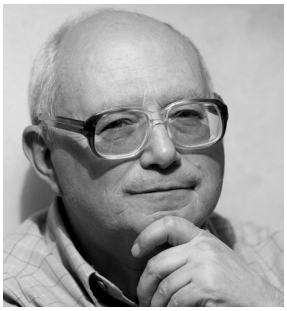
УДК 004.056.53



А.В.Скатков,
д-р.техн.наук,
профессор,
Севастопольский
национальный
технический
университет
e-mail: kvt.sevntu@gmail.com

КОМПЛЕМЕНТАРНОЕ ДЕТЕКТИРОВАНИЕ АТАК В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

А.В.Скатков. **Комплементарное детектирование атак в телекоммуникационных системах критического применения.** Рассматриваются задачи системной динамики сетей обработки данных в условиях действия вирусных атак. Предлагается совокупность оптимизационных задач выбора структуры и параметров комплементарных детекторов вирусных атак. Обсуждается возможность использования адаптивного подхода с целью повышения эффективности противовирусных мероприятий.

O.V.Skatkov. **Complementary detection of attacks in telecommunication systems critical applications.** We consider the problem of system dynamics data networks in times of virus attacks. Optimization is proposed to set-ting problems of selection of the structure and parameters of complementary detection of viral attacks. The possibility of using an adaptive approach to improve the effectiveness of anti-vovirusnyh events.

Введение. Телекоммуникационных системы (ТС) находят применение во многих промышленных приложениях и социальной деятельности, развитие соответствующих информационных технологий приводит к повышению эффективности многих инфраструктур, частью которых являются ТС. В большинстве случаев эти инфраструктуры являются инфраструктурами критического применения (КИ)[1]. Данный факт накладывает определенные ограничения и дополнительные требования к гарантоспособности и безопасности критических ТС (КТС).

Отказ или нарушение работы КТС может привести к дезорганизации работы всей инфраструктуры и, следовательно, критическим ситуациям, которые потенциально несут катастрофических последствий. Налагаемые на безопасность и гарантоспособность КТС требования делают их так же критичными. КТС, будучи одной из основных компонент КИ, должна обеспечивать высокую надежность передачи данных между подсистемами инфраструктуры, одновременно с этим иметь высокий уровень готовности, реактивности и в целом обеспечивать гарантоспособность как системное качество.

© А.В.Скатков, 2013

Высокий уровень гарантоспособности системы передачи данных не может быть достигнут без обеспечения требуемого уровня безопасности. Не смотря на интенсивное развитие компьютерных систем и информационных технологий защиты, КТС продолжают быть уязвимыми для внешних и внутренних вирусных атак (ВА). Основной угрозой безопасности КТС являются акты несанкционированного перехвата каналов обмена информацией и управления КТС. Несанкционированный перехват канала связи может быть осуществлен в результате нарушения прав доступа субъектов к объектам КТС. В настоящее время разработаны и эффективно применяются многие методы и технологии противодействия, как вирусным атакам, так и актам нарушения прав доступа (А-события). К этим методом следует отнести широкий спектр антивирусных программных средств, аппаратных средств защиты каналов связи, средства регистрации действия субъектов компьютерных систем и многие другие[2], которые интенсивно развиваются в научном и прикладном аспектах.

Материал и результаты исследования. Критическая компьютерная сеть (ККС) как элемент КТС предназначена для информационной обработки множества функциональных задач (ФЗ), поддерживающих оперативное управление нормальной работоспособности совокупности объектов критического назначения (ОКН), порождающих поток запросов с жёстким регламентом времени окончания обработки, и выдачи управляющей информации. Информационное описание множества ФЗ представимо кортежем:

$$ФЗ :< ДДС, ПЗ, ВТ, КН > \quad (1)$$

Структуры в правой части (1) являются векторными функциями операционных моментов времени принятия решений $t_k \in [0;T]$, т.е. при фиксированном t_k образуют числовые векторы:

ДДС - директивные сроки окончания обработки запросов и дисциплин их обслуживания;

ПЗ - интенсивности формирования потоков запросов по каждой ФЗ;

ВТ – вычислительные трудоёмкости запросов (объём элементарных машинных операций, необходимых для обработки запросов);

КН – нагрузки на телекоммуникационные сети, определяемые интенсивностями информационных сообщений, связанных с обработкой запросов.

Для нестационарных задач элементы кортежа (1) структурно представляют собой числовые матрицы, каждая строка которых соответствует фиксированному $t_k \in [0;T]$ и определяет текущее значение векторов ДДС, ПЗ, ВТ, КН.

Функциональное назначение ККС состоит в качественном решении ФЗ по совокупности критериев, определяемых особыми условиями функционирования ОКН. В первую очередь должны быть учтены такие характеристики информационного обслуживания, как реактивность, достоверность,

© А.В.Скатков, 2013

гарантоспособность своевременного окончания обработки каждой ФЗ.

Информационное описание ККС как системного образования – это кортеж следующей структуры:

$$ККС : \langle ФЗ, ПЦОД, СКВ, ТОВП, СПВЗ, ДДС, E, DR \rangle \qquad (2)$$

ПЦОД – множество процессорных центров обработки данных;
СКВ – множество узлов сети коммуникационного взаимодействия;
ТОВП – система технологического обеспечения вычислительного процесса;
СПВЗ - система противовирусной защиты;
Е – критерий качества функционирования ККС;
DR – доступные ресурсы.

Энтропия состояний ККС, определяемая как результат информационных взаимодействий внешних факторов и элементов кортежей (1), (2), характеризуется структурно-параметрической недоопределённостью:

$$H : \langle ФЗ, ККС, ВС \rangle ,$$

где ВС - информационное описание мгновенных воздействий внешней среды.

Общая структура функциональной модели КТС, включающей в себя систему защиты, предоставлена на рисунке 1, в которой выделены: виртуальная среда облачных вычислений (ВСОВ), серверы (С), маршрутизатры (М), стационарные и мобильные панели (СП, МП), а так же указаны места, где функционально обоснованно должны быть расположены детекторы вирусных атак (ДВА). При дефиците ресурсов возможны иные альтернативные схемы размещения ДВА. Организация работы КТС поддерживается службами системного администрирования (СА) и ЛПР.

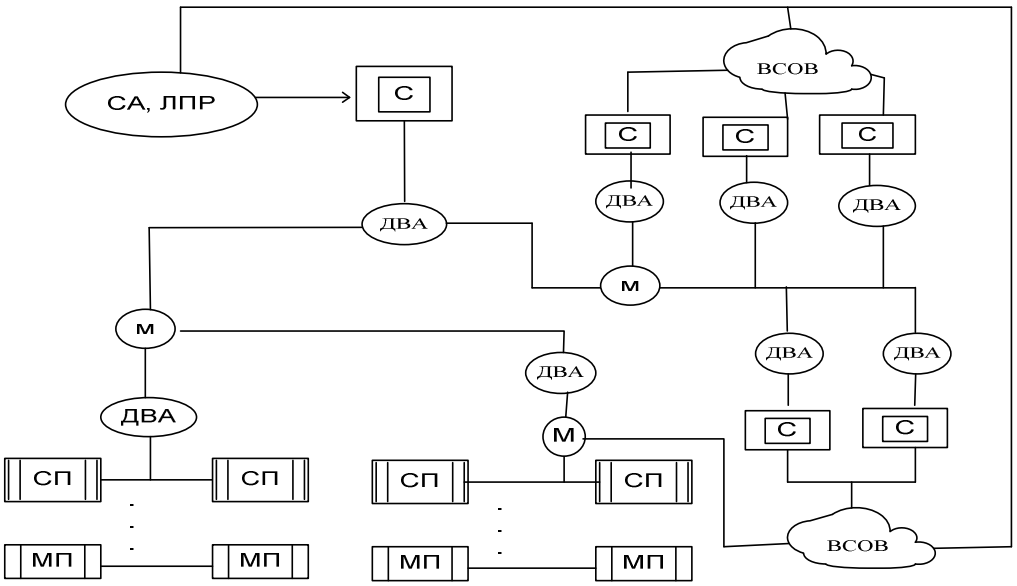


Рис. 1. Схема типовой структуры критической КТС с развитой системой защиты

© А.В.Скатков, 2013

Постановка и поиск решений оптимизационных задач синтеза детекторов А-событий диктует необходимость введения в правую часть (2) таких элементов, как λ_ϕ, μ_ϕ, $\mu_П$, $\lambda_П$, где λ_ϕ и $\lambda_П$ - фактическая и плановая интенсивности поступления запросов в ККС, μ_ϕ и $\mu_П$ - фактическая и плановая интенсивности обработки запросов.

$$ККС : \langle ФЗ, ПЦОД, СКВ, ТОВП, СПВЗ, ДДС, E, DR, H, \lambda_\phi, \lambda_П, \mu_\phi, \mu_П \rangle \quad (3)$$

Интенсивности $\lambda_\phi : \langle ФЗ, ДДС \rangle$ и $\lambda_П : \langle ФЗ, ДДС \rangle$ определяются на основе суммарной интенсивности циркулирующих потоков в ККС, представимых моделями класса замкнутых СМО класса $G|G|M|K$ с возможными прерываниями и присутствием эффекта «потери заявок».

Интенсивности μ_ϕ и $\mu_П$ определяются системными требованиями к суммарной производительности ККС как замкнутой СМО класса $G|G|M|K$ и доступными ресурсами DR

$$\mu_\phi(ККС) : \langle ПЦОД, СКВ, ТОВП, СПВЗ, \mathrm{DR}, \lambda_\phi \rangle$$
$$\mu_П(ККС) : \langle ПЦОД, СКВ, ТОВП, СПВЗ, \mathrm{DR} \rangle \quad (4)$$

Критерий качества функционирования ККС определяется, в первую очередь, принятой ТОВП и эффективностью работы СПВЗ: $E(V_i, U_j, t_k, \xi)$, где $V : \{V_i(ТОВП, t_k)\}$ и $U : \{U_j(СПВЗ, t_k)\}$ - i-й вариант технологии обработки данных и j-й вариант детектирования А-событий, ξ - случайное внешнее воздействие, связанное с А-событием, тогда $E(V_i, U_j, t_k, \xi_k)$, ξ_k - нестационарная компонента. При оценивании E следует пользоваться его математическим ожиданием, т.е. $M\{E(t_k); 0 \le t_k \le T\}$.

Информационное описание СПВЗ – это кортеж вида:

$$СПВЗ :< ФО, СО, ПО, ДО, ДВА > \quad (5)$$

Р – правила поддержки принятия решений по управлению стратегиями обнаружения атак; S – стратегии обнаружения атак и актов нарушения прав доступа в КТС; R – системные ресурсы, выделяемые на противодействие атакам в КТС; λа – интенсивность атак в КТС; Cs – вектор системных характеристик КТС; Кк – функционал эффективности применяемых к атакам контрмер.

Детекторы вирусных атак могут быть реализованы по различным технологиям, основные из которых соответствуют трём следующим классам:

-детекторы, использующие результаты сигнатурного анализа и периодически пополняемые библиотеки сигнатур;

- детекторы, реализованные с использованием интеллектуальных информационных технологий на основе нейросетевых решений и нечёткой логики;

- статистические критериальные детекторы, основанные на использова-

© А.В.Скатков, 2013

нии непараметрических критериев математической статистики.

Для ККС, на наш взгляд, наиболее оправдано применение критериальных детекторов как обладающих сравнительно наиболее высокой реактивностью, управляемым уровнем достоверности и малой вычислительной трудоёмкостью.

Критерий E зависит от интенсивностей возникновения А-событий, интенсивностей отказов и восстановлений, требований достоверности принимаемых решений. Критерий E как скалярная характеристика может интерпретироваться, например, как нестационарный коэффициент готовности с последующей стационарной аппроксимацией, вероятность гарантированного обслуживания заявки за время, не превышающее директивное, и т.д. В более общем случае к построению E следует подходить как к векторной оценке качества функционирования ККС, учитывающей совокупность скалярных критериев. В частности, эффективность ККС можно характеризовать соотношениями фактического и потенциального быстродействий, а так же соотношением функциональной и потенциальной пропускных способностей коммуникационных каналов. Тем самым определяются $К_П$ - коэффициент использования ПЦОД и $К_С$ - коэффициент использования коммутационной сети:

$$K_{П} = \frac{\mu_{\phi}}{\mu_{П}}, K_{П} \in [0;1] , \quad K_{C} = \frac{\nu_{\phi}}{\nu_{П}}, K_{C} \in [0;1]. \qquad (6)$$

В данной работе принята гипотеза о том, что основной первопричиной различия функциональных и потенциальных характеристик является последствие воздействий А-событий, так как объектом вирусных атак и несанкционированного доступа, в первую очередь, являются процессорные и канальные ресурсы. Своевременное обнаружение А-событий и последующие управления восстановлением ККС позволяют в случае их эффективности повысить значения этих коэффициентов, приближая их к правой границе области изменения.

Задача управления ККС: при известных элементах кортежей (1), (2), (3), (4) найти такие решения (u, t_k) для настройки ТОВП и СПВЗ, которые обеспечивают $\mathrm{M}(\mathrm{E}_0(\mathrm{u}, \mathrm{t}_\mathrm{k}, K_{П}, K_{C})) \in E_{C}$ или $\mathrm{M}(\mathrm{E}_0(\mathrm{u}, \mathrm{t}_\mathrm{k}, K_{П}, K_{C})) \in E_{П}$, где E_C и $E_П$ – множества эффективных векторов оценки качества ККС по Слейтеру или по Парето соответственно. Оценка $e(u, t_k)$ критерия $\mathrm{E}(\mathrm{u}, \mathrm{t}_\mathrm{k})$ определяется, таким образом, управлением $\mathrm{u} \in \mathrm{U}_0, t_k \in [0, T]$, где T имеет смысл терминального времени обработки всех заявок, связанных с решением ФЗ.

Текущие значения оценок $e = \{\mathrm{e}_1, e_2, ..., e_{|U|}\}, e_i \geq 0$ зависит от u, определяемых в моменты времени t_k, а так же от V(u),U(u). Эта последовательность содержит такое e_{i0}, что оно обеспечивает

© А.В.Скатков, 2013

$$e_{i0} = \underset{u_i \in U_0}{\text{ext}} (e_i(u_i, t_k)). \quad (7)$$

Далее будем полагать, что конструктивно оценка E построена таким образом, что целью управления является её максимизация.

Определим меру отклонения от эффективного решения как $\max_{1 \le i \le |U|} |e_{i0} - e_i| / e_{i0}$. Задача поиска оптимального управления ККС при таком подходе может быть сформулирована как нахождение такого управления, которое обеспечивает оценку качества на основе решения следующей минимаксной задачи:

$$\min_{u \in U} \max_{1 \le i \le |U|} \frac{|e_{i0} - e_i|}{e_{i0}} \quad (8).$$

В данной работе задача выбора эффективных управлений ККС рассматривается с точки зрения организации, в первую очередь, функционирования СПВЗ, т.е. управления выбором решений $U \in U_{эфф}$ при фиксированных решениях для $V \in V_{эфф}$. Отметим, что в рамках рассматриваемой задачи именно $u_i(t_k)$ определяет численные значения коэффициентов $K_{Л}(t_k, \xi)$ и $K_{C}(t_k, \xi)$ и их математические ожидания $M(K_{Л}(t_k, \xi))$ и $M(K_{C}(t_k, \xi))$ в δ-окрестности операционной точки t_k: $(t_k - \delta; t_k + \delta)$. На временном интервале $(t_k - \delta; t_k)$ осуществляется сбор статистики, на временном интервале $(t_k; t_k + \delta)$ осуществляется обработка данных и принятие решений.

Далее предлагается система комплементарного принятия решения на основе блока модулей детекторов вирусных атак (КС-система).

Структура адаптивного комплементарного детектора вирусных атак приведена на рисунке 2. Его основу составляет блок модулей детекторов, каждый из которых предназначен для обработки данных в соответствии с алгоритмами непараметрических методов математической статистики о проверке гипотез H0, H1. Таким образом, на вход каждого модуля подаются две выборки, одна из которых соответствует нормальному течению процессов обработки данных в смысле коэффициентов $K_{Л}$ и K_{C}, вторая соответствует выборочным данным, полученным в данный момент времени t_k. Если нет достаточных оснований к построению нормативной выборки, то в качестве её принимается значение выборочных данных, зафиксированное в момент времени t_{k-1}. Промежуток времени $(t_k - t_{k-1})$ используется для формирования текущих операционных выборок. На выходе каждого детекторного модуля формируется оценка вероятностей принятия гипотез P(H0|H0), P(H0|H1), P(H1|H0), P(H1|H1).

© А.В.Скатков, 2013

Целесообразность использования методов непараметрической статистики подтверждается тем, что, во-первых, исследуются выборки малых объемов, во-вторых, нет достаточных оснований для принятия адекватных моделей по их функциям распределений, и, в-третьих, они обладают сравнительно низкой вычислительной трудоемкостью. В первую очередь, при оценивании ситуаций по изменению выборочных коэффициентов $K_П$ и K_C, представляет интерес наличие эффекта сдвига распределений, т.е. сдвига выборочных данных. Вследствие этого, используя рекомендации работы [3], выбраны следующие критерии, обладающие описанным свойством: критерий знаков (модуль SIGN), критерий Уилкоксона (модуль Willcoxon), критерий Фрезера (модуль Fraser), критерий Фридмана (модуль Fridman), критерий Пейджа (модуль Page), критерий Доксама (модуль Doksum), критерий ранговых сумм Фридмана (модуль RANG SUMM Fridman), критерий Квейда (модуль Quade).

В структурной схеме коммутация информационных потоков осуществляется с помощью управляемых многопозиционных ключей. Предусмотрены следующие коммутационные блоки: K_1 – коммутатор входного трафика, K_2 – коммутатор блока детекторных модулей, K_3 – коммутатор выходных каналов детекторных модулей, K_4 – коммутатор подсистемы сбора статистики, K_5 – коммутатор тестовых трафиков.

Динамический анализ сетевого трафика может выполняться по различным альтернативным схемам, отличающимся длительностью интервалов времени регистрации такого трафика, а также правилами принятия решений по определению момента времени начала и конца регистрации. В значительной степени эта задача требует неформализованных решений на основе экспертных знаний, которые реализуются функциональным блоком «ЛПР». Совокупность альтернативных программ динамического анализа трафика содержится в блоке D. Список таких программ может пополняться, а для организации его работы можно использовать методы адаптивного выбора вариантов, в связи с чем предлагаемая технология в целом является адаптивной.

Комплекс АКД может работать в двух режимах: рабочего функционирования и тестового имитационного моделирования. Второй режим предназначен для обучения ЛПР обоснованному принятию решений при постулировании событий, связанных с возникновением ситуаций, соответствующих гипотезам H0, H1. Второй режим позволяет, кроме того, определить области устойчивого распознавания, устойчивого нераспознавания и толерантные области по отношению к используемым критериям [4]. По результатам имитационного моделирования (второй режим) становится также возможным определение совокупности следующих системных характеристик:

- наиболее мощного относительного непараметрического критерия;

© А.В.Скатков, 2013

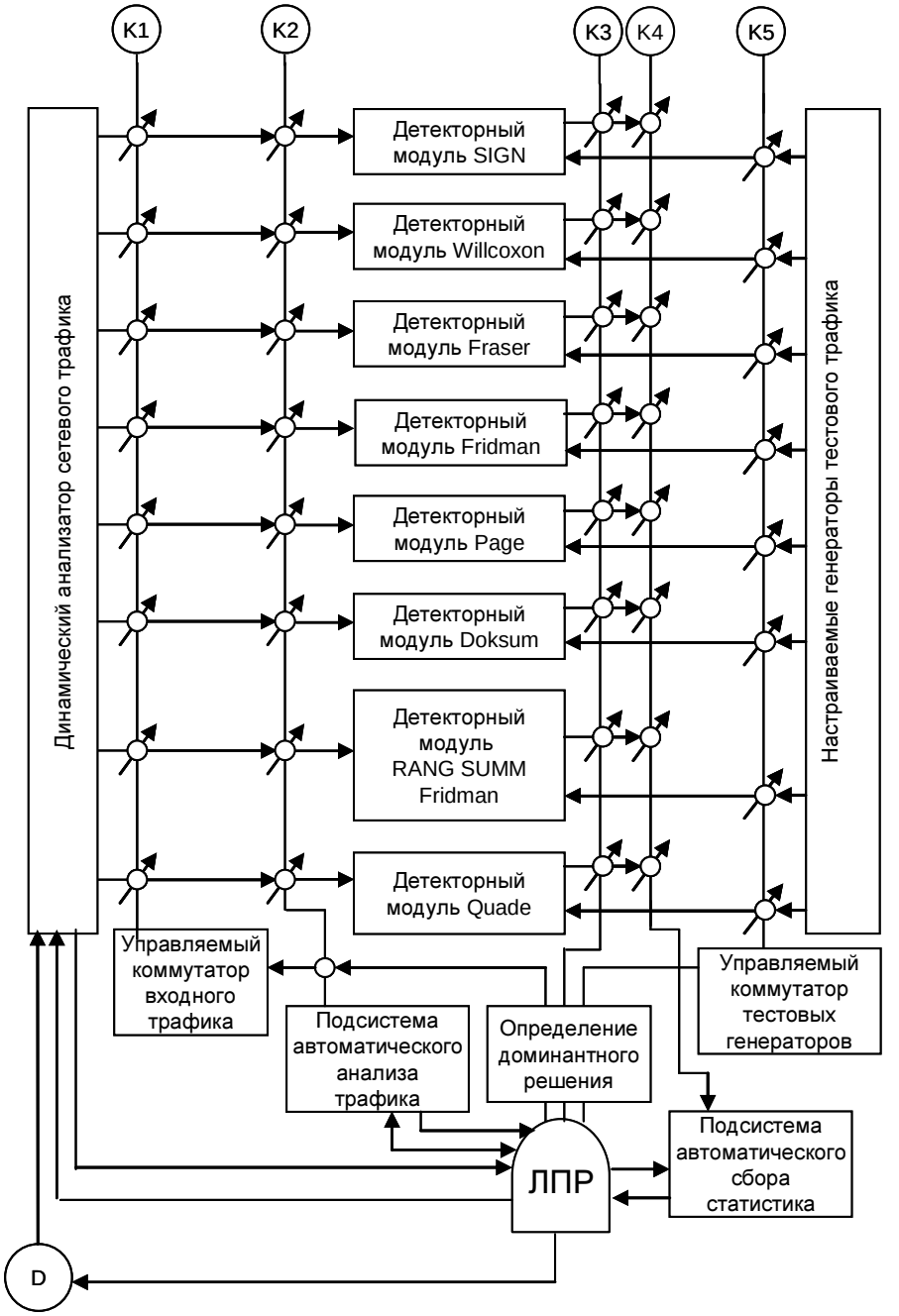


Рис. 4. Структура адаптивного комплементарного детектора (АКД) вирусных атак

© А.В.Скатков, 2013

- параметрически настраиваемого комплементарного критерия;
- области комплементарного достоверного распознавания факта вирусной атаки;
- области комплементарного уверенного нераспознавания факта вирусной атаки.

Содержательно постановка задачи комплементарного детектирования атак в телекоммуникационных системах состоит в том, что совокупность детекторных модулей (ДМ) должна быть такой, чтобы обеспечивалась следующая система требований:

1. Хотя бы один из детекторов, входящих в АКД, обеспечивал уверенное распознавание ситуации H0|H0.

2. Хотя бы один из детекторов, входящих в АКД, обеспечивал уверенное распознавание ситуации H0|H1.

3. Хотя бы один из детекторов, входящих в АКД, обеспечивал уверенное распознавание ситуации H1|H0.

4. Хотя бы один из детекторов, входящих в АКД, обеспечивал уверенное распознавание ситуации H1|H1.

5. Если имеется пара детекторов, противоречиво оценивающих информационную ситуацию, то для окончательного принятия решений используются оценки менее мощных детекторов.

Результаты имитационного моделирования достаточного объема позволили выявить области наибольшей компетентности для детекторов, используемых в АКД. На рисунке 3 показан кластер стохастических точек, используемых для посторения областей компетентности детекторов при оценивании гипотезы H0|H0, при этом $p=0,57$, $r=0,82$, $\alpha=0,67$. На рисунке 4 приведен результат аппроксимации 0-го порядка (отрезками прямых, параллельных координатным осям) областей комплементарности детекторов вирусных атак при оценивании гипотезы H0|H0. Так, например, область с вершинами *f[0,82; 0,64],c[0,82; 0,67], b[0,62; 0,67], h[0,62; 0,64]* областью наибольшей компетентности для модуля Fraser. Аналогичным образом определены области устойчивой компетентности для остальных модулей, что в совокупности позволило решить задачу их комплементарного использования.

Выводы. В заключение следует отметить, что:

1. Предлагаемая система АКД ориентирована на использование в режиме реального времени, так как обладает сравнительно низкой вычислительной сложностью и в силу этого может быть рекомендована, в первую очередь, для объектов критического применения.

2. Наличие в системе АКД режима имитационного моделирования процессов принятия решений позволяет ЛПР, во-первых, реализовать режим обучения, во-вторых, придает системе в целом адаптивные свойства.

© А.В.Скатков, 2013

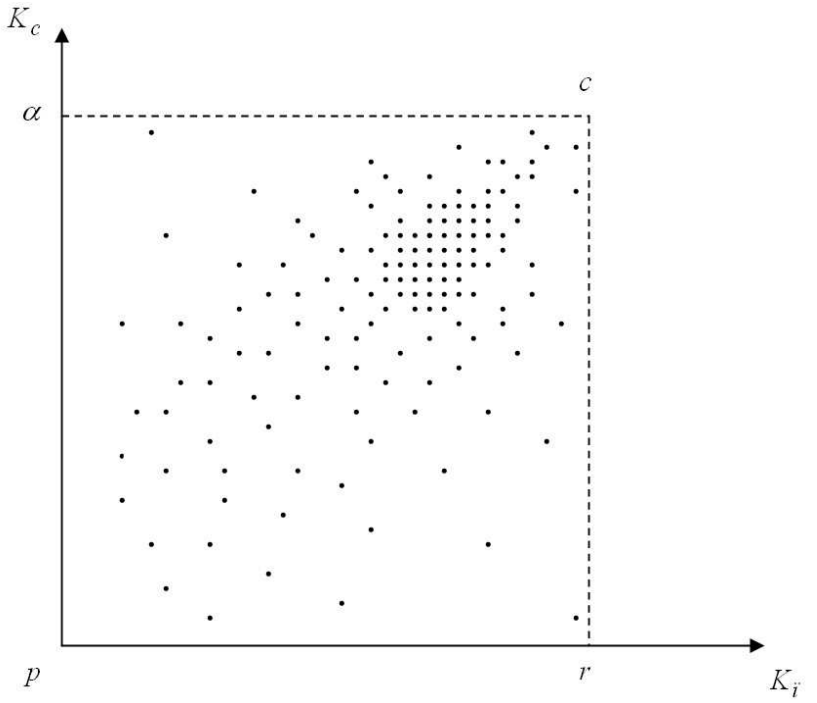


Рис. 3. Облако стохастических точек, используемых для построения областей комплементарностей детекторов атак

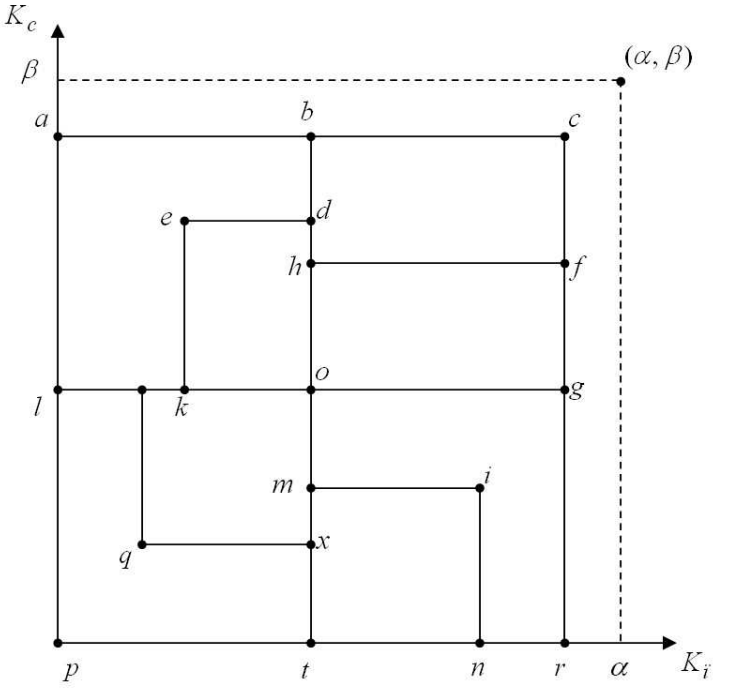


Рис. 4. Аппроксимация 0-го порядка областей комплементарности детекторов атак

© А.В.Скатков, 2013

3. Предложенная методика выявления комплементарных свойств может иметь перспективу использования и при оценивании сложных гипотез.

4. Перспективным направлением дальнейших исследований является построение процедур оценивания негаэнтропии процессов обработки данных на основе оценок гипотез, полученных с использованием системы АКД, а также разработка алгоритмов адаптивного выбора вариантов для конкретных критических приложений, позволяющих минимизировать состав комплементарного детекторного блока без нарушений его функциональной полноты.

Література

1.Информационные технологии для критических инфраструктур. /Под ред. А.В.Скаткова – Севастополь: Изд-во СевНТУ, 2012. – 306 с.

2.Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа./ А.Ю.Щеглов – СПб: Наука и Техника, 2004. – 384 с.

3.Хиценко В.Е. Непараметрическая статистика в задачах защиты информации. / В.Е.Хиценко. – Новосибирск: Изд-во НГТУ, 2012. – 196 с.

4.Ловягин В.С. и др. Программный комплекс для исследования чувствительности непараметрических критериев / В.С. Ловягин, К.Н. Маловик, А.В. Скатков // Системи обробки інформації.− Х.: − Вид-во ХУПС, 2011. – №5(95). – С. 79 − 82.

© А.В.Скатков, 2013