УДК 004.56:519.876.2 (045)

Д.В. Домарев

Национальный авиационный университет, Киев

ПРИМЕНЕНИЕ ПОЛУМАРКОВСКИХ ПРОЦЕССОВ В РАЗРАБОТКЕ И ОПИСАНИИ СОСТОЯНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Состояние информационных систем и систем защиты информации смоделировано как полумарковский процесс. Применение полумарковских процессов в разработке систем защиты информации классифицировано при помощи матрицы связей составляющих. Сделано заключение о применимости моделей, основанных на полумарковских процессах, в разработке и описании состояния систем защиты информации для повышения точности оценки их эффективности, а также в их разработке.

Ключевые слова: *системный подход к защите информации, эффективность систем защиты информации, матрица знаний, матрица оценок, полумарковский процесс.*

Введение

Ввиду стремительного развития и повсеместного распространения информационных технологий разработка систем защиты информации стала важной частью процесса создания информационных систем (ИС). На сегодняшний день возникла проблема борьбы с новейшими угрозами (так называемыми "атаками нулевого дня"). Для повышения эффективности моделирования функционирования и атак ИС могут быть применены полумарковские процессы.

Система защиты информации (СЗИ) – это комплекс законодательных, организационных, технических и других мер и средств, и обеспечивающих защиту важной информации от угроз и каналов утечки в соответствии с указанными требованиями.

Системный подход к защите информации

СЗИ имеет целевое назначение, которое на формализованном уровне приобретает многомерный характер. Многомерная (интегральная) задача защи-

ты информации требует реализации системного подхода с использованием моделирования процессов защиты на основе научных методов.

Специфическими особенностями решения такой задачи являются:

а) многокритериальность, связанная с необходимостью учета большого числа частных показателей (требований);

б) неполнота и неопределенность исходной информации;

в) невозможность применения классических методов оптимизации;

г) необходимость как качественных, так и количественных показателей эффективности систем защиты информации.

Системный подход в процессе защиты информации – это способ мышления и анализа, согласно которому система защиты рассматривается как совокупность взаимосвязанных элементов, имеющих общую цель - обеспечить безопасность информации. При целенаправленном объединении элементов СЗИ приобретает специфические свойства, изначально не присущие ни одной из ее составных частей. При этом первостепенное значение имеют те свойства элементов защиты, которые определяют степень их взаимодействия и оказывают влияние на систему в целом.

В методическом плане определение эффективности СЗИ заключается в измерении соответствующих показателей и выработке суждения относительно соответствия тех или иных способов и средств защиты заданным требованиям и целевому назначению СЗИ.

Следовательно, процесс создания СЗИ подразумевает установление жестких логических и функциональных связей между разнородными компонентами безопасности. При этом значимость свойств отдельных элементов СЗИ снижается, а на первый план выдвигаются общесистемные задачи. Как показывает практика, именно качество указанных связей определяет эффективность системы защиты в целом.

Повысить эффективность СЗИ может предложенный В.В. Домаревым в [1] системный подход, определяющий взаимные связи между понятиями, определениями, принципами, способами и механизмами защиты. Системный подход применим не только в разработке СЗИ, но и на всех этапах жизненного цикла ИС. При этом все средства, методы и мероприятия, используемые для защиты информации, объединяются в единый механизм.

Модель ИБ, используемая в системном подходе разделена на три группы составляющих: основы (из чего состоит), направления (для чего предназначена), этапы (как работает). Отношения компонентов представлены в виде матрицы знаний, в которой содержание каждого элемента описывает взаимосвязь составляющих (рис. 1).

Этапы >>>	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	044	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Рис. 1. Нумерация элементов матрицы знаний

Определение полумарковского процесса

Полумарковский процесс – это Марковский процесс со случайными интервалами между переходами. Описывая полумарковский процесс с N состояниями, необходимо указать N2 условных вероятностей pij, определяющих, что следующий переход произойдет в состояние j, из текущего состояния i, и удовлетворяющих условия

$$\sum_{j=1}^{N} p_{ij} = 1,\ i = 1,2,...,N; \qquad p_{ij} \geq 0,\ 1 \leq i, j \leq N.$$

Длительности временных промежутков между переходами – случайные величины τij, определяемые соответствующим множеством из N2 функций плотности распределения,

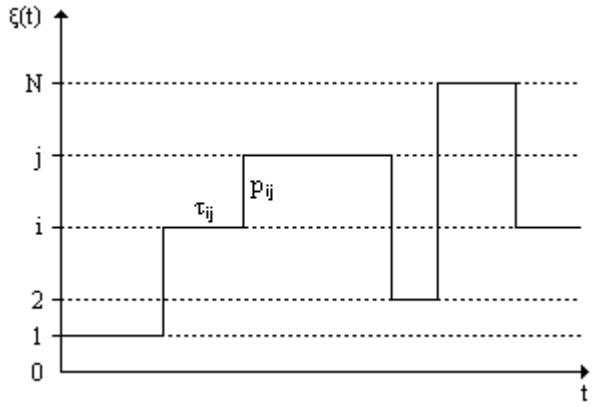
$$h_{ij}(\cdot),\ 1 \le i, j \le N.$$

Таким образом, удобно описывать полумарковский процесс матрицами вероятностей переходов и функций плотности распределения длительностей задержек, размером N×N, соответственно:

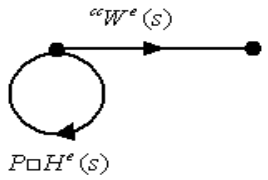
$$P = \{pij\} \text{ и } H(\cdot) = \{hij(\cdot)\}.$$

Каждый раз, когда процесс попадает в определенное состояние, выбирается следующее состояние и длительность задержки в соответствии с вероятностями переходов и функциями плотности распределения длительностей задержек. После задержки в состоянии i на время τij, процесс переходит в состояние j, а затем процедура повторяется.

Пусть текущее состояние ξ(t). Учитывая, что моделируется СЗИ, повторные переходы системы в одно и то же состояние рассматриваться не будут (pii = 0). Диаграмма полумарковского процесса представлена на рис. 2, а.



а



б

Рис. 2. Диаграмма и граф состояний общего вида полумарковского процесса

Пусть ccW(t) = {ccwi(t)} – диагональная матрица вероятностей того, что система не покинет состояние i до истечения времени t.

Матричный граф состояний полумарковских переходов представлен на рис. 2, б. Окончательно полумарковский процесс описывается матрицей вероятностей интервальных переходов

$$Фe(s) = [I - P \square He(s)] - 1\ ccWe(s),$$

где I – единичная матрица; □ – поэлементное умножение; e(s) – матрица преобразований Лапласа:

$$f^{e}(s) = \int_0^{\infty} f(t)e^{-\delta t}dt.$$

Состояние СЗИ как полумарковский процесс

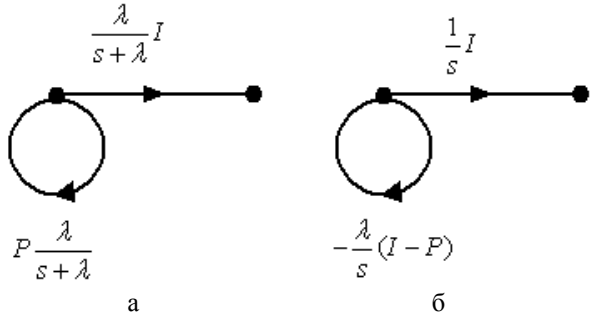
Состояние как ИС, так и СЗИ может быть описано как непрерывный полумарковский процесс с произвольной матрицей вероятностей перехода и экспоненциально распределенными длительностями задержек:

$$h_{ij}(t) = \lambda e^{-\lambda t}, \qquad 1 \le i, j \le N.$$

Тогда матрица вероятностей интервальных переходов будет иметь вид

$$\Phi^{e}(s) = [s + \lambda(I - P)]^{-1} = \left[I + \frac{\lambda}{s}(I - P) \right]^{-1} \cdot \frac{1}{s},$$

а граф состояний приобретет одну из двух форм, представленных на рис. 3.



а б

Рис. 3. Матричные графы состояний непрерывного полумарковского процесса

Вышеизложенное описание состояния ИС может быть принято за основу обобщенной модели ее функционирования. Основное назначение общих моделей состоит в создании предпосылок для объективной оценки общего состояния ИС с точки зрения меры уязвимости или уровня защищенности информации в ней. Необходимость в таких оценках обычно возникает при анализе общей ситуации с целью выработки стратегических решений при организации защиты информации. Общими моделями систем и процессов защиты информации названы такие, которые позволяют определять (оценивать) общие характеристики указанных систем и процессов в отличие от моделей локальных и частных, которые обеспечивают определение (оценки) некоторых локальных или частных характеристик систем или процессов.

Ниже представлен краткой перечень и характеристики моделей, в которых могут быть применены полумарковские процессы.

Общая модель процесса защиты информации. Данная модель в самом общем виде и для самого общего объекта защиты должна отображать

процесс защиты информации как процесс взаимодействия случайных дестабилизирующих факторов, воздействующих на информацию, и средств защиты информации, препятствующих действию этих факторов. Итогом взаимодействия будет тот или иной уровень защищенности информации;

Обобщенная модель системы защиты информации. Являясь дальнейшим развитием общей модели процесса защиты, обобщенная модель системы защиты должна отображать основные процессы, осуществляемые в ней с целью рационализации процессов защиты. Указанные процессы в самом общем виде могут быть представлены как процессы распределения и использования ресурсов, выделяемых на защиту информации, как реакции на случайным образом изменяющееся воздействие дестабилизирующих факторов;

Модель общей оценки угроз информации. Основной направленностью этой модели является оценка не просто угроз информации как таковых, а еще и оценка тех потерь, которые могут иметь место при проявлений различных угроз. Модели данного направления важны еще и тем, что именно на них в наибольшей степени были выявлены те условия, при которых такие оценки могут быть адекватны реальным процессам защиты информации;

Модели анализа систем разграничения доступа к ресурсам ИС. Модели этого класса предназначены для обеспечения решения задач анализа и синтеза систем (механизмов) разграничения доступа к различным видам ресурсов ИС и, прежде всего, к массивам данных или полям ЗУ. Выделение этих моделей в самостоятельный класс общих моделей обусловлено тем, что механизмы разграничения доступа относятся к числу наиболее существенных компонентов систем защиты информации, от эффективности функционирования которых, в значительной мере зависит общая эффективность защиты информации в ИС. В этих моделях полумарковским процессом может быть представлен доступ к информации разной степени секретности, где состояниями будут аутентификации на различных уровнях защиты.

Применение полумарковских процессов в разработке СЗИ

Проектирование, организация и применение СЗИ фактически связаны с неизвестными событиями в будущем и поэтому всегда содержат элементы неопределенности. Кроме того, присутствуют и другие причины неоднозначности, такие как недостаточно полная информация для принятия управленческих решений или социально-психологические факторы. Поэтому, например, этапу проектирования СЗИ естественным образом сопутствует значительная неопределенность. Ее уровень можно понизить, применяя наиболее адекватные модели.

Полумарковские процессы могут быть использованы в разработке СЗИ как универсальное средство моделирования работы ИС на этапах выявления угроз и каналов утечки информации, а также проведения оценки уязвимости и рисков. Область их применения соответствует элементам 204 и 304 (рис. 4). Ноль на втором знакоместе означает распространение на все направления. Таким образом, полумарковские процессы состоят в наборе средств:

Этапы >>>	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	044	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Рис . 4. Область применения полумарковских процессов в матрице знаний

а) обеспечивающих оперативность и качество выявления потенциальных каналов утечки информации на объектах ИС, в процессах и программах ИС, при передаче информации по каналам связи, за счет ПЭМИН, а также в процессе управления системой защиты;

б) определяющих проведение оценки уязвимости и рисков для информации на объектах ИС, в процессах и программах ИС, при передаче информации по каналам связи, за счет ПЭМИН, а также в процессе управления системой защиты.

Применение полумарковских процессов в описании состояния СЗИ

В соответствии с современной теорией оценки эффективности систем, качество системы защиты информации проявляется лишь в процессе его использования по назначению (целевое функционирование), поэтому наиболее объективным является оценивание по эффективности применения.

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	044	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	0,67	0,09	0,07	0,60	0,77	0,20	0,88	0,74	0,28	0,03	0,40	0,53	0,14	0,78	0,58	0,56	0,36	0,72	0,78	0,64
200	Выявление угроз и каналов утечки информации	0,19	0,87	0,78	0,76	1,00	0,93	0,36	0,07	0,38	1,00	0,81	0,12	0,53	0,04	0,94	0,17	0,94	0,37	0,30	0,83
300	Проведение оценки уязвимости и рисков	0,04	0,29	0,89	1,00	0,41	0,56	0,89	0,15	0,97	0,84	0,12	0,14	0,70	1,00	1,00	0,74	0,92	0,90	0,22	0,15
400	Определение требований к СЗИ	0,20	0,68	0,07	0,24	0,43	1,00	1,00	1,00	0,27	0,30	0,81	0,02	0,81	0,67	0,76	0,54	0,52	0,66	0,74	0,71
500	Осуществление выбора средств защиты	0,14	0,41	0,88	0,94	0,93	0,58	0,94	0,90	0,76	0,62	0,56	0,93	0,81	0,84	0,03	0,33	0,48	0,68	0,46	0,52
600	Внедрение и использование выбранных мер и средств	0,23	0,79	1,00	0,36	0,03	0,80	0,01	0,00	1,00	0,82	0,76	0,63	1,00	0,53	0,22	0,00	0,84	0,41	0,16	0,08
700	Контроль целостности и управление защитой	0,24	0,55	0,05	0,71	0,14	0,92	0,02	0,86	0,75	0,74	0,86	0,01	0,11	0,28	0,92	1,00	0,07	0,31	0,75	0,75

Рис . 5. Матрица оценок

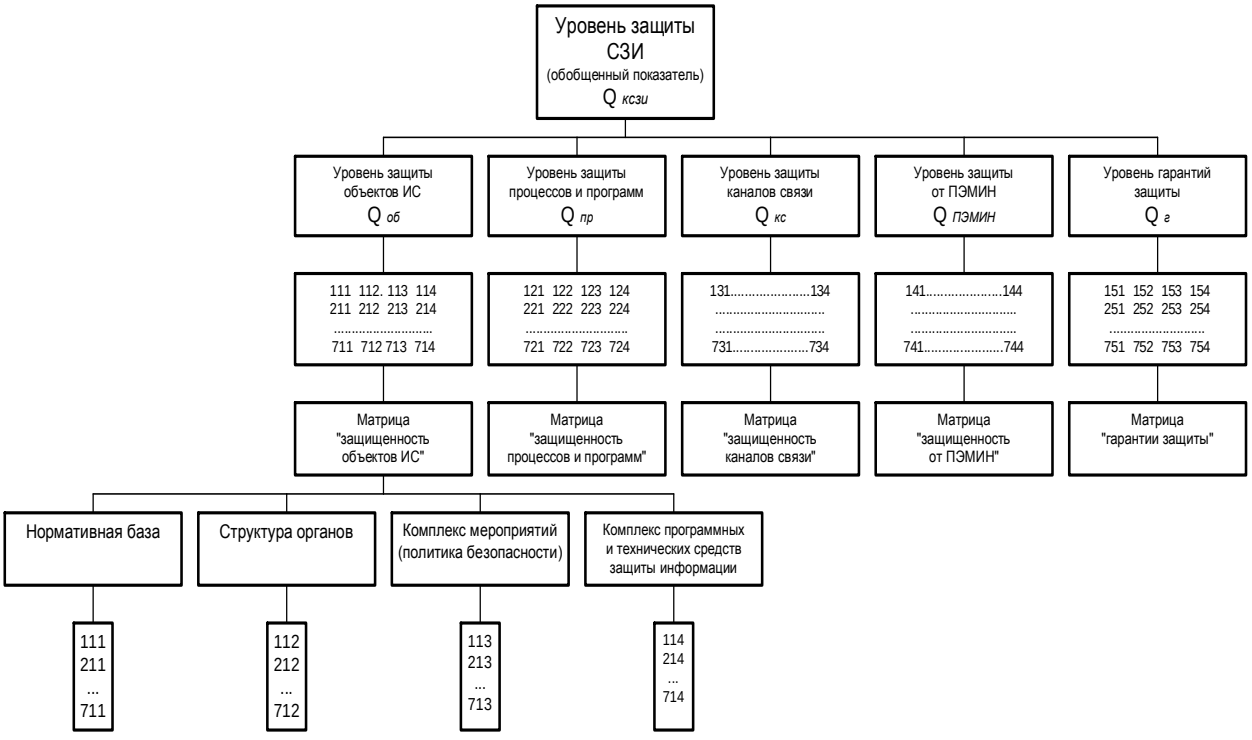


Рис. 6. Логическое дерево формирования показателей защищенности ИС

В основу комплекса показателей и критериев оценки эффективности СЗИ должна быть положена вероятность выполнения задачи системой (обеспечение требуемого уровня защищенности). При этом критериями оценки служат понятия пригодности и оптимальности. Пригодность означает выполнение всех установленных к СЗИ требований, а оптимальность – достижение одной из характеристик экстремального значения при соблюдении ограничений и условий на другие свойства системы

Для описания состояния СЗИ достаточно составить матрицу оценок (рис. 5), содержащую в ячейках оценки эффективности соответствующих элементов системы. С изменением любого параметра ИС, за счет логических связей изменяются один или несколько элементов в матрице оценок, что влияет на обобщенные показатели (рис. 6), следовательно, общее состояние СЗИ изменяется.

Учитывая, характер этих изменений, можно предположить, что функционирование СЗИ также является полумарковским процессом, что позволяет описывать изменения его состояния при помощи относительно простой математической модели. Математические модели функционирования ИС на основе полумарковских процессов могут быть использованы для симуляции атак на ИС, что повысит эффективность разработки противодействия угрозам.

Вывод

Полумарковские процессы могут быть применены в разработке и описании состояния систем защиты информации.

Модели работы информационных систем и систем защиты информации, основанные на полумарковских процессах, могут быть использованы для повышения точности оценки эффективности СЗИ, а также в их разработке.

Список литературы

1. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К.: ООО «ТИД «ДС», 2004. – 992 с.

2. Howard R.A. System analysis of semi-Markov processes / R.A. Howard // IEEE Transactions on Military Electronics, Vol. 8, issue 2, Apr. 1964. – P. 114-124.

3. Баутов А. Эффективность защиты информации. Открытые системы / А. Баутов. – 08, 2003. – № 07 – 268 с.

Поступила в редколлегию 18.02.2009

Рецензент: канд. техн. наук, доцент С.В. Кавун, Харківський національний економічний університет, Харків.

ЗАСТОСУВАННЯ НАПІВМАРКІВСЬКИХ ПРОЦЕСІВ У РОЗРОБЦІ ТА ОПИСУ СТАНУ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Д.В. Домарєв

Стан інформаційних систем і систем захисту інформації змодельований як полумарковский процес. Застосування полумарковских процесів у розробці систем захисту інформації класифіковано за допомогою матриці зв'язків складових. Зроблено висновок про застосовність моделей, заснованих на полумарковских процесах, у розробці й описі стану систем захисту інформації для підвищення точності оцінки їхньої ефективності, а також у їх розробці.

Ключові слова: *системний підхід до захисту інформації, ефективність систем захисту інформації, матриця знань, матриця оцінок, полумарковский процес.*

APPLICATION OF SEMI-MARKOV PROCESSES IN DESIGN AND STATE DESCRIPTION OF INFORMATION SECURITY SYSTEMS

D.V. Domarev

The Condition of the information systems and systems of protection to information simulate as semi-Markov process. Using semi-Markov processes in system development of protection information is classified at matrixes of the relationships of the component. Conclusion is Made about prima models, founded on semi-Markov process, in development and description of the condition of the systems of protection to information for increasing of accuracy of the estimation to their efficiency, as well as in their development.

Keywords*: system approach to protection of information, efficiency of the systems of protection in-sytuctures, matrix of the knowledges, matrix estimation, semi-Markov process.*