На правах рукописи

Баранов Василий Александрович

ОБНАРУЖЕНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК РАЗЛАДКИ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ

Специальность 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Автореферат диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург – 2012

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Санкт-Петербургский государственный политехнический университет».

Научный руководитель: Доктор технических наук,
профессор
Ростовцев Александр Григорьевич

Официальные оппоненты: Доктор технических наук,
профессор, ведущий научный сотрудник
Санкт-Петербургского
института информатики РАН
Саенко Игорь Борисович

Кандидат технических наук,
профессор Санкт-Петербургского
государственного университета
аэрокосмического приборостроения
Шехунова Наталья Александровна

Ведущая организация: ООО «Газинформсервис»,
г.Санкт-Петербург

Защита состоится « » июня 2012г. в часов на заседании диссертационного совета Д212.229.27 при ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет» (по адресу 195251, Санкт-Петербург, ул. Политехническая, д.29/1 ауд. 175 главного здания.)

С диссертационной работой можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет».

Автореферат разослан « » мая 2012г

Ученый секретарь
диссертационного совета
Платонов Владимир Владимирович

Общая характеристика работы

Актуальность. В современных информационных инфраструктурах существует множество разнообразных возможностей возникновения инцидентов ИБ (информационной безопасности). В соответствии с ГОСТ Р ИСО/МЭК 27001-2006 инцидентом ИБ является «любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность». В контексте данной работы рассматривается частный тип инцидентов ИБ, которые соответствуют выявленным изменениям в работе системы, отраженным на некоторых ее параметрах и произошедшим в результате неправомерных действий, совершаемых в ней, и/или неисправностях в программном или аппаратном обеспечении. Стандартный сценарий работы компьютерной системы (КС) в случае возникновения инцидента изменяется. Возникает необходимость выделения наблюдаемых характеристик, общих для различных сценариев работы, но по-разному используемых в штатных и нештатных режимах функционирования.

Аналитическое исследование множества возможных сценариев и выявление общих закономерностей, соответствующих легитимным последовательностям изменений характеристик, имеет неприемлемо высокую трудоемкость. Вместе с тем, фиксация момента нелегитимного изменения сценария работы или его обнаружение на временном отрезке наблюдений может дать возможность выделения инцидента ИБ по этому признаку. В работе предлагается универсальный подход к обнаружению инцидентов ИБ, основанный на моделировании их проявления в виде статистической разладки случайного процесса.

Основанием для данной работы служат исследования таких отечественных ученых как Ширяев А.Н., Бродский Б.Е., Дарховский Б.С., Будзко В.И., Грушо А.А., Зегжда П.Д., Михайлов В.Г., Скиба В.Ю., Ронжин А.Ф. и зарубежных ученых Cressie N., Read T., Salvatore J. Stolfo, Steven M. Bellovin, Shlomo Hershkop.

Подход к выявлению отклонений от стандартного сценария действий в массиве данных мониторинга системы, разработанный в рамках исследования, может найти применение и в других областях деятельности в которых применяются статистические методы исследования.

Целью диссертационной работы является разработка подхода к анализу инцидентов ИБ с их длительным проявлением во времени на основе исследования статистических характеристик, наблюдаемых параметров компьютерной системы и методики выявления их скачкообразного изменения в форме разладки процесса.

В соответствии с целью исследования к основным задачам относятся:

1. Анализ предметной области, включающий систематизацию инцидентов ИБ и исследование деятельности инсайдера.
2. Построение подхода и выработка общей модели обнаружения инцидентов ИБ априорным и апостериорным методами.
3. Разработка метода апостериорного выявления инцидентов ИБ как статистической разладки процесса наблюдения.
4. Исследование эффективности предлагаемого метода в зависимости от объемов наблюдений, наличия предварительного обучения и разности статистических характеристик процесса функционирования до и после инцидента ИБ.
5. Разработка архитектуры системы мониторинга безопасности КС в рамках концепции апостериорной защиты.

Методы исследования. При решении сформулированных задач использовался аппарат теории вероятностей и математической статистики. Для исследования предметной области проводился анализ научных наработок в областях теории оценки разладки, теории моделей. Обоснование работоспособности предлагаемого в работе подхода основано на теоретических и экспериментальных исследованиях.

Научная новизна диссертационной работы заключается в следующем:

1. Построена универсальная математическая модель инцидентов ИБ, возникающих в неизвестный момент времени периода наблюдения.
2. Предложено определение момента времени перехода из регулярного режима работы в аномальный путем исследования математической модели разладки случайного процесса.
3. Впервые для реализации апостериорного обнаружения инцидентов ИБ предложено оценивать разладку статистиками нового класса, предельные поведения которых инвариантны относительно распределения наблюдений при штатной работе КС.
4. Теоретически и экспериментально обоснована оценка эффективности алгоритмов определения и обнаружения на отрезке наблюдений инцидента ИБ.

Практическая ценность работы состоит в следующем:

1. Предложенный метод носит в значительной степени универсальный характер и позволяет анализировать нарушения ИБ, связанные как с несанкционированными действиями злоумышленников, так и с программно-аппаратными сбоями системы, независимо от их происхождения.
2. На основании предлагаемых алгоритмов поиска момента разладки можно разработать систему мониторинга функционирования КС, апостериорно выявляющую подозрительную активность в системе.

Разработанная методика анализа инцидентов ИБ использована в ООО «Газинформсервис» и ОАО «ИТМиВТ им. С. А. Лебедева РАН» в системах мониторинга, сбора, обработки и передачи информации. Практическая ценность и новизна работы подтверждается двумя Актами о внедрении. Результаты работы использовались также в составлении практических занятий по курсу лекций «Системы обнаружения вторжений» при подготовке специалистов по направлению «Информационная безопасность».

Апробация работы. Основные теоретические и практические результаты работы обсуждались на XIX и XX общероссийских научно-технических конференциях «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2010, 2011) и на XIV международной конференции «РусКрипто'2012» (Москва, 2012).

Публикации. По теме диссертации опубликовано 9 работ, в их числе 6 научных статей, из них в изданиях, входящих в перечень утвержденных ВАК РФ – 6, 3 доклада на конференциях.

Основные положения, выносимые на защиту:

1. Универсальная модель инцидентов ИБ, включающая возможные действия инсайдера.
2. Универсальный подход к апостериорному обнаружению инцидентов ИБ при помощи их моделирования разладкой случайного процесса.
3. Алгоритм определения момента разладки как метод обнаружения инцидентов ИБ.
4. Оценка эффективности предлагаемого метода на основе апостериорного подхода к обеспечению ИБ.
5. Архитектура системы мониторинга безопасности, а также программное средство, реализующее выявление разладки в процессе функционирования КС.

Структура работы. Диссертация состоит из введения, четырех глав, заключения и списка литературы из 70 наименований.

Содержание работы

Первая глава содержит постановку задачи, анализ предметной области и определение сущности рассматриваемой в работе проблемы. Систематизация инцидентов ИБ (ИИБ) представлена в виде диаграммы на рис 1.

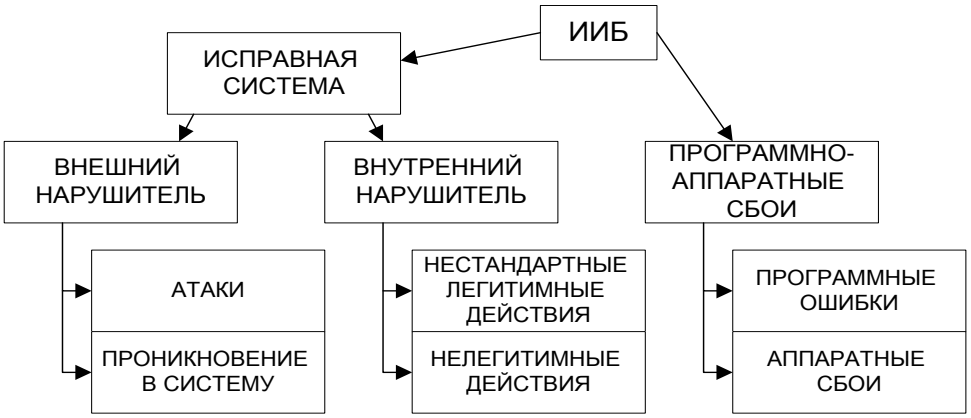

Рис. 1. Систематизация ИИБ

Для выбора адекватного метода моделирования работы КС автором был проведен анализ существующих классификаций и типов внутреннего нарушителя, включая действия инсайдера. Предложенная систематизация ИИБ явилась основанием для формирования модели наблюдаемых параметров компьютерной системы в виде случайного процесса. Существуют и другие модели наблюдаемых параметров КС, на основе которых строятся методы обеспечения ИБ. Например, анализ и выявление опасных сигнатур. Преимущество статистического метода моделирования заключается в универсальности метода выявления ИИБ независимо от источника опасности.

Как реакция на ИИБ в работе рассматриваются два подхода к обеспечению защиты, зависящие от степени важности обрабатываемой информации: априорный и апостериорный. Априорный подход применяется в основном в системах, обрабатывающих чрезвычайно важную информацию, например, содержащую гостайну. Апостериорный подход в большей степени подходит для систем с конфиденциальной информацией, не содержащих чрезвычайно важные данные, но ориентированных на применение новейших информационных технологий.

Одним из ключевых моментов в апостериорной системе защиты является блок обработки больших объемов данных о работе защищаемой системы, в котором производится автоматизированное исследование и выявление признаков ИИБ по разработанным алгоритмам. Этот блок обработки данных

можно назвать «мозгом» системы апостериорной защиты. Алгоритмы обработки основаны на определенных моделях данных о КС, которые должны отражать существенную часть функционирования КС.

Автором выделено три уровня детализации моделирования в зависимости от того, на каких процессах основывается модель: низкоуровневая, среднеуровневая и высокоуровневая. Учитывая, что для описания проявления ИИБ на низком уровне приходится анализировать достаточно длинные цепочки событий, имеющих чрезмерно большое количество возможных исходов, предлагается применять среднеуровневое или высокоуровневое моделирование.

Вторая глава посвящена разработке математической модели представления изменений параметров системы как разладки случайных процессов, а также описанию и обоснованию методов оценки момента разладки. Последовательность внутренних состояний КС

$$A_1, A_2, \dots, A_t, \qquad (1)$$

принимающих значения из алфавита $\Phi = (a_1, a_2, \dots, a_N)$, моделируется случайной последовательностью наблюдений:

$$\xi_1, \xi_2, \dots, \xi_t. \qquad (2)$$

Для упрощения теоретических расчетов предполагается, что (2) есть совокупность независимых случайных величин (СВ). Существуют предпосылки для распространения излагаемых ниже результатов и на последовательности так называемых слабо зависимых СВ, к которым относятся цепи Маркова, m-зависимые последовательности и др.

Штатная работа моделируется гипотезой H_0, в которой предполагается одинаковая распределенность СВ в (2) с N-мерным вектором вероятностей исходов $P = (p_1, \dots, p_N), p_j = P(\xi_i = a_j), j = 1, \dots, N, i = 1, \dots, t.$ Предполагается, что при возникновении ИИБ, начиная с некоторого момента θ, распре-

деления СВ $\xi_\theta, .., \xi_t$ меняются и имеют другой вектор вероятностей исходов – $\Pi = (\pi_1, \dots, \pi_N), \pi_j = P(\xi_i = a_j),\ j = 1, \dots, N,\ i = \theta, \dots, t, P \neq \Pi$.

Характеристика θ может рассматриваться как случайная ненаблюдаемая величина или как оцениваемый параметр. Ответ на вопрос о выявлении разладки при известном распределении для θ $(\theta \leq t)$ или ее отсутствии $(\theta > t)$, очевидно, сводится к различию двух гипотез – H_0, H_1:

H_0 – моделирует штатную работу системы на всем периоде наблюдаемых данных;

H_1 – моделирует возникновение ИИБ в момент θ и связанные с ним последствия на отрезке наблюдений $\theta, \theta + 1, \dots, t$.

Если P, P_θ, Π известны, что можно рассматривать как следствие обучения, то гипотезы H_0 и H_1 просты, однако оптимальный критерий Неймана-Пирсона построить не удается в силу сложности его статистик. Поэтому вместо оптимальной статистики предлагается использовать ее упрощенный вариант ζ, основанный на результатах обучения, в виде получения информации о P, Π или P_θ. Асимптотический анализ ее распределения при больших значениях t, (что моделируется условием $t \to \infty$), показал возможность выявления разладки с ошибками, стремящимися к 0. В условиях, когда распределение момента разладки на этапе обучения получить не удается, для оценки θ момента возникновения ИИБ в главе 2 предложено применять статистику

$$\zeta_k(T) = \sum_{\gamma=k}^{T+k} \ln \frac{\pi(A_\gamma)}{p(A_\gamma)},$$

являющуюся оптимальной как логарифм отношения правдоподобия при различении гипотезы H_0 $(\theta = t + 1)$ и гипотезы $\theta = 1$ как крайних значений θ.

Предварительное обучение возможно не всегда, и его данные могут не переноситься на будущую работу КС. Тогда в силу неизвестности P, P_θ, Π,

гипотезы H_0 и H_1 следует рассматривать как сложные. Классический подход оценки момента θ при неизвестных распределениях до и после разладки, заключающийся в поиске значения $\hat{\theta}$, на котором достигается максимум среди значений статистики $f(1), \dots, f(t)$, построенных по наблюдениям (1):

$$\hat{\theta} = \arg \max_{1 \le k \le t} f(k). \qquad (3)$$

Распределения предлагаемых ранее статистик $f(k)$ при $k \to \infty$ и гипотезе H_0 зависят от вектора вероятностей P. Это свойство отрицательно влияет на оценку эффективности процедуры (3), поскольку включает в эту оценку неизвестный параметр P. Приходится делать дополнительные предположения, проверить которые затруднительно.

Вместе с тем, в критериях однородности выборок $A_1, \dots, A_k$ и $A_{k+1}, \dots, A_t$, например, в критерии хи-квадрат, такая зависимость от P при $t \to \infty$ пропадает. Критерии типа хи-квадрат инвариантны к P при $t \to \infty$, так как предельным распределением этих статистик является хи-квадрат для всех P. Используя эту аналогию, автором для оценки момента разладки предложено использовать применявшиеся ранее в критериях однородности статистики, обозначаемые в работе $Cr(k, t-k, \lambda)$ и $L(k, t-k)$, где k соответствует точке разбиения последовательности наблюдений длины t, $k = 1, \dots, t$; λ – некоторый действительный параметр, определяющий конкретный вид статистики $Cr(k, t-k, \lambda), \lambda \neq 0, -1$. При $\lambda = 1$ статистика $Cr(k, t-k, \lambda)$ имеет вид хи-квадрат и была предложена ранее Ронжиным А.Ф. для выявления момента разладки. Далее в формуле (3) в качестве $f(k)$ автором использовались статистики $Cr(k, t-k, \lambda)$ и $L(k, t-k)$, и исследовалось поведение распределения этих статистик при различных λ и $t \to \infty$.

При H_0 статистики (3) порождают процесс с малым средним (не больше N), не зависящим от вида исходного распределения. При H_1 среднее и дисперсия резко возрастают, достигают величин, пропорциональных $t, t > 100N$.

Изложенное выше позволяет теоретически заключить, что предложенная модель и метод статистического анализа могут быть использованы для обнаружения разладки.

Третья глава диссертационной работы содержит описание методики применения рассмотренного во второй главе данной работы автоматизированного универсального процесса принятия решения об обнаружении ИИБ на основе апостериорного анализа выделенных данных о работе КС. Преимущество апостериорной защиты по сравнению с априорной заключается в отсутствии требований по глубокому изучению применяемых в защищаемой системе программных продуктов и возможности их быстрой модификации.

Проводятся теоретические исследования эффективности предлагаемых статистик оценки разладки, и описывается архитектура системы мониторинга и анализа состояния КС, реализующая разработанную методику. Под эффективностью статистик при различении гипотез в работе понимаются величины ошибок первого и второго рода, соответственно α и β. Чем меньше эти величины, тем статистика эффективнее. Справедливо:

Теорема. Распределение статистики $\zeta_1 = \zeta_1(t)$ для гипотезы $H_1(\theta)$ при соответствующей нормировке и центрировании

$$\frac{\zeta_1 - (\theta-1)\cdot B_0 - (t-\theta+1)\cdot B_1}{\sqrt{(\theta-1)\cdot\sigma_0^2 + (t-\theta+1)\cdot\sigma_1^2}},$$

асимптотически нормально со средним 0 и дисперсией 1, при $t \to \infty$, $N = const$, фиксированных P и Π,

$$\sigma_0^2 = D\ln\frac{\pi(\xi_1)}{p(\xi_1)}/H_0 > 0, \qquad \sigma_1^2 = D\ln\frac{\pi(\xi_1)}{p(\xi_1)}/H_1 > 0,$$

$$B_0 = E\sum_{i=1}^{N} p_i \ln\frac{\pi_i}{p_i}, \qquad B_1 = \sum_{i=1}^{N} \pi_i \ln\frac{\pi_i}{p_i}.$$

Для оценки параметра θ оптимальных, в смысле минимизации размера доверительного интервала, методов не известно. Показывается, что размер

доверительного интервала для θ при применении ζ_1 имеет величину порядка $\sqrt{t}$, что значительно повышает точность поиска момента возникновения ИИБ.

Аналогичный результат по оценке момента разладки достигается и для статистик $Cr(k, t-k, \lambda)$, $L(k, t-k)$, применяемых в случае отсутствия обучения, то есть отсутствия информации о P, P_θ, Π.

Методика применения статистического подхода изложена на рис 2. Особо следует остановиться на рекомендациях по выбору фиксируемых данных. Объем возможных вариантов значений должен быть не очень большим. С другой стороны необходимо, чтобы в эти данные вошли параметры, характеризующие парадигму действий пользователя или функционирования защищаемой системы при решении конкретной задачи.

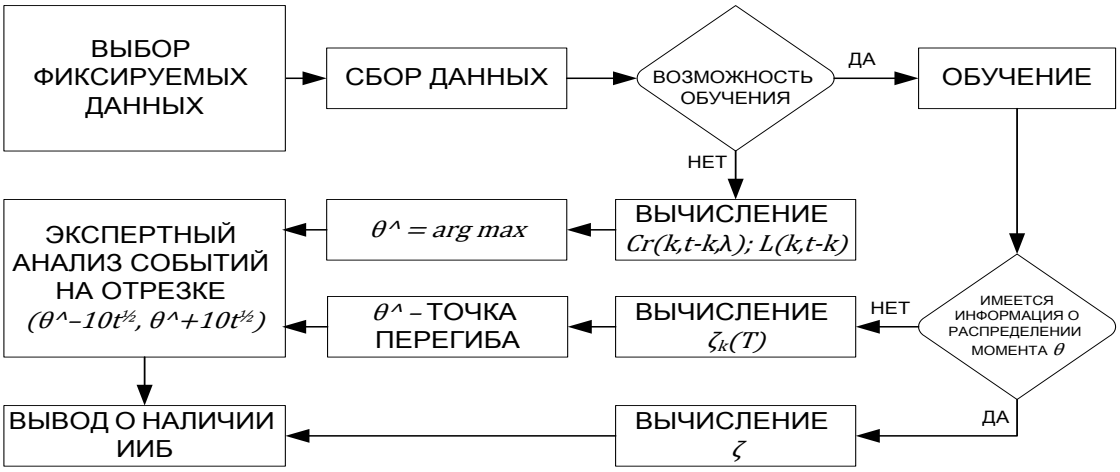

Рис. 2. Методика применения предложенного подхода

Поскольку прикладные задачи, решаемые при помощи КС, чрезвычайно разнообразны, дать универсальные рекомендации по выбору фиксируемых системой мониторинга параметров не представляется возможным. Подборка данных и их представление в значительной степени зависит от предметной области и способа реализации прикладного ПО. Как правило системы мониторинга позволяют наблюдать большое число s параметров. При этом каждый из параметров может принимать порядка 100 и более значений. Тогда $N = 100^s$ и для $s \geq 4$ эффективное применение разрабатываемого в диссертации метода возможно при сокращении количества наблюдаемых пара-

метров или объединения их возможных значений в наблюдаемые группы для выполнения условия $N \leq 100t$.

В заключение главы на основании описанной методики обнаружения ИИБ автором предложена архитектура системы мониторинга и анализа состояния КС (рис. 3).

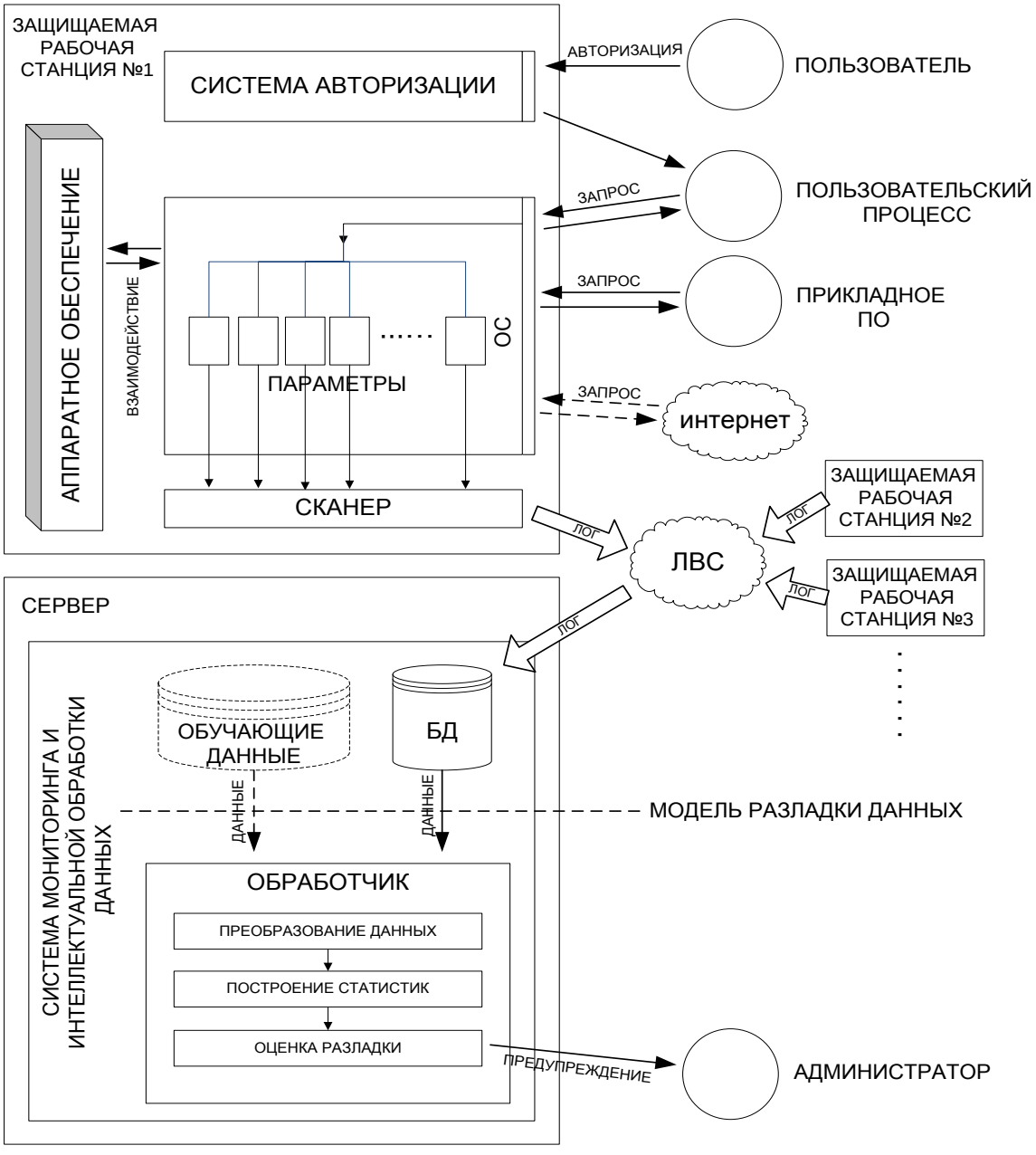

Рис 3. Архитектура системы мониторинга и анализа состояния КС

Четвертая глава содержит описание проведенного экспериментального исследования. Основная задача проведения эксперимента заключалась в под-

тверждении работоспособности предлагаемого в работе статистического метода обнаружения ИИБ.

В качестве защищаемого объекта (прикладного программного обеспечения (ПО)) было выбрано приложение Internet Explorer для операционных систем семейства Windows. Данный выбор обусловлен тем, что упомянутое приложение имеет широкое распространение в силу его интегрированности в ОС Windows. Кроме того, во время функционирования данного приложения задействуется множество различных системных ресурсов, что повышает объективность проведенных экспериментов. Разработка компонентов комплекса велась с применением языка программирования Java.

Для накопления данных, имитирующих штатную работу ПО, производились манипуляции с рассматриваемым приложением (запуск рассматриваемого приложения; посещение различных веб-ресурсов, как локальных, так и удаленных; переход по ссылкам; заполнение специальных форм; сохранение файлов и пр.). Фиксировались такие события в системе, происходившие в результате функционирования рассматриваемого приложения, как обращения к системным библиотекам, файловой системе, системному реестру. Таким образом, было накоплено порядка 7 Гб трасс как штатной, так и нештатной, после заражения вирусом, работы рассматриваемого приложения.

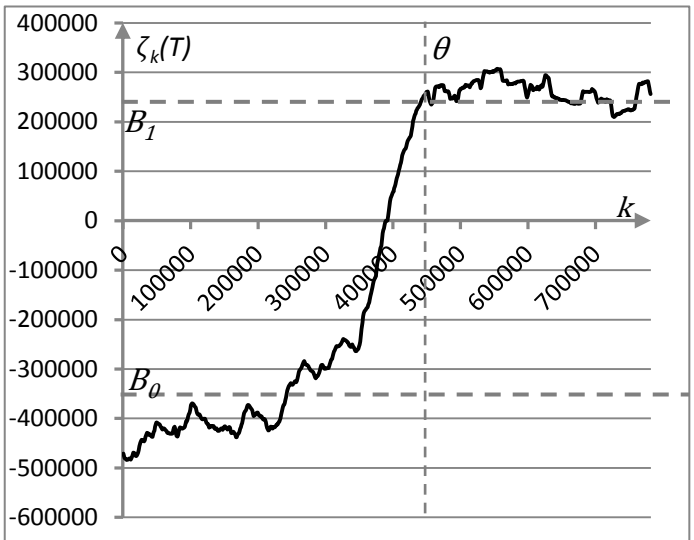

Рис. 4. График результатов для статистики $\zeta_k(T)$

На рис. 4 приведен график результатов для одного из проведенных экспериментов. Оценка $\hat{\theta} = \frac{\zeta_1(t) - tB_1}{B_0 - B_1}$, где B_0 – среднее графика до значения 0, а B_1 – после. В данном эксперименте $t \sim 9 \cdot 10^5, \theta \sim 4{,}5 \cdot 10^5, T = 10^5$, смещение равно 10^3. Результат оценки $\hat{\theta} = 4{,}59 \cdot 10^5$ практически совпал с реальным моментом разладки.

Для исследования статистик $Cr(k, t-k, \lambda)$, $L(k, t-k)$ был сформирован массив наблюдений A размером порядка $t{\sim}6{,}1 \cdot 10^6$. Момент разладки θ соответствовал примерно $2{,}5 \cdot 10^6$, а $N{\sim}\ 2{,}2 \cdot 10^4$. На рис. 5 приведен график значений среднего статистики $Cr(k, t-k, \lambda)$ для $\lambda = 0{,}1$. Для статистики $L(k, t-k)$ график близок к изображенному на рис. 5.

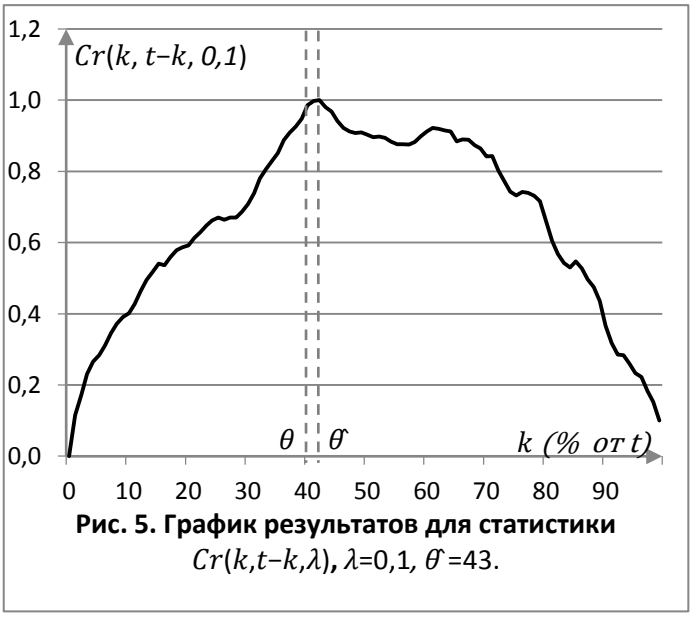

Рис. 5. График результатов для статистики $Cr(k,t-k,\lambda)$, λ=0,1, $\hat{\theta}$=43.

Результаты экспериментов подтверждают возможность практического применения предлагаемого в диссертационной работе теоретического метода решения задачи выявления ИИБ.

В ходе проведенных исследований статистики $\zeta_k(T)$ для приложения Internet Explorer было экспериментально определено, что при количестве типов наблюдений N порядка 10^4, предпочтителен размер обучаемого материала порядка 10^6.

Применение статистик $Cr(k, t-k, \lambda)$ и $L(k, t-k)$ для обнаружения ИИБ в работе приложения Internet Explorer показало, что при количестве типов наблюдений N порядка 10^4, обнаружение разладки возможно в массиве наблюдений порядка 10^6. Для других прикладных ПО подобная оценка объемов данных, скорее всего, будет отлична.

В результате диссертационных исследований:

1. Предложена модель ИИБ, и произведена систематизация деятельности инсайдера.
2. Предложена вероятностная модель обобщенных ИИБ на основе изменения параметров системы как разладки случайного процесса, на базе которой сформулирован подход к апостериорному обнаружению ИИБ.
    - Предложен метод оценки момента разладки процесса с применением предварительного обучения, и проведено теоретическое доказательство его работоспособности.
    - Предложен ряд методов оценки момента разладки процесса без применения предварительного обучения на основе статистик нового вида.
3. Разработана методика обнаружения ИИБ как момента разладки в последовательности дискретных случайных величин.
4. Проведена теоретическая оценка и сравнительный анализ эффективности предлагаемых статистик, а также ряд экспериментальных исследований, подтверждающих работоспособность метода.
5. Разработана архитектура системы мониторинга безопасности КС, основывающаяся на предлагаемой методике обнаружения ИИБ, а также создано программное средство, реализующее данную систему.

Основные результаты диссертации изложены в 9 печатных работах:

1. **Баранов В.А. Применение статистик критерия однородности для выявления разладки. / В.А.Баранов // М.: Системы высокой доступности. Из-во «Радиотехника», 2012. - №1, т. 8, С. 59-70.**
2. **Баранов В.А. О доверительном интервале для момента вторжения. / В.А. Баранов // СПб.: Проблемы информационной безопасности. Компьютерные системы. СПбГПУ, 2012. – № 1, С. 46-56.**
3. **Баранов В.А. Оценка момента вторжения статистическими методами. / В.А. Баранов // СПб.: Проблемы информационной безопасности. Компьютерные системы. СПбГПУ, 2011. – № 2, С. 24-31.**
4. **Баранов В.А. Выявление разладки процесса наблюдений как метод определения вторжения. / В.А. Баранов // СПб.: Проблемы информационной безопасности. Компьютерные системы. СПбГПУ, 2011. – № 1. С. 7-16.**
5. **Баранов В.А. Формализация определения понятия инсайдеров в вычислительных системах. / В.А. Баранов // СПб.: Проблемы информационной безопасности. Компьютерные системы. СПбГПУ, 2010. – № 2, С. 56-63.**
6. **Баранов В.А. Анализ уязвимостей веб-приложений, связанных с внедрением специального вредящего кода. / В.А. Баранов // СПб.: Проблемы информационной безопасности. Компьютерные системы. СПбГПУ, 2009. – № 1, С. 19-24.**
7. Баранов В.А. Построение доверительного интервала для момента вторжения, моделируемого разладкой. / В.А. Баранов // СПб.: Сб. Материалов XX общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации», СПбГПУ, 2011. - С. 46-47.
8. Баранов В.А. Выявление разладки процесса наблюдений как метод определения вторжения. / В.А. Баранов // СПб.: Сб. Материалов XX общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации», СПбГПУ, 2011. - С. 45-46.
9. Баранов В.А. Модель действий «инсайдера» и его обнаружение. / В.А. Баранов // СПб.: Сб. Материалов XIX общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации», СПбГПУ, 2010. - С. 29-30.