Дровникова Ирина Григорьевна,
доктор технических наук, доцент;
Алфёров Владимир Павлович,
Овчинникова Елена Сергеевна

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДИНАМИКИ ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

MATHEMATICAL MODEL OF DYNAMICS OF FUNCTIONING OF SUBSYSTEM OF PROTECTION OF CONFIDENTIAL INFORMATION IN SYSTEMS OF ELECTRONIC DOCUMENT FLOW

В статье представлена математическая модель динамики функционирования подсистемы защиты конфиденциальных сведений в системах электронного документооборота, разработанная на основе графовой формализации с использованием аппарата сетей Петри и описанная с помощью матрицы вероятностно-временных характеристик переходов между состояниями функционирования системы. Модель позволяет обеспечить количественный анализ показателя эффективности указанных систем, используя математический аппарат теории конечных полумарковских процессов.

The article presents a mathematical model of the dynamics of the subsystem of protection of confidential information in electronic document management systems, developed on the basis of graph formalization using the apparatus of Petri nets and described by a matrix of probabilistic-temporal characteristics of transitions between states of the system. The model provides a quantitative analysis of the efficiency of these systems using the mathematical apparatus of the theory of finite semi-Markov processes.

Для проведения исследования процессов защиты информационного ресурса (ЗИР) в современных сложных системах, включая системы электронного документооборота (СЭД), широко используются методы математического моделирования [1]. При этом качество модели определяется адекватностью формализации динамики функционирования подсистемы защиты конфиденциальных сведений (ПЗКС) СЭД. Для осуществления указанной формализации предлагается использовать аппарат сетей Петри [2], разработанный в рамках теоретико-графового подхода к формализации процессов функционирования систем [3].

Для сетей Петри характерно наличие ряда особенностей, существенно расширяющих их потенциал при моделировании системы: существуют позиции различного типа, где единственная дуга входит в соответствующую позицию или выходит из неё; имеющийся случайный переход связан с переменной, значение которой характеризуется ненулевой задержкой, отражающей время,

и динамическими элементами сети, представляющими собой фишки, обладающие свойствами атрибутов объектов; для реализации управления переключениями и условными ветвлениями в процессе перемещения объектов определены разрешающие позиции.

Имеет место структурная связь между позицией, переходом и дугой. Переход l в совокупности с его структурными связями составляет соответствующую ему элементарную сеть E_l [2]. В данном случае позиции, образующие структурную связь позиции с переходом, считаются входными, в то же время позиции, образующие структурную связь обратного вида, — выходными для обычной простой сети.

Существующее разделение элементарных сетей позволяет создавать сети Петри любой сложности путём соединения этих сетей из произвольно выбранного их конечного множества. В любой элементарной сети возможна единственная разрешающая входная позиция, которая описывается конечным числом состояний, разрешающей процедурой и в начале активной фазы сработавшего перехода решает функциональную задачу управления. Положение, представляющее собой текущее состояние разрешённой позиции простой сети, рассчитывается на основе разрешённой существующей процедуры, определяющей конкретную позицию (выход), в которую из входного состояния перейдёт объект после срабатывания соответствующего перехода.

Движение ПЗКС между позициями как результат срабатывания соответствующих переходов характеризует динамику сети Петри. Условием срабатывания перехода элементарной сети является наличие объекта в одной из его входных позиций (то есть позиция должна быть маркированной). Если элементарная сеть содержит разрешающую позицию, то необходимо предварительно определить её текущее состояние, вычисляя имеющуюся разрешённую процедуру. Фаза срабатывания перехода определяется параметром τ, имеющим значение временной задержки. Движение ПЗКС осуществляется в том и только в том случае, если при наступлении завершения фазы произошло её перемещение из соответствующей позиции (входной) в текущую конечную (завершающую) позицию, реализующую процедуру преобразования π над атрибутами подсистемы.

Формализации динамики функционирования ПЗКС должно предшествовать проведение её априорной многоуровневой структуризации [4]. При этом существующий процесс эксплуатации ЗИР может представляться в виде последовательности выполнения различных функций ПЗКС СЭД. Точная идентификация текущих состояний функций по ЗИР ПЗКС конкретным состояниям позиций сети определяет формальное описание произвольного допускаемого перехода между случайными состояниями с использованием возможностей существующей простой сети. Имеющие вероятностный характер переходы между случайными состояниями выполнения ПЗКС защитных функций могут реализовываться разрешёнными функциональными процедурами. Реальная эксплуатация ПЗКС может быть представлена конкретным положением подсистемы в существующей сети и её параметрами-атрибутами. При этом чётко прослеживается явная идентичность между

временными моментами определения ПЗКС в сети (её однозначного ухода из сети) и моментами, связанными с обращением к ПЗКС и характеризующими завершение эксплуатации подсистемы по своему прямому функциональному назначению. Реальное движение объекта по соответствующим позициям и изменение его атрибутов с использованием преобразования π характеризуется изменением длительности состояния функционирования ПЗКС, вычисляемой с помощью процедуры временной задержки τ [4].

Элементарные сети позволяют построить графовую формализацию динамики функционирования произвольной ПЗКС в том случае, если все входные простые позиции соответствуют одинаковому состоянию функционирования подсистемы в любой её простой сети. В результате становится целесообразным реальное применение процедуры, связанной с временем переходных задержек, которая соответствует имеющейся простой сети. Данный способ позволяет математически описать временной фактор, непосредственно связанный с реальным нахождением ПЗКС в конкретном состоянии выполнения функциональной задачи. Таким образом, можно утверждать, что имеет место определённое равенство между количеством функциональных задач ПЗКС и формальной моделью элементарных сетей Петри [5].

Графовая модель динамики функционирования исследуемой ПЗКС приведена на рисунке 1. Сведения о сервисных задачах и соответствующим им функциях ЗИР, описывающих процесс функционирования исследуемой подсистемы, полученные с использованием данных для типовой ПЗКС [5], представлены в таблице 1. Функциональные задачи ЗИР, определяемые состояниями 1.0 и 0, необходимо рассматривать как фиктивные, описывающие выполнение начальной и завершающей функций ПЗКС по соответствующему обращению.

Для оценки эффективности мероприятий по управлению разграничением доступа (РД) к программно-информационному ресурсу (ПИР) СЭД значительный интерес представляет своевременность реализации ПЗКС защитных функций.

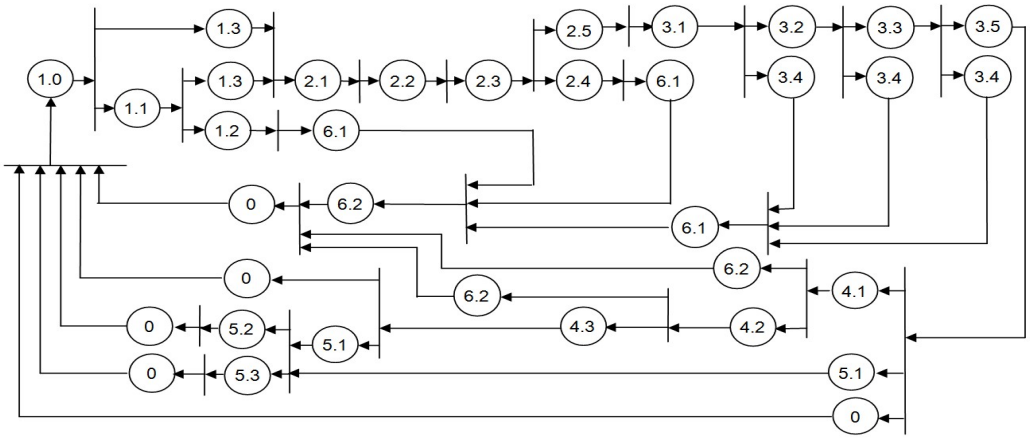


Рис. 1. Графовая модель динамики функционирования исследуемой ПЗКС

Таблица 1

Сервисные задачи и функции ЗИР, характеризующие процесс функционирования исследуемой ПЗКС

Номер и наименование	
Сервисная задача	Функция
1. «Закрытие от загрузки через внешний накопитель»	1.0. Фиктивная функция — начало реализации функций ПЗКС по данному обращению
	1.1. Идентификация системного накопителя
	1.2. Блокировка клавиатуры и монитора
	1.3. Допуск пользователя к системе
2. «Обеспечение санкционированного доступа»	2.1. Идентификация пользователя
	2.2. Ввод пароля
	2.3. Аутентификация пользователя
	2.4. Блокировка клавиатуры и монитора
	2.5. Допуск пользователя в систему
3. «Разграничение доступа»	3.1. Проверка полномочий доступа к логическим дискам
	3.2. Проверка полномочий доступа к файлам, каталогам и функциональным клавишам
	3.3. Проверка полномочий доступа по действиям над файлами
	3.4. Блокировка клавиатуры и монитора
	3.5. Допуск пользователя к ресурсам
4. «Поддержание целостностирабочей среды»	4.1. Обнаружение изменений в вычислительной среде, вызванных машинными сбоями
	4.2. Автоматическое восстановление компонент вычислительной среды
	4.3. Информирование пользователя об отсутствии повреждений вычислительной среды
5. «Преобразование данных»	5.1. Ввод запроса по форме преобразования информации
	5.2. «Прозрачное» преобразование информации
	5.3. Специальные преобразования отдельных файлов
6. «Администрирование работы ПЗКС»	6.1. Снятие блокировки клавиатуры и монитора
	6.2. Регистрация нарушений работоспособности ПЗКС и инструкций по работе с ней
0. Фиктивная задача «Окончание реализации функций ПЗКС»	0. Окончание реализации функций ПЗКС по данному обращению

Время реализации ПЗКС защитных функций в общем случае является величиной случайной. Поскольку для обеспечения функционирования ПЗКС необходимо учитывать временную избыточность при проектировании СЭД, то существенную роль играет не наличие времени реализации подсистемой защитных функций, а факт возможного превышения им некоторого максимального значения, которое рассчитывается с использованием временной избыточности СЭД [4, 5]. Максимально допустимое время может задаваться в виде детерминированной или случайной величины. Защитные функции ПЗКС рассматриваются как своевременно реализованные при условии, что время τ_{pi} выполнения функций ЗИР не будет превышать некого максимального времени $\tau_{\max}$, нормированного эксплуатационной документацией на СЭД и рядом требований разработки ПЗКС [5]:

$$\tau_{pi} \le \tau_{\max}. \qquad (1)$$

В формуле (1) τ_{pi} следует рассматривать, как промежуток времени между моментом обращения к ПЗКС и моментом окончания выполнения подсистемой защитных функций по конкретному обращению. В случае превышения τ_{pi} максимально допустимого значения становится возможным не

только нарушение защищённости СЭД, но и снижение эффективности функционирования системы по своему прямому назначению.

Выше изложенное показывает, что важное значение для оценки эффективности мероприятий по управлению РД к ПИР СЭД имеют вероятностно-временные характеристики (ВВХ) динамики функционирования ПЗКС, которые целесообразно оценивать с использованием количественного показателя эффективности функционирования подсистемы. Оценку количественного показателя эффективности функционирования ПЗКС при управлении РД к ПИР СЭД предлагается осуществлять по показателю вероятности своевременной реализации ПЗКС защитных функций E [4] в соответствии с неравенством:

$$E = P(\tau_{pi} \le \tau_{\max}). \qquad (2)$$

Поскольку оба параметра, представленные в модели, являются случайными величинами, то и выражение (2) имеет вероятностный характер. В этом случае случайная величина $\tau_{\max}$ аппроксимируется экспоненциальным законом распределения [1, 5, 6].

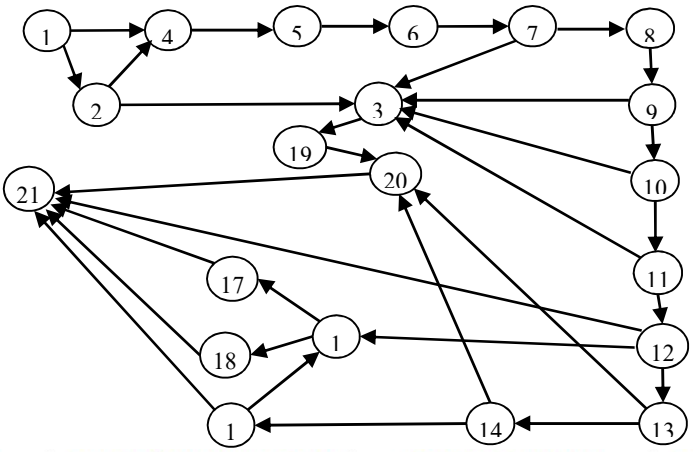
С целью формализации процесса функционирования ПЗКС как сложной динамической системы необходимо разработать математическую модель указанного процесса с использованием основных положений теории графов. Для этого целесообразно использовать матрицу $\|H_{ij}(\tau)\|$, случайные элементы которой $H_{ij}(\tau)$ носят вероятностный характер и представляют собой вероятность того, что при условии срабатывания случайного перехода сети Петри ПЗКС перейдёт из состоянии i в текущее случайное состояние j за время, меньшее τ [5]. При проведении анализа имеющейся случайной модели адекватным математическим аппаратом является использование теории конечных полумарковских процессов (КПМП) [6]. В данном случае динамика функционирования ПЗКС представляется КПМП, описывающимся полумарковской матрицей $H = \|H_{ij}(\tau)\|$, что характеризуется инвариантностью закона распределения времени нахождения ПЗКС в любом случайном (с определённой вероятностью перехода) состоянии. Представленная полумарковская модель в соответствии с теорией конечных марковских процессов и КПМП описывается матрицей вероятностей случайных переходов в различные состояния сети Петри, что позволяет проводить количественную оценку эффективности функционирования ПЗКС [5]. Можно констатировать, что конечное состояние сети Петри, соответствующее выполнению функциональной задачи ПЗКС по ЗИР в СЭД, является поглощающим. Состояния КПМП соответствуют случайным вероятностным состояниям эксплуатации ПЗКС и могут нумероваться натуральными числами в промежутке от 1 до n (1 и n — начальное и конечное состояния соответственно), а случайная величина τ_{pi} рассматривается как временной интервал между входами КПМП в начальное (1-ое) и в конечное (n-ое) состояния. Графическое представление КПМП, моделирующего динамику функционирования ПЗКС с целью оценки количественного показателя её эффективности, приведено на рисунке 2, а взаимосвязь состояний указанного процесса с соответствующими

функциями ЗИР графовой формализации динамики функционирования ПЗКС — в таблице 2.

Рис. 2. КПМП, моделирующий динамику эксплуатации ПЗКС СЭД

Таблица 2

Соответствие состояний КПМП функциям ЗИР процесса функционирования ПЗКС



Номер состояния КПМП	Номер функции ПЗКС	Номер состояния КПМП	Номер функции ПЗКС
1	1.0	12	3.5
2	1.1	13	4.1
3	1.2, 2.4, 3.4	14	4.2
4	1.3	15	4.3
5	2.1	16	5.1
6	2.2	17	5.2
7	2.3	18	5.3
8	2.5	19	6.1
9	3.1	20	6.2
10	3.2	21	0
11	3.3		

Таким образом, разработана математическая модель динамики функционирования ПЗКС в СЭД, обеспечивающая количественный анализ эффективности функционирования ПЗКС. Предложенная математическая модель включает формализацию динамики функционирования ПЗКС на основе аппарата сетей Петри и её описание с использованием матрицы, отражающей ВВХ переходов между состояниями функционирования подсистемы. В качестве математического аппарата, применяемого для анализа

данной модели, предложен аппарат теории КПМП.

ЛИТЕРАТУРА

1. Советов Б.Я. Моделирование систем: учеб. для вузов / Б.Я. Советов, С.А. Яковлев. — 3-е изд., перераб. и доп. — М.: Высш. шк., 2001. — 343 с.
2. Мараховский В.Б. Моделирование параллельных процессов. Сети Петри / В.Б. Мараховский, Л.Я. Розенблюм, А.В. Яковлев. — СПб.: Профессиональная литература, 2014. — 400 с.
3. Торопов Б.А. Теоретико-графовая формализация некоторых аналитических задач, возникающих в ходе расследования преступлений / Б.А. Торопов // Кибернетика и программирование. — 2018. — № 3. — С.48-56.
4. Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса при её проектировании в системах электронного документооборота: монография / И.И. Застрожнов [и др.]. — Воронеж: Воронеж. гос. техн. ун-т, 2015. — 106 с.
5. Авсентьев О.С. Методика управления защитой информационного ресурса системы электронного документооборота / О.С. Авсентьев, И.Г. Дровникова, И.И. Застрожнов, А.Д. Попов, Е.А. Рогозин // Труды СПИИРАН. № 2 (57) (2018). — С.-Пб.: СПИИРАН, 2018. — 2018. — № 2(57). — С. 188-210. — DOI 10.15622/sp.57.8.
6. Даниленко А.В. Безопасность систем электронного документооборота. Технология защиты электронных документов / А.В. Даниленко. — М.: Ленанд, 2015. — 232 с.