АНАЛИЗ МОДЕЛЕЙ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ МОДИФИЦИРОВАННЫХ СЕТЕЙ ПЕТРИ

Яхонтов Иван Владимирович
Аспирант, Всероссийская государственная налоговая академия Министерства финансов Российской Федерации
05.13.19
ivan.yakhontov@gmail.com

Аннотация. *В статье рассмотрены различные методы анализа и построения систем защиты информации на основе сетей Петри.*
Ключевые слова: информация, информационная безопасность, сети Петри, системы защиты информации.

THE ANALYSIS OF MODELS OF INFORMATION PROTECTION SYSTEMS ON THE BASE OF MODIFIED PETRI NETWORKS

Yakhontov Ivan Vladimirovich
Postgraduate student,
The tax academy of the Russian Federation

Abstract. *In article various methods of the analysis and construction of information systems protection based on Petri's networks are considered.*
Key words: information, information security, networks of Petri, system of protection of the information.

Введение

Насколько важна любая информация, относящаяся к бизнесу понятно многим. Пользуясь собранной и обработанной информацией, можно успешно конкурировать на своем рынке и захватывать новые. Информация помогает в поиске партнеров и способствует четкому определению позиции по отношению к ним.

Кроме того, при переходе к рыночной экономике информация становится товаром и должна поэтому подчиняться специфическим законам товарно-рыночных отношений. В этих условиях проблема защиты информации весьма актуальна и для организаций любой формы собственности.

Вопросы безопасности — важная часть концепции внедрения новых информационных технологий во все сферы жизни общества. Широкомасштабное использование вычислительной техники и телекоммуникационных систем в рамках территориально-распределенной сети, переход на этой основе к безбумажной технологии, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости.

Системный подход обеспечивает адекватную многоуровневую защиту информации, рассматриваемую как комплекс организационно-правовых и технических мероприятий. Кроме того, при реализации механизмов защиты должны использоваться передовые, научно обоснованные технологии защиты, обеспечивающие требуемый уровень безопасности, приемлемость для пользователей и возможность наращивания и модификации систем защиты информации (СЗИ) в дальнейшем.

Современные вычислительные системы могут работать в мультипрограммном режиме (одновременно решается несколько задач), в

мультипроцессорном режиме (создаются условия для решения программы задачи несколькими параллельно работающими процессорами), а также в режиме разделения времени, когда к информационным ресурсам одновременно может обращаться большое количество абонентов. При таких режимах работы в памяти компьютеров одновременно могут храниться программы и массивы данных различных пользователей, с ПК или серверами одновременно будет поддерживать связь значительное число абонентов. В этом случае необходимо решение как проблем физической защиты информации, так и защита ее от пользователей несанкционированно вклинивающихся в вычислительный процесс.

В условиях возрастающих возможностей современной технологий задача совершенствования средств анализа, оценки и оптимизации систем физической защиты, особенно на ранних этапах проектирования, становится все более актуальной. Это связано в первую очередь с возрастающей сложностью систем физической защиты и увеличением числа, альтернативных вариантов построения системы. В то же время, важность решения задачи обеспечения безопасности объектов жизнедеятельности человека предъявляет жесткие требования к эффективности систем физической защиты и рентабельности проектных решений, что диктуется условиями рыночной экономики. При этом высокая стоимость систем физической защиты не позволяет провести практическую проверку принимаемых проектных решений. Сложный и дорогостоящий процесс проектирования систем физической защиты предъявляет жесткие требования к проектным решениям, принятым на ранних стадиях разработки проекта.

1. Анализ систем физической защиты информации

Анализ моделей СЗИ проводился по следующим показателям:

- возможность рассчитать вероятность реализации угрозы в зависимости от используемых средств защиты, и уязвимостей в них;
- возможность рассчитать время реализации угрозы в зависимости от используемых средств защиты, уязвимостей в них;
- возможность моделирования параллельных процессов преодоления СЗИ;
- возможность моделирования скоординированных действий группы злоумышленников;

Для наглядности результаты сравнительного анализа были помещены в таблицу 1:

«+» возможность реализации данной характеристики;

«–» невозможность реализации данной характеристики;

В результате анализа моделей СЗИ можно сказать, что для оценки защищенности информационной системы (ИС), из рассмотренных моделей, наиболее подходящей с точки зрения характера получаемых показателей является модель, построенная с использованием вероятностных сетей Петри

Таким образом, обобщая полученные результаты анализа, выделим следующее.

Для построения модели оценки защищенности ИС были определены структурные компоненты исследуемой ИС, подлежащие защите, выделены защищаемые ресурсы ИС, проведен анализ модели типичного поведения злоумышленника при взломе ИС, были сформулированы особенности процесса реализации угроз.

В результате анализа моделей СЗИ можно сказать, что для оценки защищенности ИС, из рассмотренных моделей наиболее подходящей с точки зрения характера получаемых показателей является модель, построенная с использованием вероятностных сетей Петри, так как она позволяет рассчитать вероятность реализации угрозы за заданное время и поддерживает возможность моделирования параллельных процессов преодоления СЗИ и моделирования скоординированных действий группы злоумышленников.

Э.Р. Бейбутов в своей статье «Анализ защищенности корпоративных систем на основе

Таблица 1

Результаты сравнительного анализа программных средств оценки эффективности системы безопасности

Критерии оценки Модель СЗИ	возможность рассчитать вероятность реализации угрозы	возможность рассчитать время реализации угрозы	возможность моделирования параллельных процессов преодоления СЗИ	возможность моделирования скоординированных действий группы злоумышленников
обобщенные модели	-	-	-	-
модели, теории вероятностей	+	-	-	-
модели, теории случайных процессов	+	+ (для полумарк.)	-	-
модели, теории сетей Петри	+	+	+	+
модели, теории автоматов	-	-	-	-
модели, теории графов	-	-	-	-
модели, теории нечетких множеств	+	-	-	-
модели, теории катастроф	+	-	-	-
модели, теории игр	-	-	-	-
модели, энтропийного подхода	-	-	-	-

вероятностных сетей Петри» [6] рассматривает основные элементы защиты корпоративных систем (КС) от внешних и внутренних угроз. Он говорит, что получить количественную оценку защищенности и определить уровень доверия можно с помощью моделирования критических событий, используя вероятностные сети Петри.

Метод, изложенный в его статье, предполагает:

1) выделение и моделирование отдельных механизмов защиты от конкретных типов угроз;

2) вычисление вероятности реализации выбранных типов угроз;

3) определение общей вероятности нарушения безопасности объектов КС;

4) вывод уровня доверия к защищенной КС, исходя из рангов защищаемых объектов и вероятностей проявления угроз.

Полученные результаты можно использовать, как при оценке проектов, так и для контроля существующих КС. Анализ промежуточных значений поможет выявить слабые места и уязвимости в рассматриваемых корпоративных системах.

2. Действия по достижению целей атак

Для успешной реализации угрозы злоумышленник предпринимает конкретные действия, список которых не бесконечен. Можно разбить по группам известные активности в зависимости от их принадлежности к конкретным целям атак (таблица 2).

Таблица 2

Действия злоумышленника

	Серверы демили-таризо-ванной зоны	Серверы корпора-тивной сети	ЭВМ и серверы внутренней локальной сети	ЭВМ и серверы внешних подразделений корпорации	Соответствующие системы защиты (сокращения раскрыты в тексте)
Mailbombing	X			X	Антиспам
Атаки (D)DoS	X	X		X	МЭ
Подбор пароля	X	X	X	X	IDPS
Rootkits, дыры в ПО	X	X	X	X	Скан., IDPS
Инъекция(SQL,PHP)	X	X		X	Скан.
Вирусы, трояны, черви	X	X	X	X	Антивир., МЭ
Сетевая разведка	X	X		X	МЭ, IDPS
Man-in-the-Middle	X			X	Крипт.
Сниффинг пакетов	X	X	X	X	VPN, Крипт.
IP-спуфинг	X	X		X	Крипт.

Конечно, в общем случае стоило бы рассматривать всевозможные сочетания действий и целей, но надо учитывать реальные условия эксплуатации КС. Тем более, что, рассматривая только технические аспекты проблемы защищенности корпоративной системы, не стоит забывать об обязательных организационно-правовых режимах, установленных на объекте информатизации, в контролируемой зоне которого она функционирует.

Развитие инфраструктуры вычислительных сетей даёт много возможностей для автоматизированной обработки информации, ускоряет обмен документов и снижает долю рутинных операций в системе. Огромное количество достоинств делает корпоративную сеть с установленными программно-аппаратными системами автоматизации процессов незаменимой при выполнении повседневных задач и ведении бизнеса. Но неизбежно появляются информационные риски, снижение которых достигается установкой защитных комплексов. Вопрос о составе и стоимости необходимых программно-аппаратных систем защиты является основным при создании преград действиям злоумышленников. Это индивидуальная задача проектирования, решение которой выходит за пределы статьи.

3. Построение вероятностной сети Петри (ВСП) для анализа средств защиты КС

На рисунке 1 представлена типовая ВСП, которая строится для решения поставленной задачи. Естественно, что при анализе конкретных корпоративных систем, сеть будет меняться, а её параметры перерассчитываться.

Рассмотрим подробнее сеть Петри, изображенную на рисунке 1. Начальная позиция P0 отражает совокупность угроз вирусов, червей и троянских коней. Срабатывание одного из трех переходов (T0,T1,T2) определяет конкретный тип атаки. Позиция P6 с маркером отвечает за безопасное функционирование антивирусной системы. Если срабатывает переход T3, то маркер перемещается в P4, P5, что говорит о появлении новых эпидемий в сети, против которых антивирус может оказаться бессильным. В свою очередь, активация одного из переходов {T5, T6, T7} является следствием не удачной работы эвристического метода, а активация T8 – сигнатурного метода. При успешной реализации угрозы маркер перемещается в позицию P8.

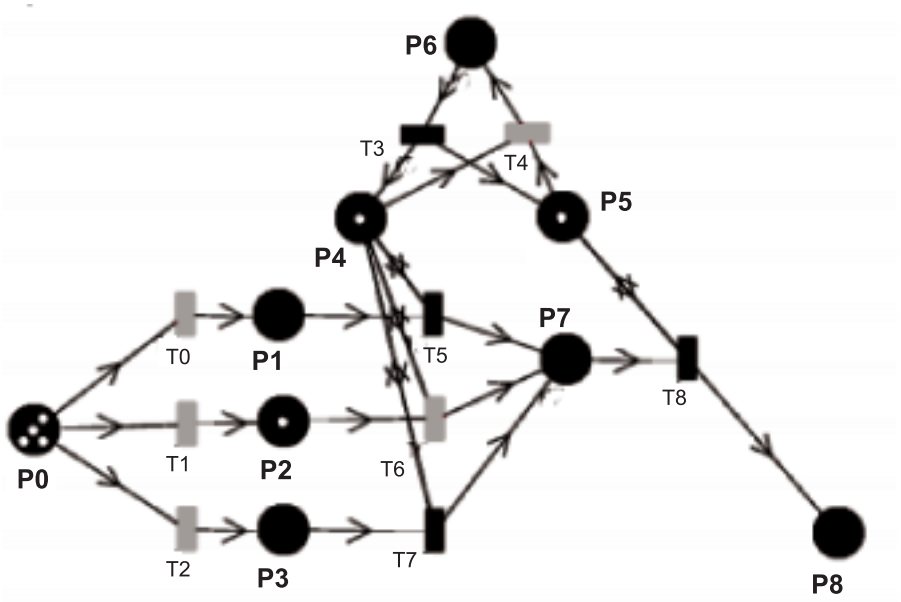

Рис. 1. Сеть Петри работы антивируса.

Аналогичными способами взаимодействия строятся сети Петри других систем защиты КС. Для получения вероятностной сети Петри необходимо заполнить матрицу P(r), которая связана с достижимыми разметками, изучаемой сети. Вероятности смены разметок определяются следующими значениями: P01(t0)=q01; P02(t1)=q02; P03(t2)=q03; P14(t3)=q14; P25(t3)=q25; P36(t3)=q36; P47(t5)=q47; P57(t6)=q57; P67(t7)=q67; P78(t4)=q78; P79(t8)=q79.

Параметры вероятностных сетей Петри межсетевого экрана и других средств защиты КС находятся аналогичным способом.

4. Решение задачи о нахождении вероятности реализации угрозы

На этом этапе предполагается, что смоделирована работа всех средств защиты и найдены вероятности смены разметок в соответствующих ВСП. Следующим шагом является вычисление вероятности успешной реализации атаки, т.е. возможности перехода сети Петри из начальной разметки в разметку, соответствующую успешной реализации угрозы.

Вернёмся к вероятностной сети Петри, изображенной на рисунке 1. Для ответа на поставленный вопрос необходимо вычислить вероятность перехода из начальной разметки M0 (∞,0,0,0,0,0,1,0,0) к разметке M'(x, x, x, x, x, x, x, x, 1), которая соответствует проникновению вирусной атаки в корпоративную систему.

Очевидно, что M' соответствует элементу M9 множества R(N). Начальное состояние M0 и состояние M9 соединяют несколько путей.

Так как переход от разметки M' к M'' не зависит от того, как появилась разметка M', а зависит лишь от данного состояния системы, то переходы от одной разметки к другой можно представить цепью Маркова, для которой вероятность перехода от состояния S_i к состоянию S_j есть произведение вероятностей перехода к промежуточным между S_i и S_j состояниям. Следует, что вероятность $\overline{P}\left(M_0 \xrightarrow{V} M\right)$ определяется формулой (1):

$$\overline{P}\left(M_0 \xrightarrow{V} M\right) = \prod_{j=1}^{k} P_{j-1}, j\left(r_j\right) \qquad (1)$$

Очевидно, величина $\overline{P}\left(M_0 \mapsto M\right)$ определяется по формуле (2):

$$\overline{P}\left(M_0 \xrightarrow{V} M\right) = \sum_{i=1}^{l} \overline{P}\left(M_0 \xrightarrow{Vi} M\right) \quad (2)$$

где l – число путей.

5. Определение уровня доверия к защищенной корпоративной системе

Вернёмся к таблице 1. Предполагается, что уже найдены все вероятности реализации угроз P_{ij}. Для определения степени критичности целей атак необходимо ввести понятие коэффициента важности объекта c_i. Перечислим конкретные значения коэффициентов некоторой корпоративной системы ($\sum c_i=1$):серверы демилитаризованной зоны – 0,25; серверы корпоративной сети – 0,35; ЭВМ пользователей и серверы внутренней локальной сети – 0,1; ЭВМ пользователей и серверы внешних подразделений корпорации – 0,3.

Для каждого объекта по формуле (3) вычислим среднее значение вероятности реализации угроз.

$$\overline{P}_i^{Cp} = \frac{\sum_{j=1}^{R_i} \overline{P_{ij}}}{R_i} \quad (3)$$

где Ri – общее количество реализуемых атак.

Далее определим уровень доверия к защищенной КС как сумму произведений соответствующих коэффициентов и средних значений вероятности успешной работы средств защиты:

$$Q = \sum_{i=1}^{4} x_i \times \left(1 - \overline{P_i^{Cp}}\right), Q \in [0;1]$$

Разработанный метод позволяет дать количественную оценку информационной безопасности корпоративной системы. Поэтапные действия, исходящие из логичного структурирования объектов, средств защиты и угроз КС, основываются на известных математических аппаратах сетей Петри, цепей Маркова и теории вероятностей.

Таким образом можно сделать следующие выводы:

1. Моделирование различных механизмов защиты от конкретных типов угроз является гибкой процедурой. Это говорит о том, что степень приближения модели к реальной системе зависит только от наличия соответствующей информации и требований менеджмента ИБ к детальности проводимого анализа.

2. Вычисление вероятности реализации выбранных типов угроз происходит по апробированным расчетам на основе математического аппарата вероятностных сетей Петри, являющего развитием теории конечных автоматов.

3. Определяемая общая вероятность нарушения безопасности объекта КС служит важным промежуточным показателем защищенности. Анализ этого значения важен при идентификации рисков, так как помогает оценить уровень угроз интересующего объекта, а не системы в целом.

4. Вывод уровня доверия к КС учитывает коэффициент важности защищаемых объектов, что говорит о его адекватности. Итоговый количественный показатель может использоваться при точном сравнении нескольких корпоративных систем, а также незаменим при выборе наилучших вариантов при проектировании комплексных систем безопасности.

6. Модель оценки защищенности корпоративной системы на основе вероятностных сетей Петри

Реализация угрозы в корпоративной информационной системе предполагает поэтапное использование уязвимостей системы защиты информации в данной корпоративной информационной системе. Причинами возникновения уязвимостей СЗИ могут быть различные факторы — это могут быть уязвимости аппаратного и программного обеспечения, некорректно настроенная политика безопасности, уязвимости физической или технической подсистем защиты информации и т.д. Использование какой-либо уязвимости СЗИ дает злоумышленнику новые возможности в корпоративной информационной системе, однако уровень этих возможностей различается в зависимости от

использованных уязвимостей. При этом не все уязвимости доступны злоумышленнику изначально. Часть из них может стать доступной для злоумышленника в процессе преодоления СЗИ как результат использования изначально доступных уязвимостей СЗИ.

Модель реализации угрозы, основывается на работе Арькова П.А. и описывает последовательное использование уязвимостей системы защиты информации, корпоративной системы и отображается в виде сети Петри, описанной кортежем представленным ниже:

$$N= (P1, T, I,W, M0)$$

где P1 – множество мест сети; T – множество переходов представляет собой фактически множество способов эксплуатации той или иной уязвимости; I – отношение между вершинами соответствующее дугам сети; W – функция задающая кратность дуги, W=1.

условии, что в дальнейшем он перейдет в j-ое состояние.

Анализ сети осуществляется моделированием. При моделировании до достижения одного из поглощающих состояний определяется среднее время, затрачиваемое на осуществление угрозы tyrp, и вероятность P осуществления злоумышленником угрозы при отсутствии ограничений времени.

Архитектура программного комплекса реализующего модель оценки защищенности КИС на основе вероятностных сетей Петри, состоит из четырех блоков (рис. 2).

Первый блок. Пользовательский интерфейс приложения. Пользователь формирует сеть Петри и вводит входные данные: наименование уязвимости, вероятность выбора данной уязвимости, вероятность успешной эксплуатации данной уязвимости, а также пользователь вводит параметры логнормального рас-

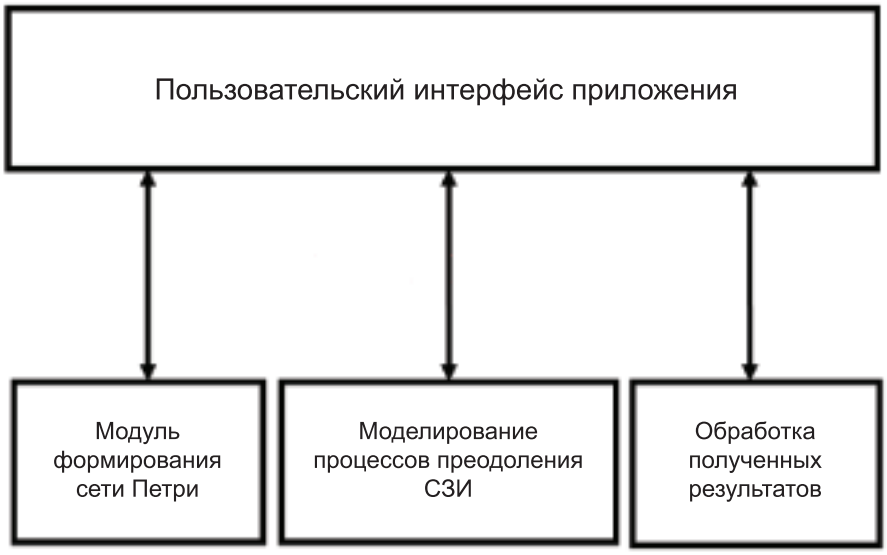

Рис. 2. Архитектура программного комплекса.

Для разрешения конфликтов используется предварительный выбор по вероятности срабатывания перехода, которая интерпретируется как вероятность выбора злоумышленником данного способа эксплуатации уязвимости. В модели время пребывания в состоянии интерпретируется как время необходимое злоумышленнику на эксплуатацию i-й уязвимости, при пределения для данной уязвимости и время моделирования.

Второй блок. Моделирование процессов преодоления СЗИ. Осуществляется заданное число экспериментов по преодолению СЗИ, в результате чего накапливается статистика успешных и безуспешных атак, а также времени преодоления СЗИ.

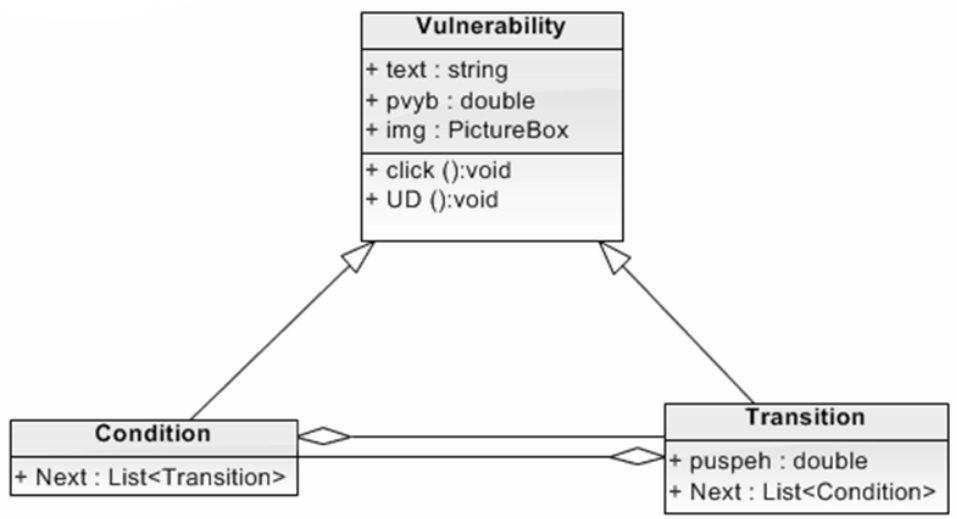

Рис. 3. Классы программного комплекса.

Третий блок. Обработка полученных результатов. Осуществляется обработка полученной статистики экспериментов, на основании которой вычисляется вероятность и среднее время преодоления СЗИ.

В программном комплексе реализованы три класса (см. рисунок 3): родительский класс «Vulnerability» (уязвимость), класс «Condition» (состояние), класс Transition (переход).

Класс «Vulnerability» содержит поля:

- text: string содержит текстовое описание узла сети;
- параметр pvyb: double вероятность выбор этого узла;
- img: PictureBox параметр для графического представления узла.

В классе присутствуют два основных метода click():void вызывается при нажатии на графическое представление узла, для выбора узла сети и второй метод UD():void вызывается при передвижении узла. В нем происходит пересчет координат центра верхней и нижней грани для отображения связей между узлами.

От класса «Vulnerability» (уязвимость) наследуются еще два класса «Condition» (состояние) и «Transition» (переход).

Класс «Condition» наследует все свойства и методы родительского класса «Vulnerability» и описывает дополнительные свойства характерные для состояния, это: Next: List<Transition> – список объектов класса «Transition» следующих за этим узлом.

Класс «Transition» так же наследует свойства и методы класса «Vulnerability» и имеет свои уникальные свойства, это puspeh: double – вероятность преодоления перехода и Next: List <Condition> – объекты класса «Condition» следующий за данным узлом сети.

На диаграмме показана связь между классами «Transition» и «Condition», от класса «Condition» к классу «Transition» идет ассоциация агрегация, так как к одному объекту класса «Condition» может идти несколько объектов класса Transition.

7. E-сеть

E-сеть является расширением сети Петри, которая позволяет реализовать множество параллельных информационных процессов. Математическая модель на базе E-сетей – это графическая модель в сочетании с логическими правилами изменения состояния (разрешающие позиции) E-сетей, позволяющими воспроизвести динамику функционирования информационной системы, представляет собой математическую модель имитационного типа.

Структурно Е-сеть – это граф, состоящий из двух типов вершин: позиций и переходов, соединенных друг с другом ориентированными дугами, причем каждая дуга может связывать лишь позицию с переходом или, наоборот, переход с позицией.

Заключение

Проведен анализ методов оценки и построения систем защиты информации на основе сетей Петри. Выявлены ограничения каждого из подходов и показаны возможные пути их применения в задачах анализа защищенности корпоративных систем.

Список литературы

1. “Математическое моделирование распределенных систем защиты информации”, Давыдова Е.Н. (Davidova_EN@mail.ru) http://swsys.ru/index.php?page=article&id=2764;
2. Сравнительный анализ моделей систем защиты информации. http://inf-bez.ru/?p=767;
3. Модель оценки защищенности корпоративной системы на основе вероятностных сетей Петри. http://inf-bez.ru/?p=769;
4. Специальные методы неформального моделирования основаны на применении неформальной теории систем.http://www.virustory.net/infosave42.html;
5. “Теория сетей Петри и моделирование систем” Питерсон Джеймс. http://www.kodges.ru/57650-teoriya-setej-petri-i-modelirovanie-sistem.html;
6. Актуальные проблемы безопасности информационных технологий: Сборник материалов II Международной научно-практической конференции 2008 года. http://window.edu.ru/library/pdf2txt/576/61576/31607;
7. «Анализ защищенности корпоративных систем», А.А. Астаханов, открытые системы №07-08 2002.