МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНИВАНИЮ ЭФФЕКТИВНОСТИ ЛОЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Язов Юрий Константинович, *доктор технических наук, профессор*
Сердечный Алексей Леонидович
Шаров Иван Александрович

В настоящее время при защите информационных систем актуальным становится применение «стратегии обмана» и отвлечения нарушителя на ложные ресурсы. Вместе с тем при использовании ложных информационных систем важно знать, насколько эффективно можно обмануть с ее помощью нарушителя при ограничении на потребление ресурсов. В данной статье предложен возможный методический подход к оцениванию эффективности ложных информационных систем и сделаны выводы о направлениях дальнейшего развития методического обеспечения оценивания их эффективности.

Ключевые слова: *ложная информационная система (ЛИС), уязвимость программного обеспечения, несанкционированный доступ (НСД), эффективность защиты*

METHODICAL APPROACH FOR ESTIMATION OF EFFICIENCY OF HONEYPOT SYSTEM

Yuri Yazov, *Doctor of Technical Sciences, Professor*
Alexey Serdechnyy
Ivan Sharov

Nowadays becomes very actual application of «deception strategies» and intruder distraction at false resources in aspect of information systems protecting. In addition to that it's important to know when using honeynets, how efficiently it could deceive the intruder with restriction of low resources consumption. In the current article possible method of evaluation of efficiency of honeypot systems is suggested and conclusion about line of further development of methodogical support of estimate of efficiency is made.

Keywords: *honeynet, software vulnerability, unauthorized access, effectiveness of protection*

При защите информационных систем (ИС) большое внимание уделяется вопросам обнаружения и нейтрализации уязвимостей входящего в их состав программного обеспечения (ПО). В настоящее время все основные способы решения данной задачи основываются на применении «стратегии запрета». Для этого в ручном или автоматизированном режиме проводится поиск уязвимостей ПО ИС, информация о которых имеется в открытых или закрытых базах данных. После обнаружения уязвимость нейтрализуется либо за счет обновления ПО, либо за счет использования средств защиты информации, таких как межсетевые экраны, системы обнаружения вторжений, средства антивирусной защиты и т.д., которые делают невозможным эксплуатацию данной уязвимости для реализации НСД.

Однако, как показывает практика, такая стратегия оказывается неэффективной против уязвимостей «нулевого дня». Это связано с тем, что между выпуском ПО и появлением информации об уязвимости, а тем более устранением ее разработчиками, в большинстве случаев проходит большое количество времени, в течение которого система оказывается уязвимой для НСД. Несмотря на то, что правильно настроенные средства защиты информации делают эксплуатацию некоторых из таких уязвимостей невозможной, всегда остается вероятность наличия не устраненных уязвимостей, а также уязвимостей в ПО самих средств защиты.

В связи с этим в настоящее время актуальным становится применение «стратегии обмана» или

отвлечения нарушителя на ложный информационный ресурс. Необходимость применения средств, реализующих такую стратегию и называемых ложными информационными системами (ЛИС), отмечается и в одном из последних утвержденных нормативных правовых актов «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [1]. Как показали исследования [2], реализуя с помощью ЛИС «стратегию обмана» нарушителя и отвлекая его на ложный информационный ресурс, можно не только не позволить злоумышленнику получить несанкционированный доступ (НСД) к защищаемой информации, но и найти неизвестные ранее уязвимости ПО.

Развитию практики применения ЛИС способствует все большее внедрение технологии виртуализации, появление программных средств виртуализации, таких как VMware ESX/ESXi, Microsoft Hyper-V, Citrix Xen Server и др., позволяющих создать виртуальную инфраструктуру и управлять ею.

Вместе с тем при использовании ЛИС важно знать, насколько эффективно можно обмануть с ее помощью нарушителя и при этом не создать сложностей для функционирования защищаемой ИС, поскольку значительный вычислительный ресурс может оказаться задействованным на обеспечение функционирование ЛИС. С учетом изложенного под эффективностью ЛИС здесь и далее понимается степень достижения цели отвлечения нарушителя от защищаемого информационного ресурса при условии, что ЛИС не влияет существенным образом на функционирование защищаемой ИС.

До настоящего времени методическое обеспечение оценивания эффективности ЛИС, в том числе построенных с использованием средств виртуализации, не разрабатывалось. При этом следует отметить, что в таких системах крайне важно учитывать ограничения на потребление вычислительных ресурсов, поскольку такие ограничения существенно влияют на количество эмулируемых ложных объектов, а, следовательно, и на эффективность защиты.

В данной статье предлагается возможный подход к такому оцениванию, основанный на вероятностной оценке возможности выполнения одновременно двух условий:

срыва НСД к защищаемой информации за счет использования ЛИС;

отсутствия превышения затрат вычислительных ресурсов информационной системы установленного (недопустимого) уровня.

Срыв НСД достигается за счет того, что нарушитель или инициированный им процесс доступа (например, с использованием вредоносной программы) переориентируется на ложные, созданные в виртуальной среде объекты - эмулируемые с помощью виртуальных машин (ВМ) компьютеры в составе компьютерной сети, подключенной к сети общего пользования.

Вероятность НСД ($P_D^{(I)}(t)$) при условии выполнения указанного ограничения на используемый вычислительный ресурс R в общем случае зависит от времени и может быть оценена следующим образом:

$$P_D^{(I)}(t) = \begin{cases} P_{(НСД)}(I,t), \text{если } R \le R_{lim}, \\ 0, \text{в противном случае}, \end{cases} \quad (1)$$

где $P_{(НСД)}(I,t)$ - вероятность того, что за время t нарушитель сумеет получить НСД к I объектам (компьютерам) в составе информационной системы;

R_{lim} - допустимый уровень затрат вычислительных ресурсов R информационной системы.

Эффективность ЛИС как средства защиты по аналогии с [3] рассчитывается с использованием разностного показателя:

$$\eta_{\Delta}(t) = P_D^{(I)}(t) - P_{D(ЛИС)}^{(I)}(t), \quad (2)$$

или относительно-разностного показателя:

$$\eta(t) = \frac{P_D^{(I)}(t) - P_{D(ЛИС)}^{(I)}(t)}{P_D^{(I)}(t)} = 1 - \frac{P_{D(ЛИС)}^{(I)}(t)}{P_D^{(I)}(t)}, P_{D(ЛИС)}^{(I)}(t) > 0, \quad (3)$$

где $P_D^{(I)}(t)$ - вероятность того, что в условиях отсутствия ЛИС за время t нарушитель сумеет получить НСД к I объектам (компьютерам) в составе ИС;

$P_{D(ЛИС)}^{(I)}(t)$ - вероятность того, что в условиях функционирования ЛИС за время t нарушитель сумеет получить НСД к I объектам (компьютерам) в составе ИС.

Следует отметить, что если вероятность НСД в условиях отсутствия ЛИС близка к единице, то значения показателей эффективности совпадают и определяются только значением вероятности $P_{D(ЛИС)}^{(I)}(t)$:

$$\eta(t) = 1 - P_{D(ЛИС)}^{(I)}(t). \quad (4)$$

Рассмотрим подход к оценке этой вероятности. При реализации НСД нарушитель или вре-

доносная программа осуществляет случайный поиск компьютера, являющегося целью атаки, и распознавание его с отнесением к целевому объекту (то есть к компьютеру с защищаемой информацией). При этом поиск может начинаться с любого элемента информационной системы, имеющей IP-адрес или с ложного элемента в составе ЛИС, формируемого ВМ. Пусть в составе информационной системы имеется N_{Tr} истинных объектов, ЛИС формирует N_F ложных объектов, а для анализа каждого объекта на предмет отнесения его к целевому тратится в среднем время $\bar{\tau}_a$. Тогда за время t нарушитель сможет реализовать k шагов, на каждом из которых будут анализироваться попавшиеся ему истинные или ложные объекты:

$$k = \left[\frac{t}{\bar{\tau}_a}\right], \quad (5)$$

где знак $[\,]$ означает выделение целой части дроби.

Вероятность того, что нарушитель за k шагов сумеет получить доступ к i целевым объектам в условиях применения ЛИС, а также примерно равной исходной вероятности доступа к объектам $P_{НСД}$ на каждом шаге, определяется следующим образом:

$$P^{(i)}_{D(ЛИС)}(k) = P^{i}_{НСД} \cdot \prod_{j=0}^{i-1} \frac{N_{Tr} - j}{N_{Tr} + N_F - j} \cdot \cdot \left(1 + \sum_{m=1}^{k-i} C^{m}_{i+m-1} \prod_{j=1}^{m} \frac{N_F - j + 1}{N_{Tr} + N_F - j - i + 1}\right), \quad (6)$$

где C^{m}_{i+m-1} – количество сочетаний из $i + m - 1$ по m.

Кроме того, учитывая (1), при расчете показателя эффективности ЛИС необходимо оценивать ограничение на потребление ЛИС вычислительных ресурсов защищаемой информационной системы. К вычислительным ресурсам в данном случае относятся [4]: объём свободной оперативной памяти, необходимой для работы истинных виртуальных машин *для каждого* сервера виртуализации[1]; резерв свободного процессорного времени, необходимый для надёжной работы *каждого* сервера виртуализации; доля зарезервированного объема трафика, который может передаваться в информационной системе. Ни один из указанных ресурсов не должен превысить допустимый уровень (как правило, резерв свободного процессорного времени должен быть не менее 25%, а доля зарезервированного объема трафика – 50%).

Рассмотрим пример, когда нарушитель осуществляет выбор целевого объекта, в информационной системе, состоящей из 15 объектов, среди которых серверы виртуализации, рабочие станции пользователей, файловые серверы, ложные ВМ и т.п. ($N_{Tr} = 15$). Из них 5 объектов являются ложными ($N_F = 5$), а 3 – целевыми. Анализ объектов осуществляется методом сканирования сетевыми пакетами, в ходе которого определяется тип операционной системы объекта и состав сетевых служб. Продолжительность такого сканирования составляет 30 секунд ($\bar{\tau}_a = 30$), таким образом, для того, чтобы проанализировать все 15 объектов нарушитель должен затратить 7,5 секунд. Предположим, что $P_{НСД} = 0,8$,. Кроме того, в информационной системе работает система предотвращения вторжений, позволяющая в течении 2 секунд выявить и нейтрализовать действия нарушителя ($t = 120, k = 4$).

В информационной системе присутствует два одинаковых сервера виртуализации со следующими характеристиками: 32 ГБ оперативной памяти, пропускная способность канала связи – 1 ГБ/сек, 4 ТБ памяти на жестком диске, процессор – Intel Xeon E7. Расход вычислительных ресурсов сервера виртуализации на работу ВМ (как целевых, так и ложных) представлен в таблице 1.

[1] Сервер виртуализации представляет собой высокопроизводительный компьютер с установленным гипервизором первого типа, обеспечивающий работу виртуальных машин

***Таблица 1** – Расход вычислительных ресурсов сервера виртуализации*

Объект	Процессорное время	Загруженность канала связи	Оперативная память	Память на жестком диске
Целевая ВМ	0,7%	0,001%	2 ГБ	42 ГБ
Ложная ВМ	0,75%	0,00005%	512 МБ	21 ГБ
Гипервизор	0,5%	0,0005%	256 МБ	0,5 ГБ

Условие $R \le R_{lim}$ выполняется, когда на каждом сервере виртуализации свободно не менее 8 ГБ оперативной памяти, на жестком диске – не менее 40 ГБ, канал связи загружен не более чем на 50%, а процессор – на 75%. Данное условие верно, если количество ложных ВМ на одном сервере виртуализации не превышает 15 (количество ложных ВМ в данном случае ограничено дефицитом свободной оперативной памяти). С учётом приведенных данных эффективность ЛИС рассчитывается следующим образом:

$$\eta = 1 - \left(0{,}729 \cdot \prod_{j=0}^{2} \frac{15-j}{20-j} \cdot \left(1 + C_3^3 \prod_{j=1}^{1} \frac{6-j}{11-j}\right)\right) = 0{,}271. \quad (7)$$

На рисунках 1 – 4 показаны зависимости вероятности доступа к целевым объектам от количества ложных объектов, исходной вероятности доступа, определяемой в условиях отсутствия ЛИС, количества целевых объектов в защищаемой ИС и времени.

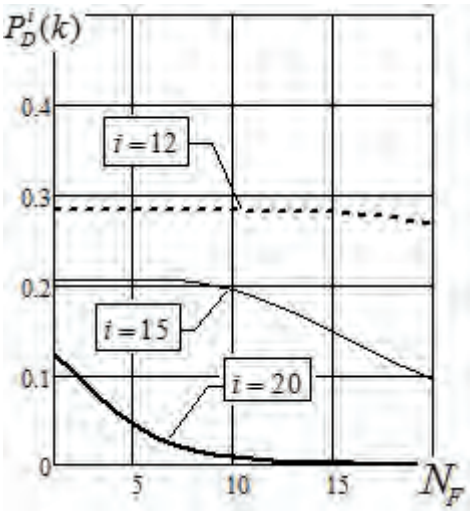

Рис. 1. *Зависимость вероятности несанкционированного доступа за 20 шагов к целевым объектам от количества эмулируемых ложных объектов при исходной вероятности доступа, равной 0.9, и количестве истинных объектов - 50*

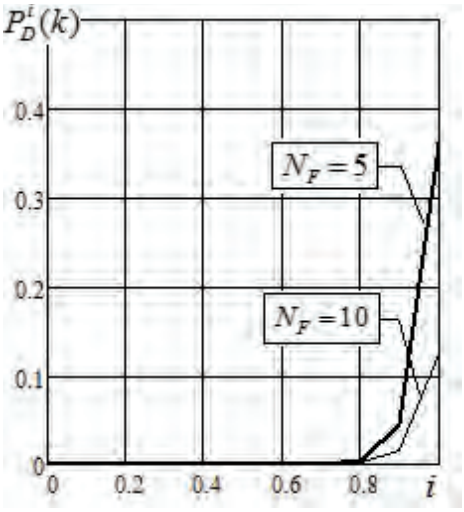

Рис. 2. *Зависимость вероятности несанкционированного доступа к 20 целевым объектам от исходной вероятности доступа к ним в отсутствии ЛИС при исходной вероятности доступа, равной 0.9, если информационная система состоит из 50 истинных объектов*

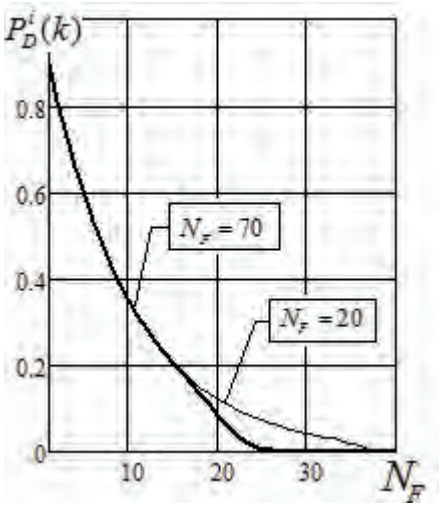

Рис. 3. *Зависимость вероятности несанкционированного доступа за 20 шагов к целевым объектам от количества эмулируемых ложных объектов при исходной вероятности доступа, равной 0.9, и количестве истинных объектов - 50*

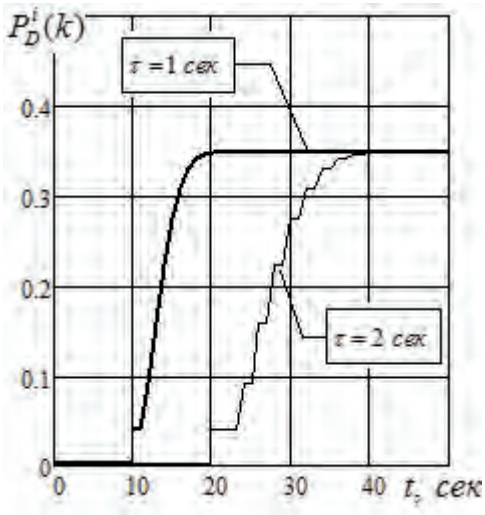

Рис. 4. *Зависимость вероятности несанкционированного доступа к 10 целевым объектам от времени при исходной вероятности доступа, равной 0.9 и 20 ложных объектов, если информационная система состоит из 50 истинных объектов*

Анализ полученных результатов показал, что после достижения определенного количества эмулируемых ложных объектов рост эффективности ЛИС становится несущественным. Это позволяет выбирать целесообразное количество эмулируемых ложных объектов в зависимости от заданных условий.

Однако полученные соотношения и зависимости позволяют оценивать эффективность ЛИС и влияние на нее существенных параметров и характеристик таких средств защиты при условии, что ложные объекты, эмулируемые ЛИС, абсолютно идентичны истинным (целевым) объектам. Если это условие не выполняется, то необходимо оценивать вероятность распознавания ложных объектов и дискредитации таким образом самой ЛИС.

Кроме того, изложенный подход к оценке эффективности ЛИС правомерен в основном для статических ЛИС, состав и параметры которых не меняются в процессе защиты. В реальных ИС состав функционирующих объектов постоянно меняется: часть компьютеров включается или выключается, создаются новые или закрываются действующие виртуальные каналы взаимодействия, изменяется состав программного обеспечения в сети, наконец, изменяется состав защищаемых информационных ресурсов. В этих условиях возникают демаскирующие признаки, по которым нарушитель может распознать наличие ложных объектов и это должно учитываться при оценке эффективности ЛИС.

Все это обусловливает необходимость создания специализированного методического обеспечения оценивания эффективности ЛИС, учитывающего как возможности распознавания ложных и истинных объектов, так и динамику функционирования самой защищаемой ИС и динамических ЛИС, меняющих свой состав и характеристики по аналогии с реальными ИС. Такое обеспечение должно базироваться не только на аналитических методах оценки, но и включать в себя имитационные модели, позволяющие верифицировать аналитические алгоритмы, обосновывать состав демаскирующих признаков ложных объектов, создаваемых в виртуальной среде, и истинных объектов в составе ИС, определять допустимый уровень затрат вычислительных ресурсов ИС на функционирование ЛИС, определять временные характеристики доступа нарушителя или инициируемого им процесса как к целевым, так и к ложным объектам и т.д.

С учетом изложенного на рисунке 5 показаны состав и структура первоочередного методического обеспечения, которое, на наш взгляд, необ-

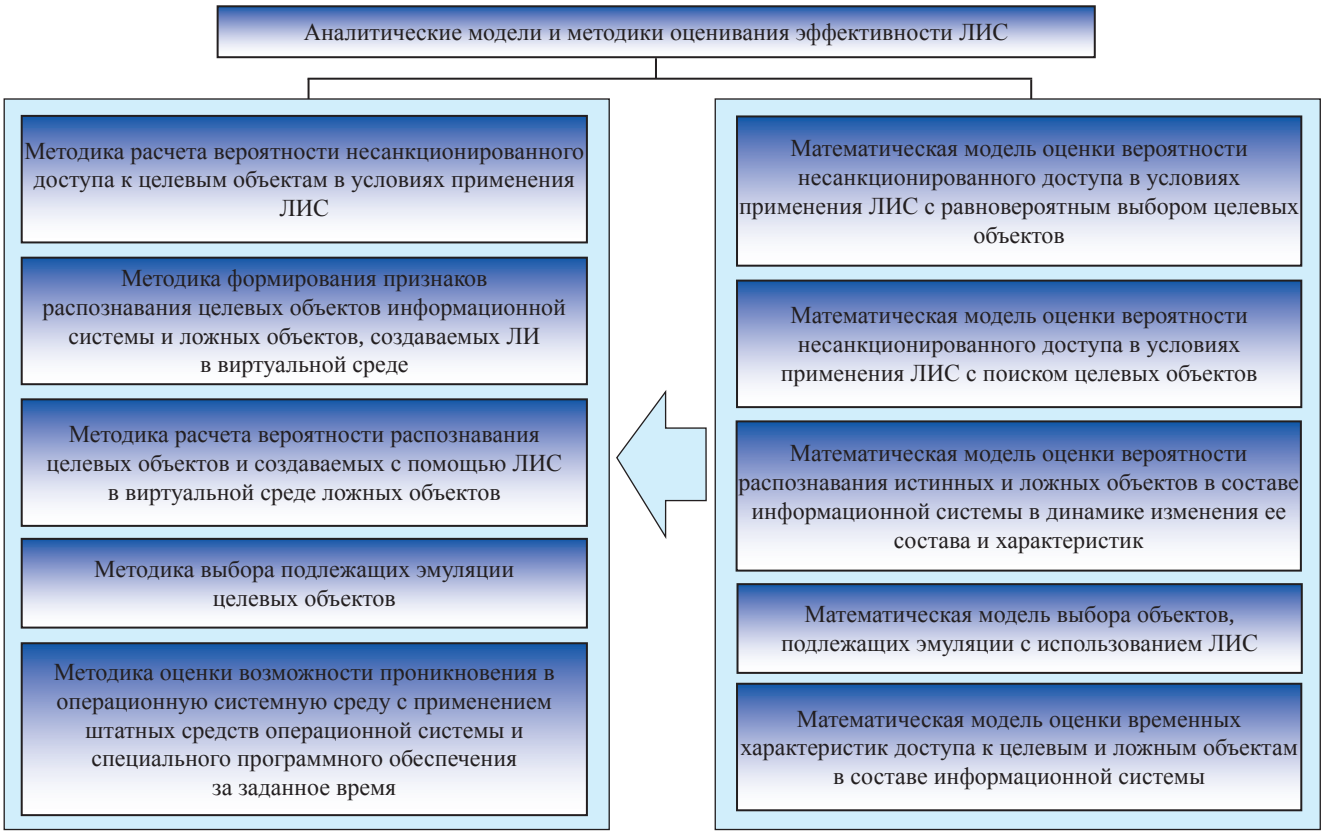

***Рис. 5.** – Состав и структура методического обеспечения оценивания эффективности ложных информационных систем*

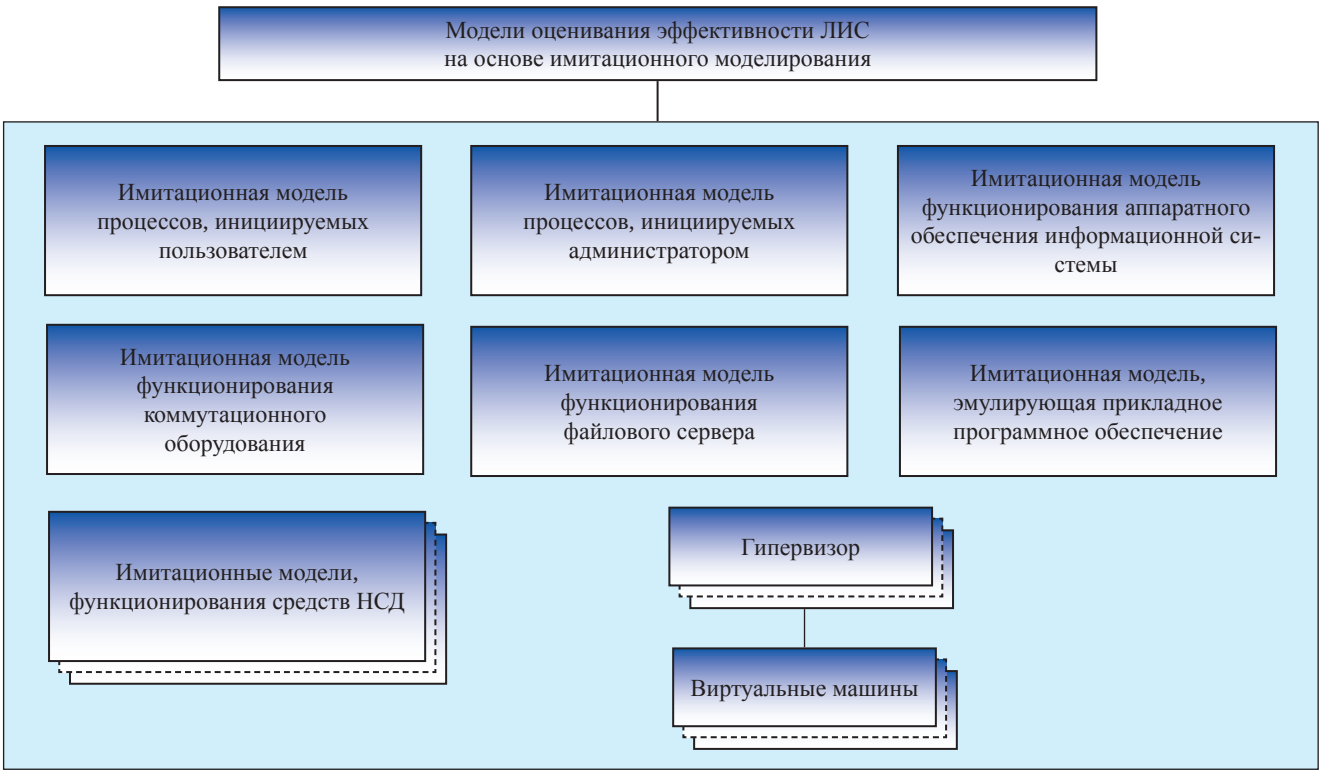

Рис. 5. *– Состав и структура методического обеспечения оценивания эффективности ложных информационных систем*

ходимо разработать в интересах решения задачи оценивания эффективности ЛИС.

Разработанный методический подход к оцениванию эффективности ЛИС направлен на развитие методического обеспечения, которое позволило бы перейти от качественных к количественным процедурам оценивания, что существенно повысит обоснованность характеристик и путей построения ЛИС как перспективных средств защиты информации.

Литература

1. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11.02.2013 № 17 г. Москва.
2. Сердечный, А.Л. Инновационный подход к защите информации в виртуальных вычислительных сетях, основанный на стратегии обмана / А.Л. Сердечный // Информация и безопасность. – 2013. – №3. – 399-403 с.
3. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах – Ростов-на-Дону: СКНЦ ВШ, 2006. – 274 с.
4. Михеев, М.О. Администрирование VMware vSphere 5 // М.:ДМК Пресс, 2012.

References

1. Requirements about protection of the information which are doing not make the state secret, containing in the government information systems. Are confirmed by order FSTEC Russia from 11.02.2013 № 17, Moscow.
2. Serdechnyy A.L., 2013. The innovative approach to information protection in the virtual computer networks, based on deceit strategy // Information and Security 3, 399-403.
3. Yazov Y.K., 2006. Bases methodology of a quantitative estimation effectiveness of information protection in computer systems // Rostov on Don: SKNTS VSH.
4. Miheev, M.O., 2012. VMware vSphere 5 administration // M.:DMK Press.