Коноваленко Сергей Александрович, Королев Игорь Дмитриевич

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПОСРЕДСТВОМ КОМБИНИРОВАННОГО МЕТОДА АНАЛИЗА ПАРАМЕТРИЧЕСКИХ ДАННЫХ, ОПРЕДЕЛЯЕМЫХ СИСТЕМАМИ МОНИТОРИНГА ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

В статье проведено сравнение сигнатурного и поведенческого методов анализа параметрических данных, определяемых системами мониторинга вычислительных сетей. Построена обобщенная модель комбинированного метода анализа параметрических данных на основе технологий интеллектуального анализа данных, позволяющая повысить эффективность работы специалиста по выявлению уязвимостей контролируемых информационных систем.

Адрес статьи: www.gramota.net/materials/1/2016/11/16.html

Источник

Альманах современной науки и образования

Тамбов: Грамота, 2016. № 11 (113). С. 60-66. ISSN 1993-5552.

Адрес журнала: www.gramota.net/editions/1.html

Содержание данного номера журнала: www.gramota.net/materials/1/2016/11/

8. **Конгар Н. М.** Современное состояние сельского хозяйства Тувы // Ученые записки ТНИИЯЛИ. Кызыл: ТНИИЯЛИ, 1975. Вып. 17. С. 71-77.
9. **Народное хозяйство Тувинской АССР в девятой пятилетке**: статистический сборник. Кызыл: Тувинское книжное издательство, 1976. 240 с.
10. **Народное хозяйство Тувинской АССР в десятой пятилетке**: статистический сборник. Кызыл: Тувинское книжное издательство, 1981. 215 с.
11. **Осипова В. В.** Колхозное строительство в Туве // Ученые записки ТНИИЯЛИ. Кызыл: ТНИИЯЛИ, 1957. Вып. 5. С. 113-118.
12. **Осипова В. В.** Сельскохозяйственная и демографическая перепись 1931 г. как важнейший источник характеристики экономического строя сельского хозяйства Тувы (1921-1930 гг.) // Ученые записки ТНИИЯЛИ. Кызыл: ТНИИЯЛИ, 1961. Вып. 9. С. 99-124.
13. **Республика Тыва. 60 лет**: юбилейный статистический сборник / под ред. С. Н. Ламоченко. Кызыл, 2004. 86 с.
14. **Самарина Н. Г.** Состояние животноводства на территории Тувинской АССР в 1970 – начале 1980-х гг. // Сборник научных трудов Тывинского государственного университета. Кызыл: РИО ТывГУ, 2008. Вып. 6. Т. 1. С. 17-19.
15. **Солдатов В. П.** К вопросу о размещении и специализации сельского хозяйства в Туве // Ученые записки ТНИИЯЛИ: 20 лет Советской Тувы. Кызыл: ТНИИЯЛИ, 1964. Вып. 11. С. 164-178.
16. **Солдатов В. П.** Тувинская АССР в системе сельского хозяйства Восточной Сибири // Ученые записки ТНИИЯЛИ. Кызыл: ТНИИЯЛИ, 1963. Вып. 10. С. 87-115.
17. **Сычев Н. В.** Рациональное использование земель – важный резерв дальнейшего подъема сельского хозяйства в Туве // Ученые записки ТНИИЯЛИ. Кызыл: ТНИИЯЛИ, 1961. Вып. 9. С. 57-61.
18. **Томилин И. Е.** Некоторые итоги развития народного хозяйства области за 1960 г. и задачи дальнейшего развития экономики области // Ученые записки ТНИИЯЛИ. Кызыл: ТНИИЯЛИ, 1961. Вып. 9. С. 41-48.
19. **Томилин И. Е.** Некоторые итоги четырех лет семилетки и перспективы дальнейшего развития народного хозяйства Тувинской АССР // Ученые записки ТНИИЯЛИ. Кызыл: ТНИИЯЛИ, 1963. Вып. 10. С. 58-67.
20. **Тульчинский Л. И.** Социально-экономический анализ материалов переписи населения Тувы 1959 г. // Ученые записки ТНИИЯЛИ: 20 лет Советской Тувы. Кызыл: ТНИИЯЛИ, 1964. Вып. 11. С. 205-222.
21. **Филимонов В. П.** Агроклиматические особенности Тувинской АССР // Труды Тувинской государственной сельскохозяйственной опытной станции. Кызыл: Тувинское книжное издательство, 1969. Вып. 4. С. 7-36.

DEVELOPMENT OF TUVA AGRICULTURE IN THE SOVIET PERIOD

Kozlova Ekaterina Andreevna
Khakas State University named after Nikolai F. Katanov
Katya.120394@yandex.ru

The article considers preconditions and peculiarities of Tuva agriculture development in the Soviet period – 1944-1991. Decisions of the party to raise agriculture that were made in the 1920-1930s are specified as the prerequisites. The severe natural and weather-climatic conditions, preservation of the traditional sectors of economy, the role of Soviet agrarian policy are named among the peculiarities.

Key words and phrases: The Tuvan People's Republic; The Tuvan Autonomous Oblast; The Tuvan Autonomous Soviet Socialist Republic; Tuva; crop farming; agriculture; stock-breeding; traditional farming; crop area; livestock.

УДК 004.048
Технические науки

В статье проведено сравнение сигнатурного и поведенческого методов анализа параметрических данных, определяемых системами мониторинга вычислительных сетей. Построена обобщенная модель комбинированного метода анализа параметрических данных на основе технологий интеллектуального анализа данных, позволяющая повысить эффективность работы специалиста по выявлению уязвимостей контролируемых информационных систем.

Ключевые слова и фразы: комбинированный метод анализа данных; поведенческий метод анализа данных; сигнатурный метод анализа данных; системы мониторинга; технологии интеллектуального анализа данных.

Коноваленко Сергей Александрович
Королев Игорь Дмитриевич, д.т.н., профессор
Краснодарское высшее военное училище
konovalenko_rcf@mail.ru; pi_korolev@mail.ru

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПОСРЕДСТВОМ КОМБИНИРОВАННОГО МЕТОДА АНАЛИЗА ПАРАМЕТРИЧЕСКИХ ДАННЫХ, ОПРЕДЕЛЯЕМЫХ СИСТЕМАМИ МОНИТОРИНГА ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

В целях возможной реализации синтеза различных специальных средств [9], осуществляющих выявление уязвимостей контролируемых информационных систем (далее по тексту – КИС), направленного на повышение эффективности оценки защищенности контролируемой вычислительной сети в целом (далее по тексту – КВС), необходимо рассмотреть перечень параметрических данных (далее по тексту – ПД), определяемых системами мониторинга (далее по тексту – СМ), значения которых формируют реальный образ КИС (далее по тексту – ОКИС).

Работа [10] показала, что существующим СМ присущ как общий, так и специфический набор базовых функциональных возможностей, в связи с чем СМ КИС способны осуществлять сбор и обработку большого количества однотипных и специфических ПД, которые сводятся в Табл. 1.

Таблица 1.

Основные ПД, определяемые СМ КИС

№ п/п	Параметрические данные	СМ КИС		
		Zabbix	***Cacti***	***Nagios***
1.	IP-адреса, MAC-адреса, DNS-имена КИС	+	+	+
2.	Информация о количестве наблюдаемых КИС	+	+	+
3.	Информация о доступности и работоспособности КИС и сервисов, о времени их отклика	+	+	+
4.	Различная информация о сетевых портах (TCP/UDP) КИС, например: - доступность TCP/UDP портов; - состояние сервисов и принимают ли они TCP/UDP подключения; - производительность TCP/UDP сервисов и т.д.	+	+	+
5.	Информация о состоянии аппаратного обеспечения КИС (например, параметры температуры, напряжения, частота вращения вентиляторов, состояние питания КИС и т.д.)	+	+	+
6.	Идентификационная информация об операционной системе и программном обеспечении, установленном на КИС	+	+	+
7.	Информация об обновлениях на КИС	+	+	+
8.	Информация о системном времени на КИС	+	+	+
9.	Инвентаризационная информация о КИС, например: - информация о шасси (модель, серия, тип, поставщик); - информация о PCI (например, видеокарта, сетевая карта, звуковая карта, TV-тюнер и т.п.) или USB устройствах, подключаемых к КИС и т.д.	+	-	+
10.	Информация о специализированных агентах, установленных на КИС (например, действительное значение (host name) агента из файла конфигурации; его версия и т.п.)	+	-	+
11.	Информация о жестких или сменных дисках, установленных на КИС, например: - размер свободного или использованного пространства; - суммарное количество данных, переданных (чтением или записью) на диск (байт в секунду); - количество передач за секунду, которые произошли на физическом диске; - размер использования дисков, подключенных по протоколу SMB (обычно это диски от Windows-систем); - состояние локального диска (в Linux-системах) по технологии SMART и т.д.	+	+	+
12.	Информация о состоянии аппаратных датчиков КИС	+	+	+
13.	Информация о состоянии виртуальной и физической памяти (общий, свободный или задействованный объем)	+	+	+
14.	Информация о необходимом файле (папке) по конкретному критерию (например, размер, дата создания, время последнего доступа или внесений изменений, содержимое файла и т.п.)	+	+	+
...	...	...	...	...
n	Информация о доступности и содержимом (в том числе информация о конкретной строке) web-ресурсов.	+	+	+

Соответственно, СМ КИС не ограничиваются только сбором ПД, указанных в Табл. 1. Стоит отметить, что перечень ПД, подлежащих сбору и анализу, практически во всех СМ подвержен постоянному расширению посредством применения плагинов и скриптов [Там же]. Логичным будет вывод, который свидетельствует о корреляционной зависимости между количеством собираемых значений ПД и эффективностью работы специалиста по выявлению уязвимостей КИС. Однако существует и отрицательная сторона, которая связана со сложностью представления и анализа большого количества входных ПД, обрабатываемых посредством функционирования модуля анализа собранных значений ПД, в котором реализуются различные методы [9]:

- сигнатурные методы анализа ПД;
- поведенческие методы анализа ПД;
- комбинированные методы анализа ПД.

Сигнатурные методы анализа ПД заключаются в сопоставлении (сравнении) собранных значений ПД (S_n^{ex}) с сигнатурами (образами) известных уязвимостей ($S_{уяз}$), присущих КИС (например, строки символов, семантические выражения на специальном языке, формальные математические модели и т.д.), хранящимися в базе данных (далее по тексту – БД) [15].

Поведенческие методы анализа ПД заключаются в обнаружении несоответствий между текущим режимом функционирования КИС ($F_n^{тек}$) и режимом его штатной работы ($F_{штат}$) [Там же].

В работах [2; 4; 5; 8; 11; 12; 14-16; 18; 19] рассматриваются различные способы выявления уязвимостей КИС, вследствие чего проведем сравнительный анализ двух вышеуказанных методов (Табл. 2).

Таблица 2.

Сравнительный анализ сигнатурных и поведенческих методов анализа ПД

Используемые методы	Преимущества	Недостатки
Сигнатурные методы анализа		
Общие особенности	1. Высокая точность и оперативность выявления образов известных уязвимостей КИС. 2. Низкая вероятность возникновения ложных срабатываний. 3. Средние требования к аппаратно-программному обеспечению специального средства, на котором реализуется данный метод анализа.	1. Неспособность выявления образов неизвестных (модифицированных известных) уязвимостей КИС, сигнатуры которых отсутствуют в БД. 2. Необходимость в постоянном (систематическом) обновлении сигнатур (образов) уязвимостей КИС, хранящихся в БД. 3. Ориентированность в большей степени на анализ локально-стационарных процессов, протекающих в КИС.
Метод контекстного поиска	1. Простота синтаксиса регулярных выражений, используемых для поиска конкретных данных в потоке собранных значений ПД. 2. Поддержка различных языков программирования, используемых для поиска дополнительных сигнатур, что свидетельствует о способности метода анализа к расширению.	1. Необходимость в ручном написании дополнительных регулярных выражений или описании параметров поиска посредством различных языков программирования. 2. Использование текстовых моделей представления метода анализа. 3. Низкий уровень адаптации к внешним факторам.
Метод анализа состояний КИС на основе теории графов или временных сетей Петри	1. Использование графических моделей представления метода анализа. 2. Способность к прогнозированию. 3. Способность выявления корреляционно зависимых состояний КИС. 4. Склонность метода к масштабируемости, связанной с сохранением эффективности его реализации при увеличении количества собираемых значений ПД.	1. Выявление только явно выраженных признаков изменения состояний КИС. 2. Зависимость метода анализа от множества изменений состояний КИС.
Метод экспертных систем	1. Логичность и понятность принятых решений по выявленным уязвимостям КИС. 2. Простота реализации метода анализа.	1. Необходимость в описании характерных признаков уязвимостей КИС и точно сформулированных правил. 2. Снижение эффективности реализации метода анализа с увеличением объема входных значений ПД (низкий уровень адаптации к внешним факторам), что влечет за собой увеличение количества правил. 3. Отсутствие способности к обучению. 4. Высокая степень зависимости метода от квалификации специалиста, занимающегося формированием базы знаний и правил экспертной системы.
Поведенческие методы анализа		
Общие особенности	1. Способность к выявлению образов известных и неизвестных уязвимостей КИС. 2. Способность к анализу динамических процессов, протекающих в КИС.	1. Высокий уровень вероятности возникновения ложных срабатываний или пропусков в выявлении уязвимостей КИС. 2. Необходимость в точном описании штатного режима функционирования каждой КИС. 3. Повышенные требования к аппаратно-программному обеспечению специального средства, на котором реализуется данный метод анализа.
Статистический метод	1. Использование графических и текстовых моделей представления метода анализа. 2. Логичность и понятность принятых решений по выявленным уязвимостям КИС. 3. Анализ собранных значений ПД осуществляется в зависимости от временных показателей. 4. Способность к прогнозированию. 5. Способность выявления корреляционных зависимостей между собранными значениями ПД. 6. Высокий уровень адаптации к внешним факторам. 7. Способность на основе собранных значений ПД вычислять новые значения ПД (например, средние значения).	1. Зависимость от правильно проведенной статистической выборки ПД, значения которых подлежат анализу, а также от корректного определения минимальных и максимальных пороговых значений ПД. 2. Выполнение значительных математических вычислений, что отрицательно воздействует на выявление уязвимостей КИС в режиме реального времени. 3. Усреднение входных значений ПД, приводящее к возможной потери информативности данных.

Используемые методы	Преимущества	Недостатки
Метод, основанный на кластерном анализе	1. Высокий уровень адаптации к внешним факторам. 2. Способность отнесения входящих значений ПД к кластерам, не обладающим заранее определенными признаками. 3. Способность к параллельной обработке большого объема собранных значений ПД.	1. Сложность в понимании специалистом процедур анализа. 2. Сравнительно длительные временные затраты на реализацию метода анализа.
Методы, используемые в сигнатурном и поведенческом анализе		
Метод, основанный на применении искусственных нейронных сетей	1. Использование графических моделей представления метода анализа. 2. Способность к обучению. 3. Отсутствие необходимости в формализованном описании уязвимостей КИС. 4. Способность к классификации и кластеризации собранных значений ПД по различным признакам. 5. Способность к выявлению корреляционных зависимостей между собранными значениями ПД. 6. Высокий уровень адаптации к внешним факторам. 7. Способность к параллельной обработке большого объема собранных значений ПД. 8. Способность к обработке нечетких входных значений ПД. 9. Способность к прогнозированию. 10. Сравнительно высокий уровень оперативности реализации метода анализа.	1. Зависимость эффективности реализации метода анализа от емкости и сложности искусственной нейронной сети. 2. Метод реализуется без объяснения процесса и логики принятия решений о выявленных уязвимостях КИС. 3. Сложность в обучении нейронной сети, связанная с необходимостью наличия большого количества обучающих ПД и с определенными временными затратами. 4. Способность обработки только численных значений ПД (при обработке других типов значений ПД требуется их преобразование путем численного кодирования), а в случае если большое количество ПД принимает нечисленные значения, то нейронные сети не применимы. 5. Искусственные нейронные сети подвержены проблеме *overfitting* (переобучения).
Метод, основанный на генетических алгоритмах	1. Высокий уровень адаптации к внешним факторам. 2. Способность к эффективному отбору и синтезу наиболее важных входных значений ПД, на основании анализа которых принимается решение о впервые выявленных уязвимостях КИС. 3. Способность к совершенствованию алгоритма выявления уязвимостей КИС на основе механизма естественного отбора наилучших решений, полученных в процессе непрерывного анализа наиболее важных собираемых значений ПД. 4. Способность к параллельной обработке большого объема собранных значений ПД.	1. Сложность процедур настройки генетических алгоритмов. 2. Сравнительно длительные временные затраты на реализацию метода анализа.
Байесовские сети и метод	1. Использование графических моделей представления метода анализа. 2. Эффективное представление вероятностных зависимостей (или отсутствия таковых) между разнородными значениями ПД. 3. Генерирование вероятностных выводов о выявлении уязвимостей КИС на основе результатов анализа разнородных значений ПД. 4. Способность к классификации собранных значений ПД на основе вероятностных предположений (стохастических принципов). 5. Способность к обучению. Байесовские сети не подвержены проблеме *overfitting* (переобучения). 6. Способность к прогнозированию. 7. Логичность принятых решений по выявленным уязвимостям КИС. 8. Способность к параллельной обработке большого объема собранных значений ПД. 9. Сравнительно высокая оперативность реализации метода анализа.	1. Сложность в определении набора ПД, на основе значений которых осуществляется обучение Байесовской сети. 2. Зависимость метода от используемого алгоритма опроса КИС. 3. Неспособность к анализу непрерывных входящих значений ПД, вследствие чего необходимо их разбиение на множества интервалов. 4. При классификации входных значений ПД не учитывается влияние их возможных сочетаний (комбинаций).
Метод, основанный на применении алгоритмов нечеткой логики	1. Описание правил в незавершенном (абстрактном) виде, что позволяет принимать решения (эвристические) о вероятности возникновения уязвимостей КИС. 2. Способность обработки нечетких входных значений ПД. 3. Гибкость в процессах классификации (кластеризации) разнородных значений ПД. 4. Эффективное упрощение процедур выявления уязвимостей КИС. 5. При реализации метода эффективно учитываются особенности каждой КИС. 6. Сравнительно высокая оперативность реализации метода анализа.	1. Зависимость метода от работы специалиста по правильному формированию исходных нечетких правил для каждой КИС. 2. Нечеткость (в отдельных случаях слабая математическая обоснованность) в принятии решений по выявленным уязвимостям КИС. 3. Сравнительно низкая точность в выявлении уязвимостей КИС.

Используемые методы	Преимущества	Недостатки
Метод, основанный на построении деревьев решений	1. Логичность и понятность принятых решений по выявленным уязвимостям КИС. 2. Использование графических моделей представления метода анализа. 3. Способность к прогнозированию. 4. Способность к классификации собранных значений ПД. 5. Способность к обработке различных типов входных значений ПД (численных и атрибутивных). 6. Способность к обучению. 7. Сравнительно высокая оперативность реализации метода анализа.	1. Снижение эффективности реализации метода при анализе входных значений ПД, которые неявно свидетельствуют об уязвимостях КИС. 2. Снижение эффективности метода анализа при необходимости классифицирования входных значений ПД на большое количество группировочных классов. 3. Зависимость метода от правильного и четкого определения признакового пространства, которым обладают входные значения ПД и на основе которого осуществляется их классификация. 4. Деревья решений подвержены проблеме *overfitting* (переобучения).
Метод, основанный на применении иммунных систем	1. Достаточно высокий уровень надежности результатов. 2. Способность к параллельной обработке большого объема собранных значений ПД. 3. Эффективный механизм фильтрации входных значений ПД. 4. Способность к классификации и кластеризации собранных значений ПД по различным признакам. 5. Способность к обучению.	1. Неспособность выявления уязвимостей КИС, функционирующих по UDP протоколу, а также при последовательном внесении изменений на КИС, осуществляемых в целях формирования новых уязвимостей. 2. Сложность процедур настройки иммунных систем. 3. Необходимость в определенном интервале времени, которое затрачивается на обучение иммунной системы. 4. Достаточно высокий уровень сложности проводимых вычислительных операций.

Стоит отметить, что рассмотренные методы (Табл. 2) являются одними из наиболее распространенных и конечно обладают более расширенным перечнем преимуществ и недостатков. Отдельные представленные методы могут характеризоваться набором схожих преимуществ и недостатков. Практически любой указанный метод, в основе которого лежит определенный алгоритм или математический аппарат (модель), может с разной степенью эффективности применяться как в сигнатурном, так и поведенческом анализе. Необходимо обратить внимание на то, что большинство методов (например, искусственные нейронные сети, искусственные иммунные системы, метод, основанный на применении алгоритмов нечеткой логики, генетические алгоритмы, Байесовские сети и метод, деревья решений, MAP-сплайны, алгоритмы кластеризации, алгоритмы регрессии, роевые алгоритмы, метод опорных векторов и т.д.) относятся к перспективным технологиям интеллектуального анализа данных (Data Mining) (далее по тексту – ИАД) [4].

Сравнительный анализ методов (Табл. 2) указывает на то, что модели ИАД представляют собой динамический итеративный процесс, главными целями которого являются [2; 5]:

- извлечение из множества собранных значений ПД ($S_n^{вх}$, $F_n^{тек}$) новых (актуальных, полезных, понятных, наиболее важных и т.п.) знаний ($K_{иад}$), позволяющих оперативно выявлять известные и неизвестные уязвимости КИС;
- выявление неочевидных практически важных закономерностей (корреляционных зависимостей) между собранными значениями ПД (событиями и т.п.);
- выдвижение на основе знаний и закономерностей гипотез об уязвимостях КИС.

Принимая во внимание вышеуказанное, наибольшей эффективности в выявлении уязвимостей КИС можно достичь посредством реализации комбинированного метода, который заключается в синтезе сигнатурного и поведенческого анализа, с обязательным применением моделей (алгоритмов) ИАД (Рис. 1). Здесь стоит отметить, что применение моделей ИАД невозможно без четкого понимания этапов, реализуемых в его пределах:

- 1-й этап заключается в постановке задач;
- в рамках 2-го этапа осуществляются сбор и фильтрация входных значений ПД ($S_n^{вх}$, $F_n^{тек}$) (устранение избыточной, явно ошибочной и иной информации), нормализация $S_n^{вх}$, $F_n^{тек}$ (приведение значений ПД к форме, пригодной для анализа в конкретной модели ИАД), классификация $S_n^{вх}$, $F_n^{тек}$ (отнесение входных значений ПД к одному из заранее известных классов), регрессия $S_n^{вх}$, $F_n^{тек}$ (определение значений ПД по известным характеристикам КИС) или кластеризация $S_n^{вх}$, $F_n^{тек}$ (логическое предположение классификации при условии, что классы изучаемого набора значений ПД заранее не определены; процессы классификации и регрессии явно противоположны процессу кластеризации, причем в разных моделях ИАД реализуются те или/и другие процессы);
- в начале 3-го этапа выполняется процедура сопоставления (сравнения) $S_n^{вх}$ с $S_{уяз}$ (сигнатурного анализа), а в последующем – процедура выявления несоответствий между $F_n^{тек}$ и $F_{штат}$ (поведенческого анализа), которая необходима для подтверждения результатов процедуры сопоставления (сравнения), а также для выявления неизвестных уязвимостей, образы которых отсутствуют в БД. Стоит обратить внимание на то, что указанная последовательность анализа ПД является неслучайной, так как $T_{сиг} < T_{повед}$, где $T_{сиг}$, $T_{повед}$ – время, затрачиваемое на осуществление процедур сопоставления (сравнения) и выявления несоответствий, соответственно (при условии выявления известных уязвимостей);

- 4-й этап заключается в агрегировании знаний (объединение однотипной информации в одну), полученных на 3-м этапе, выявлении между множеством извлеченных знаний корреляционных зависимостей (например, каждый отдельно взятый элемент (информация) из извлеченных знаний может не свидетельствовать об уязвимостях КИС) и приоритезации извлеченных знаний (присвоение извлеченным знаниям соответствующего уровня опасности);
- 5-й этап необходим для применения новых извлеченных знаний ($K_{иад}$).

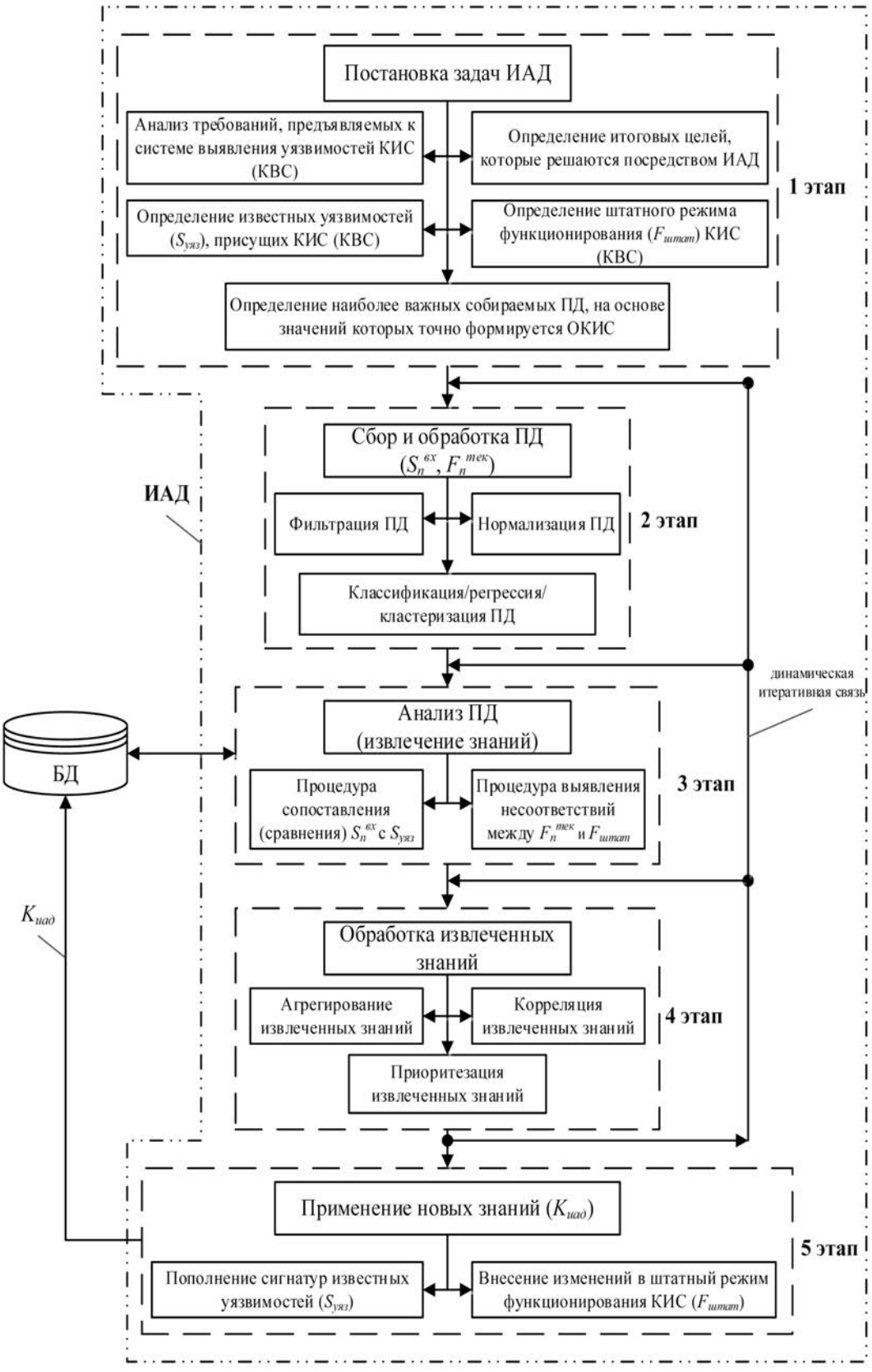

Рис. 1. *Обобщенная модель комбинированного метода анализа ПД на основе ИАД*

Наряду с тем, что, как и в любом другом процессе, качественная реализация всех указанных этапов модели ИАД оказывает влияние на достижение поставленных целей, в нашем случае – выявление уязвимостей КИС, – стоит обратить внимание на принципиально важное значение 1-го этапа. Без правильной, четкой и своевременной постановки задач невозможно обеспечить необходимый уровень защищенности КИС (КВС). В связи с вышеизложенным, следует вывод о том, что для разработки системы выявления уязвимостей КИС (КВС) необходимо определить требования, предъявляемые нормативными правовыми актами, руководящими документами и вышестоящими органами управления к контролю и оценке защищенности как конкретных КИС, так и КВС в целом [10].

Список литературы

1. **Ачилов Р.** Система Nagios. Комплексный мониторинг. Часть 1 // Системный администратор. 2014. № 9 (142). С. 28-31.
2. **Барсегян А. А., Куприянов М. С., Холод И. И., Тесс М. Д., Елизаров С. И.** Анализ данных и процессов: учеб. пособие. 3-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2009. 512 с.
3. **Бешков А.** Мониторинг Windows-серверов с помощью Nagios // Системный администратор. 2003. № 7 (8). С. 12-19.
4. **Браницкий А. А., Котенко И. В.** Анализ и классификация методов обнаружения сетевых атак // Труды Санкт-Петербургского института информатики и автоматизации Российской академии наук: сб. науч. трудов / ред. Р. М. Юсупов. СПб.: СПИИРАН, 2016. № 2 (45). С. 207-244.
5. **Булдакова Т. И., Джалолов А. Ш.** Выбор технологий Data Mining для систем обнаружения вторжений в корпоративную сеть [Электронный ресурс] // Инженерный журнал: наука и инновации. 2013. № 11 (23). URL: http://elibrary.ru/item.asp?id=20928241 (дата обращения: 24.11.2016).
6. **Кенин А. М.** Практическое руководство системного администратора. 2-е изд. СПб.: БХВ-Петербург, 2010. 464 с.
7. **Кенин А. М.** Самоучитель системного администратора. 3-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2012. 512 с.
8. **Климов С. М.** Методы и модели противодействия компьютерным атакам. Люберцы: КАТАЛИТ, 2008. 316 с.
9. **Коноваленко С. А., Королев И. Д.** Анализ систем мониторинга вычислительных сетей // Молодой ученый. 2016. № 23 (127). Ч. 1. С. 66-72.
10. **Коноваленко С. А., Королев И. Д., Новоселов Д. А.** Базовые функциональные возможности существующих систем мониторинга вычислительных сетей // Приволжский научный вестник. 2016. № 12 (64).
11. **Корнеев В. В., Райх В. В.** Интеграция сигнатурного и поведенческого механизмов анализа данных мониторинга в системах обнаружения атак // Материалы II Международной научной конференции по проблемам безопасности и противодействия терроризму (Московский государственный университет им. М. В. Ломоносова, 25-26 октября 2006 г.). М.: МЦНМО, 2006. С. 186-198.
12. **Лукацкий А. В.** Обнаружение атак. 2-е изд. СПб.: БХВ-Петербург, 2003. 608 с.
13. **Моррис У. Т.** Наука об управлении. Байесовский подход. М.: Мир, 1971. 304 с.
14. **Норткат С., Новак Д.** Обнаружение нарушений безопасности в сетях / пер. с англ. 3-е изд. М.: Издательский дом «Вильямс», 2003. 448 с.
15. **Сердюк В. А.** Новое в защите от взлома корпоративных систем. М.: Техносфера, 2007. 360 с.
16. **Тулупьев А. Л., Николенко С. И., Сироткин А. В.** Байесовские сети: логико-вероятностный подход. СПб.: Наука, 2006. 607 с.
17. **Установка системы Cacti под Unix** [Электронный ресурс]. URL: http://www.cacti.net/downloads/docs/contrib/install_russian_unix.pdf (дата обращения: 08.11.2016).
18. **Установка системы Cacti под Windows** [Электронный ресурс]. URL: http://www.cacti.net/downloads/docs/contrib/install_russian_windows.pdf (дата обращения: 07.11.2016).
19. **Хайкин С.** Нейронные сети: полный курс / пер. с англ. 2-е изд. М.: Издательский дом «Вильямс», 2006. 1104 с.
20. **Яремчук С.** Cacti – простой и удобный инструмент для мониторинга и анализа сети // Системный администратор. 2007. № 4 (53). С. 22-27.
21. **The Cacti Manual** [Электронный ресурс]. URL: http://www.cacti.net/downloads/docs/pdf/manual.pdf (дата обращения: 07.11.2016).
22. **Unix и Linux: руководство системного администратора** / Э. Немет, Г. Снайдер, Т. Хейн, Б. Уэйли; под ред. Д. А. Клюшина; пер. с англ. 4-е изд. М.: ООО «И.Д. Вильямс», 2012. 1312 с.
23. **Zabbix Documentation** [Электронный ресурс]. URL: https://www.zabbix.com/documentation (дата обращения: 05.11.2016).

IDENTIFICATION OF VULNERABILITIES OF INFORMATION SYSTEMS THROUGH COMBINED ANALYSIS OF PARAMETRIC DATA DETERMINED BY SYSTEMS FOR MONITORING NETWORKS

Konovalenko Sergei Aleksandrovich
Korolev Igor' Dmitrievich, Doctor in Technical Sciences, Professor
Krasnodar Higher Military School
konovalenko_rcf@mail.ru; pi_korolev@mail.ru

The article compares signature and behavioral analyses of parametric data determined by systems for monitoring networks. The authors construct a generalized model of the combined method of parametric data analysis on the basis of technologies of intellectual analysis of data, which enables to increase efficiency of the specialist's work on identification of vulnerabilities of controlled information systems.

Key words and phrases: combined method of data analysis; behavioral method of data analysis; signature method of data analysis; monitoring systems; technologies of intellectual analysis of data.