табл. 6).

Таблица 5

Правила классификации угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	низкий	средний	высокий
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

Таблица 6

Актуальные и неактуальные угрозы

Наименование угрозы безопасности данных	Тип угрозы	Возможность реализации угрозы	Показатель опасности
Угроза 1	Нарушение целостности	Актуальная	
		средняя	средний
Угроза 2	Нарушение доступности	Неактуальная	
		средняя	низкий
Угроза 3	Потеря конфиденциальности актуальность	Актуальная	
		высокая	средний

Анализ приведенной типовой методики позволяет утверждать, что значительное место в ней занимает сбор и обработка данных, получаемых путем экспертных оценок. Таким образом, можно считать допустимой и полезной формализацию построения модели угроз ИБ САПР с помощью методов, составляющих основу экспертных систем, т.е. через “обучение” среды подсистем САПР. Однако для части подсистем САПР перечень угроз имеет детерминированное и постоянное описание. Это характерно для технических средств и специального программного обеспечения. Поэтому из приведенных методов формализации построения модели угроз наиболее рациональным можно считать метод построения автоматных моделей. При таком подходе

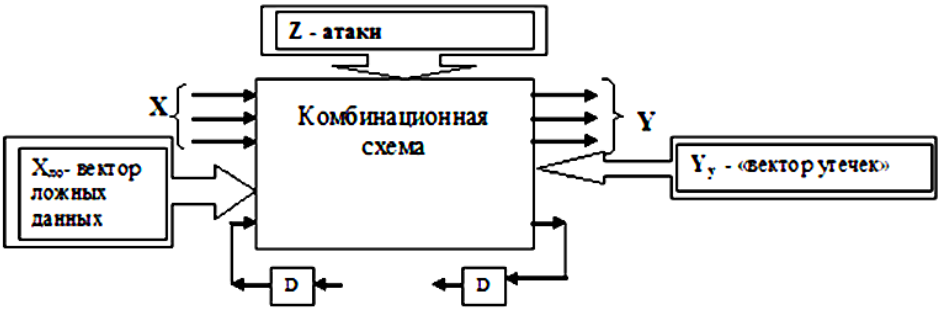

Рис. 4. Структура абстрактного автомата — элемента полугруппы автоматов, моделирующей объект защиты (*D* — элемент задержки (памяти автомата) на такт автоматного времени)

необходимо сочетать детерминированные, вероятностные и нечеткие конечные автоматы.

Автоматные модели процессов проектирования и угроз ИБ подсистем САПР. Как отмечалось в работе [3], перечень специфических угроз, характерных для каждого иерархического уровня САПР, дополняется перечнем, характерным для любой информационной системы. Известная обобщенная схема алгоритма построения модели угроз ИБ в САПР в автоматной форме приведена на рис. 4.

Логическая функция, моделирующая комбинационную схему, имеет вид

$$X,\ Y \xrightarrow{COMB(Z)} Y'.$$

На каждом иерархическом уровне содержательные части **X, Y**, а также логическая функция $X,\ Y \xrightarrow{COMB(Z)} Y'$ могут иметь свое фактическое описание.

Различные варианты вычислительных моделей, основанных на использовании конечных автоматов, и их взаимосвязь приведены в табл. 7.

Таблица 7

Варианты вычислительных моделей, основанных на использовании конечных автоматов

Вариант модели	Конечный автомат
Детерминированная	Порождающий
Недетерминированная	Недетерминированный порождающий
Вероятностная	Марковская модель
Нечеткая	Нечеткий порождающий

Вероятностный автомат (ВА) определяется следующей совокупностью [9]:

$$\text{ВА} = \langle X, Y, Z, \{P(z(t) = zj/x(t) = xm,\ z(t-1) = zi)\},$$
$$\{P(y(t) = yn/z(t) = zj, x(t) = xm, z(t-1) = zi)\}, P(0)\rangle.$$

Это традиционное задание ВА, где $X = \{x_1, \ldots, x_b\}$ — входной алфавит; $Y = \{y_1, \ldots, y_n\}$ — выходной алфавит, $Z = \{z_1, \ldots, z_i\}$ — алфавит состояний; $P = \{P(z(t) = z_j/x(t) = x_m,\ z(t-1) = z_i)\}$ — множество условных вероятностей, определяющих пребывание ВА в такте времени t в состояние $z(t) = z_j$ при условии подачи в этом такте на вход параметра $x(t) = x_m$ и пребывания ВА в предшествующем такте $(t-1)$ в состоянии $z(t-1) = z_i$; $R = \{P(y(t) = y_n/z(t) = z_j,\ x(t) = x_m,\ z(t-1) = z_i)\}$ — множество условных вероятностей, определяющих наличие на выходе ВА в такте времени t параметра $y(t) = y_n$ при условии подачи в этом такте на вход параметра $x(t) = x_m$, нахождения ВА в состоянии $z(t) = z_j$ и пребывания ВА в предшествующем такте $(t-1)$ в состоянии $z(t-1) = z_i$; $P(0)$ — матрица вероятностей начальных состояний, $P(0) = \|P_1(0), P_2(0), \ldots, P_i(0)\|$, $|Z| = I$, $P_i(0) = P(z(t0) = z_i)$, $i = 1, \ldots, I$.

Процессы проектирования можно представить в виде многофазных автоматных моделей. При этом каждой фазе процесса соответствует определенная проектная процедура.

Обучающийся нечеткий автомат. Рассмотрим автомат с четким входом $i(t)$ и зависимым от времени нечетким отношением перехода $\delta(t)$. Пусть $s(t)$ — нечеткое состояние автомата в момент времени t на конечном множестве состояний $S = \{s_1, \ldots, s_n\}$ и i_l — оценка значения $i(t)$. Состояние автомата в момент времени t определяется min–max композицией

$$\mu_{s(t+1)}(s_k) = \sup \min(\mu_{s(t)}(s_j), (\mu_{\delta(t)}(s_x, i_l s_j)) \quad (\sup = \sup_j)$$

или аналогичной ей. Обучение направлено на изменение нечеткой матрицы переходов:

$$\mu_{\delta(t)}(s_k, i_l s_j) = \mu_{\delta(t-1)}(s_k, i_l s_j),\ j \neq k,$$
$$\mu_{\delta(t)}(s_k, i_l s_j) = a_k \mu_{\delta(t-1)}(s_k, i_l s_j) + (1 - a_k)\lambda_k(t),$$

где $0 < a_k < 1$, $0 < \lambda_k(t) < 1$, $k = 1, \ldots, n$. Константа λ_k определяет скорость обучения. Начало работы автомата возможно без априорной информации ($\mu_{s(0)}(s_k) = 0$ или 1), а также с априорной информацией: $\mu_{s(0)}(s_k) = \lambda_k(0)$. Параметр $\lambda_k(t)$ зависит от оценки функционирования автомата. Доказано, что имеет место сходимость матрицы переходов независимо от того, есть ли априорная информация, т.е. $\mu_{s(0)}(s_j)$ может быть любым значением из интервала [0, 1].

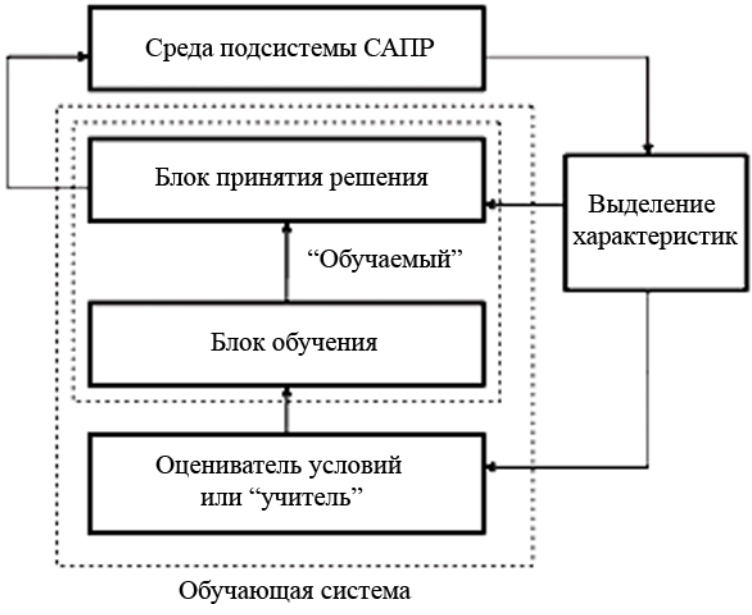

Рис. 5. Условная модель классификации угроз ИБ подсистемы САПР

Рассмотрим пример. На рис. 5 изображена условная модель классификации угроз ИБ подсистемы САПР. Роль входа и выхода можно кратко объяснить следующим образом. Во время каждого интервала времени классификатор атак получает новый образец из среды подсистемы. Далее реакция подсистемы x' обрабатывается в рецепторе, из которого поступает как в блок “обучаемый”, так и в блок “учитель” для оценки. Критерий оценки должен быть выбран так, чтобы его минимизация или максимизация отражала свойства классификации (классов угроз). Поэтому критерий может быть включен в систему, чтобы служить в качестве учителя для классификатора. Модель обучения формируется следующим образом. Предполагается, что классификатор имеет в распоряжении множество дискриминантных функций нескольких переменных. Система адаптируется к лучшему решению. Лучшее решение выделяет множество дискриминантных функций, которые дают минимум последствий среди множества дискриминантных функций для данного множества образцов атак.

К достоинствам такого подхода можно отнести возможность учета расширения САПР проектантами и тот факт, что в САПР используются CALS-технологии.

Обучение на основе условной нечеткой меры. Пусть $X = \{x_1, \dots x_n\}$ — множество причин (входов) и $Y = \{y_1, \dots y_n\}$ — множество результатов. Если h — функция из X в интервале [0, 1], $h(x_1) < \dots < h(x_n)$

и G_x — нечеткая мера на X, то

$$\int_X^{\cdot} h(x)G_x(*) = \max\min(h(Xi), Gx(Hi)), \quad i = 1, \ldots, n,$$

где $Hi = \{xi, \ldots xn\}$.

Задача состоит в оценке (уточнении) причин по нечеткой информации. Пусть G_y — нечеткая мера на Y, G_y связана с G_x условной нечеткой мерой $\sigma Y(^*\mathrm{I}x)$:

$$G_Y = \int_X^{\cdot} \sigma Y(^*\mathrm{I}x)Gx.$$

Предполагается следующая интерпретация вводимых мер: G_x оценивает степень нечеткости утверждения "один из факторов x угроз X был причиной", $\sigma Y(A\mathrm{I}x)$, $A \in Y$ оценивает степень нечеткости утверждения "один из элементов A является результатом благодаря причине x"; $G_Y(\{y\})$ характеризует степень нечеткости утверждения "y — действительный результат". Пусть $\mu A(y)$ описывает точность информации A, тогда по определению

$$G_y(A) = \int_X^{\cdot} \mu A(y)Gx.$$

Метод обучения должен соответствовать обязательному условию: при получении информации A нечеткая мера G_x меняется таким образом, чтобы $G_Y(A)$ возрастала.

Детерминированные конечные автоматы. Далее принимается, что детерминированным конечным автоматом, или просто автоматом, называется пятерка $A = (S, I, O, T, r)$, где S — конечное множество состояний с выделенным начальным состоянием r, I — входной алфавит, O — выходной алфавит и $T \subseteq I \times S \times S \times O$ — отношение переходов. Четверка $(i, p, n, o) \in T$ описывает переход в автомате из состояния p в состояние n под действием входного символа i с выходным символом o.

В теории автоматов [10] показано, что состояние q недетерминированного автомата $B = (Q, I, O, T', q)$ называется *редукцией* состояния s недетерминированного автомата $A = (S, I, O, T, s_o)$ (обозначение $q \leq s$), если $L_s(q) \subseteq L_A(s)$. Состояния q и s называются *эквивалентными* (обозначение $q \cong s$), если q есть редукция s и s есть редукция q. В противном случае состояния q и s не являются эквивалентными.

Автомат $B = (Q, I, O, T', q_o)$ есть *редукция* автомата $A = (S, I, O, T, s_o)$, если $L_B \subseteq L_A$. Если $L_B = L_A$, автоматы A и B называются эквивалентными. Для детерминированных полностью

определенных автоматов отношения редукции и эквивалентности совпадают.

Автомат, который не имеет эквивалентных состояний, называется *приведенным*. Известно [9], что для каждого автомата A существует эквивалентный приведенный автомат, который называется *приведенной формой* автомата A. Более того, для каждого недетерминированного автомата также есть эквивалентный *наблюдаемый* автомат (S, I, O, T, r), в котором для любой тройки $(i, p, o) \in I \times S \times O$ существует не более одного состояния $n \in S$ такого, что $(i, p, n, o) \in T$.

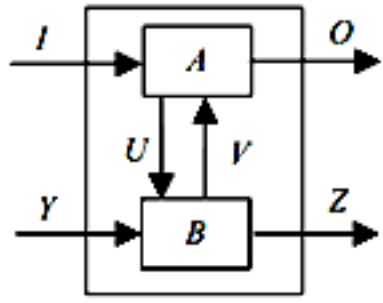

Рис. 6. Композиция автоматов

Рассмотренные модели различных автоматов можно объединить в единую модель путем композиции. Рассмотрим композицию автоматов A и B на рис. 6. Автомат A имеет входной алфавит $I \times V$ и выходной алфавит $U \times O$; автомат B имеет входной алфавит $Y \times U$ и выходной алфавит $V \times Z$. Таким образом, язык автомата A есть $LA \subseteq (I \times V \times \times U \times O)^*$, язык автомата B есть

$$L_A \subseteq (Y \times U \times V \times Z)^*.$$

Синхронная композиция (см. рис. 6) или просто композиция $A \bullet B$ автоматов A и B имеет входной алфавит $I \times Y$ и выходной алфавит $O \times Z$. Входной-выходной символ $(iyoz) \in I \times Y \times O \times Z$ принадлежит языку композиции, если и только если существует согласованная пара внутренних символов $uv \in U \times VZ$ таких, что $(ivuo) \in L_A$ и $(yuvz) \in L_B$.

Синхронная композиция автоматов строится следующим образом. Сначала язык автомата A расширяется на множество $Y \times Z$ и язык автомата B расширяется на множество $I \times O$ посредством добавления на каждом переходе всех возможных пар из алфавита расширения. Полученные языки пересекаются и строится проекция пересечения на алфавит композиции $I \times Y \times O \times Z$. Приведенный наблюдаемый автомат с полученным языком и называется композицией $A \bullet B$ автоматов A и B. Все операции над языками осуществляются на основе соответствующих известных методов [8]. В зависимости от типа автоматов композиция может быть детерминированным или недетерминированным автоматом, полностью определенным или частичным автоматом.

Выводы. Таким образом, можно утверждать, что рассмотренный автоматный подход к формализации построения модели ИБ САПР можно считать корректным и теоретически обоснованным. Практическая реализация синтезированного автомата возможна с использованием любых известных программных средств, например UML. Условия

и способы привнесения соответствующих экспертных оценок целиком определяются нечеткими условиями сохранения адекватности и полноты, которые требуют отдельного рассмотрения.

ЛИТЕРАТУРА

1. *Норенков И.П.* Разработка систем автоматизированного проектирования: М.: Изд-во МГТУ им. Н.Э. Баумана, 1994.
2. *Волосатова Т.М.*, *Чичварин И.Н.* Специфика информационной безопасности САПР // Изв. вузов. Машиностроение. 2012. Спец. вып. С. 89–94.
3. *Чичварин Н.В.* Экспертные компоненты САПР. М.: Машиностроение, 1991.
4. *Волосатова Т.М.*, *Денисов А.В.*, *Чичварин Н.В.* Комбинированные методы защиты данных в САПР // Информационные технологии. Приложение. 2012. № 5. С. 1–32.
5. *Мишин Е.Т.*, *Оленин Ю.А.*, *Капитонов А.А.* Системы безопасности предприятия – новые акценты // Ж. Конверсия в машиностроении. 1998. № 4. С. 31–47.
6. *ОКБ САПР*: Программно-аппаратные комплексы защиты информации от НСД // www.accord.ru
7. *Мещеряков В.А.*, *Вялых С.А.*, *Герасименко В.Г.* Методическое обеспечение обоснования требований к системам защиты информации от программно-математического воздействия в автоматизированных информационных системах критического применения // Безопасность информационных технологий. 1996. Вып. 2. С. 37–51.
8. *Hill I.O.* Search Technique for Multimodal Surfaces // J. IEEE Trans. 1969. Vol. SSC-5, No. 1. P. 2–8.
9. *Алгебраическая* теория автоматов, языков и полугрупп / пер. с англ.; под ред. М. Арбиба. М.: Статистика, 1975.

REFERENCES

[1] Norenkov I.P. Razrabotka sistem avtomatizirovannogo proektirovaniya [Computer-aided design]. Moscow, Bauman Moscow State Tech. Univ. Publ., 1994. 203 p.

[2] Volosatova T.M., Chichvarin I.N. Specifics of information security in CAD. *Izv. Vyssh. Uchebn. Zaved. Ser. Mashinostr. Spets. Vyp.* [Bull. Inst. Higher Educ. Ser. Mach. Constr. Spec. Issue], 2012, pp. 89–94 (in Russ.).

[3] Chichvarin N.V. Ekspertnye komponenty SAPR [Expert CAD components]. Moscow, Mashinostroenie Publ., 1991. 240 p.

[4] Volosatova T.M., Denisov A.V., Chichvarin N.V. Combined methods for protecting data in CAD. *Inf. Tekhnol.* [Inf. Technol.], 2012, no. 5, pp. 1–32 (in Russ.).

[5] Mishin E.T., Olenin Yu.A., Kapitonov A.A. Enterprise security: new accents. *Konvers. Mashinostr.* [Convers. Mach. Build.], 1998, no. 4, pp. 31–47 (in Russ.).

[6] OKB SAPR: Programmno-apparatnye kompleksy zashchity informatsii ot NSD [EDO CAD: Software and hardware systems to protect information from unauthorized access]. Available at: www.accord.ru

[7] Meshcheryakov V.A., Vyalykh S.A., Gerasimenko V.G. Methodical justification of requirements to the information protection from software and mathematical influence in automated information systems in critical applications. *Zh. Bezop. Inf. Tekhnol.* [J. Saf. Inf. Technol.], 1996, no. 2, pp. 37–51 (in Russ.).

[8] Hill I.O. Search technique for multimodal surfaces. *J. IEEE Trans*, 1969, vol. SSC-5, no. 1, pp. 2–8.

[9] Arbib M.A. Algebraic theory of machines, languages, and semi-groups. London, Academic Press, 1968. 359 p. (Russ. ed.: Arbib M. Algebraicheskaya teoriya avtomatov, yazykov i polugrupp. Moscow, Statistika Publ., 1975. 335 p.).

Статья поступила в редакцию 26.11.2012

Тамара Михайловна Волосатова — канд. техн. наук, доцент кафедры “Системы автоматизированного проектирования” МГТУ им. Н.Э. Баумана. Автор более 60 научных работ в области информационной безопасности систем автоматизированного проектирования и цифровой обработки сигналов и изображений.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

T.M. Volosatova — Cand. Sci. (Eng.), assoc. professor of "Systems of Computer-Aided Design" department of the Bauman Moscow State Technical University. Author of more than 60 publications in the field of information security of computer-aided design systems and digital processing of signals and images.
Bauman Moscow State Technical University, Vtoraya Baumanskaya ul., 5, Moscow, 105005 Russian Federation.

Иван Николаевич Чичварин — инженер кафедры “Системы автоматизированного проектирования” МГТУ им. Н.Э. Баумана. Автор трех научных работ в области информационной безопасности систем автоматизированного проектирования и цифровой обработки сигналов и изображений.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

I.N. Chichvarin — engineer of “Systems of Computer-Aided Design” department of the Bauman Moscow State Technical University. Author of three publications in the field of information security of computer-aided design systems and digital processing of signals and images.
Bauman Moscow State Technical University, Vtoraya Baumanskaya ul., 5, Moscow, 105005 Russian Federation.