РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 610 395**(13) **C1**

(51) МПК
G06F 21/55 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2015155443, 24.12.2015**

(24) Дата начала отсчета срока действия патента:
24.12.2015

Дата регистрации:
09.02.2017

Приоритет(ы):
(22) Дата подачи заявки: **24.12.2015**

(45) Опубликовано: **09.02.2017** Бюл. № **4**

Адрес для переписки:
127287, Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1, Открытое акционерное общество "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Гайнов Артур Евгеньевич (RU),
Заводцев Илья Валентинович (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2477929 C2, 20.03.2013. US 7647622 B1, 12.01.2010. US 2010/0125911 A1, 20.05.2010. RU 2481633 C2, 10.05.2013. RU 2460122 C1, 27.08.2012. RU 148692 U1, 10.12.2014.**

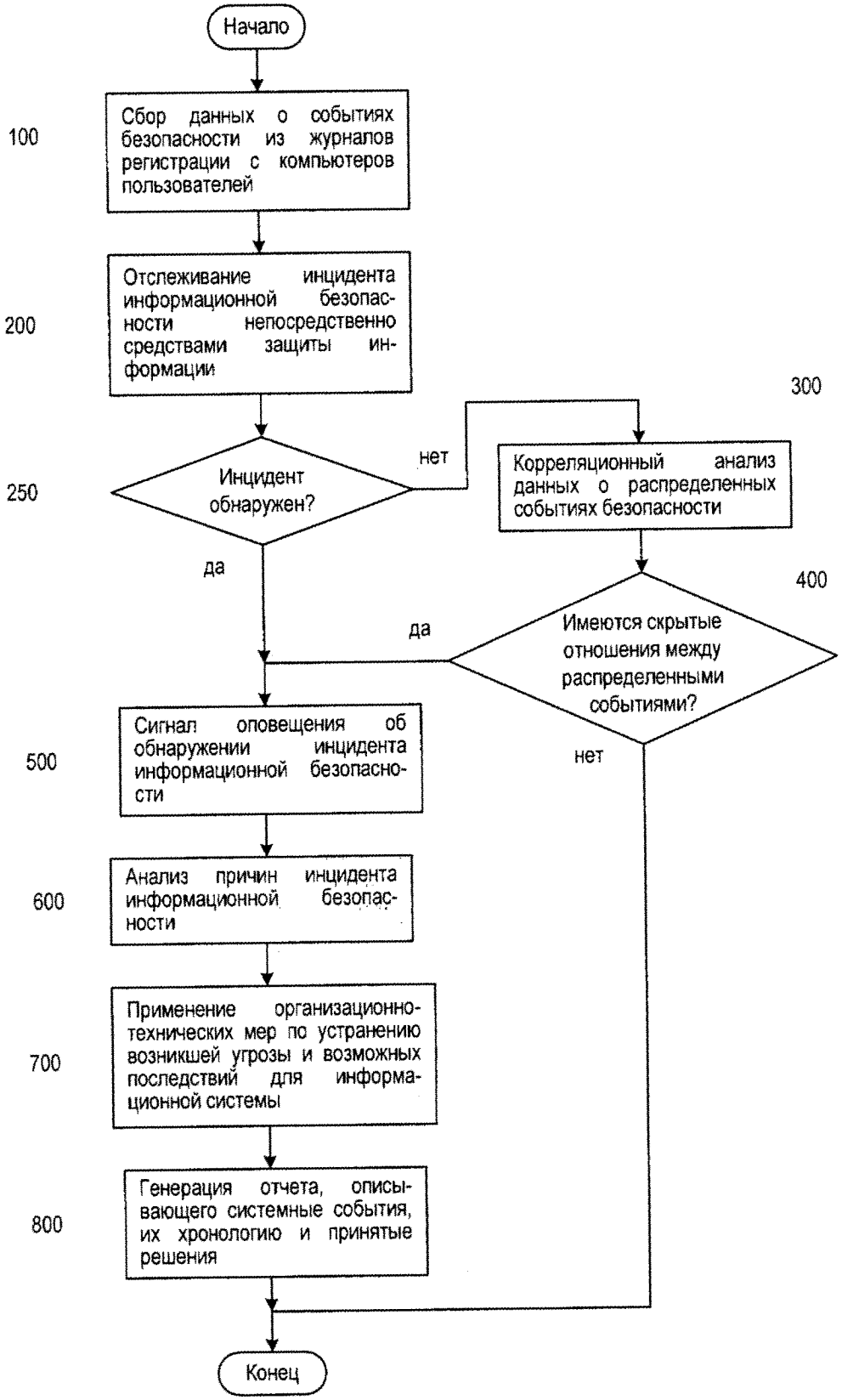
(54) **Способ расследования распределенных событий компьютерной безопасности**

(57) Реферат:

Изобретение относится к области защиты информации в компьютерных системах. Технический результат заключается в снижении количества необнаруженных инцидентов компьютерной безопасности. Предложен способ, в котором загружают данные о системных событиях из всех компьютеров пользователей на сервер безопасности; регистрируют среди этих событий по меньшей мере одно системное событие, вызвавшее инцидент безопасности; анализируют загруженные события путем поиска среди них таких, которые аналогичны событиям, предшествующим уже зарегистрированному инциденту безопасности; проводят корреляционный анализ данных о событиях, распределенных по времени и месту, с использованием дополнительных правил, включающих следующие действия: задают фоновые условия и уровень глубины анализа; формируют исходное множество правил для выполнения корреляционного анализа; производят отбор значимых правил в действующее множество; выявляют и устраняют конфликты среди отобранных правил; проверяют для каждого правила из действующего множества соответствие фактической глубины анализа заданной; проводят поиск и применение решения для устранения последствий и предотвращения инцидента безопасности; формируют отчет об инциденте безопасности. 6 з.п. ф-лы, 4 ил., 2 табл.

RU 2610395 C1

RU 2610395 C1



Фиг. 1

RU 2610395 C1

RU 2610395 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 610 395**(13) **C1**

(51) Int. Cl.
G06F 21/55 (2013.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2015155443, 24.12.2015**

(24) Effective date for property rights:
24.12.2015

Registration date:
09.02.2017

Priority:
(22) Date of filing: **24.12.2015**

(45) Date of publication: **09.02.2017** Bull. № **4**

Mail address:
127287, Moskva, Staryj Petrovsko-Razumovskij pr-d, 1/23, str. 1, Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy"

(72) Inventor(s):
Gajnov Artur Evgenevich (RU),
Zavodtsev Ilya Valentinovich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy" (RU)

RU 2610395 C1

(54) METHOD OF COMPUTER SECURITY DISTRIBUTED EVENTS INVESTIGATION

(57) Abstract:

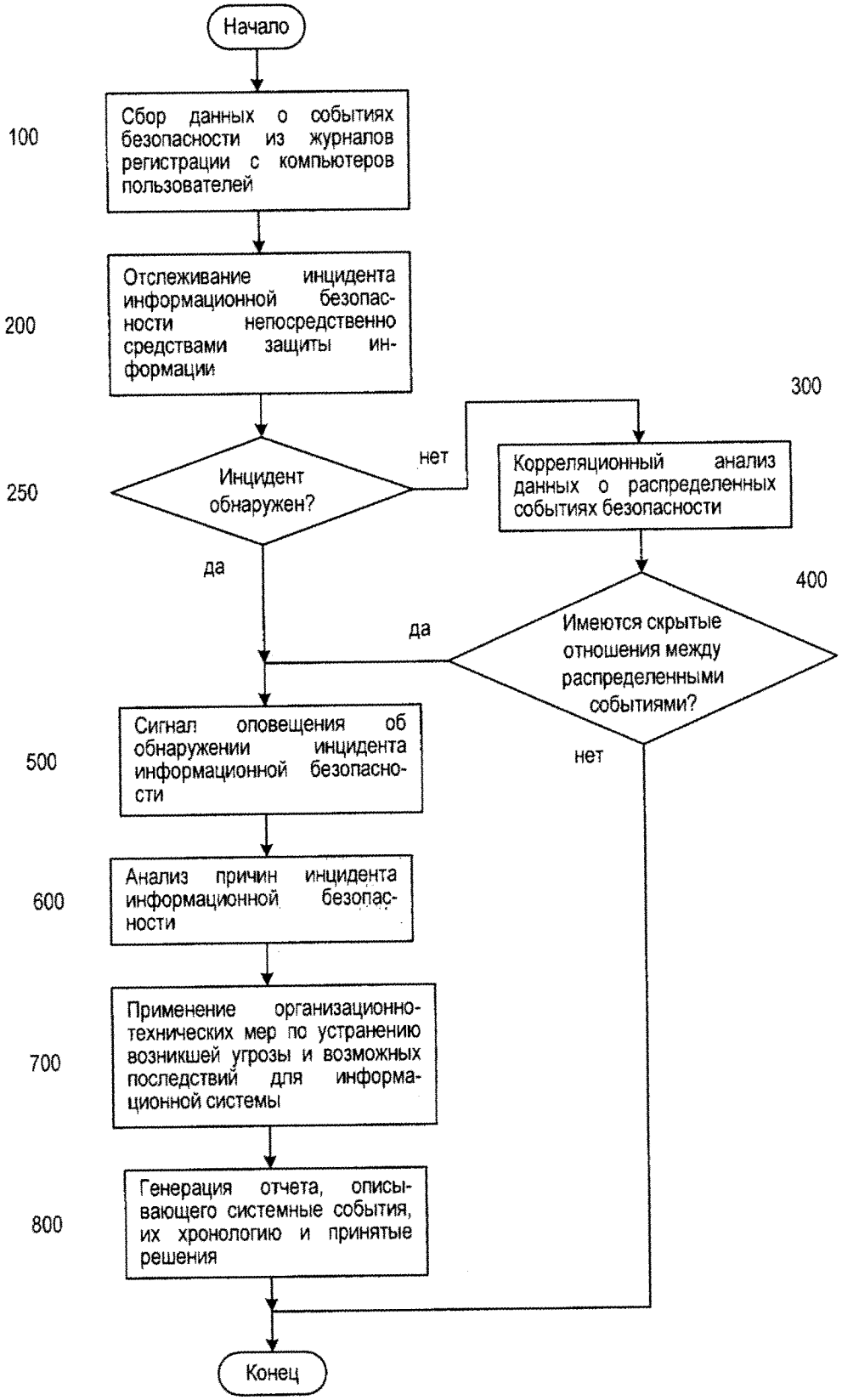
FIELD: information technologies.

SUBSTANCE: invention relates to field of information protecting in computer systems. Disclosed is method, in which loading data on system events from all users computers to security server; among these events recording, at least, one system event, caused safety incident; analyzing loaded events by searching among them of such, which similar to events, preceding to already registered safety incident; performing correlation analysis of event data distributed over time and place, using additional rules, including following actions: setting background conditions and analysis depth level; generating initial plurality of rules to perform correlation analysis; performing significant rules selection into active plurality; detecting and eliminating conflicts among selected rules; checking for each of active plurality rule for conformity of actual analysis depth to specified; performing search and application of solution for elimination of consequences and safety incident prevention; generating security incident report.

EFFECT: technical result consists in reduction of number of undetected computer security incidents.

7 cl, 4 dwg, 2 tbl

RU 2610395 C1



Фиг. 1

RU 2610395 C1

Область техники, к которой относится изобретение

Предполагаемое изобретение относится к области защиты информации в компьютерных системах и может быть использовано для обнаружения и расследования распределенных событий компьютерной безопасности, носящих деструктивных характер.

Уровень техники

Известен способ прогнозирования и предотвращения инцидентов безопасности на основании рейтингов опасности пользователей [1], в котором сокращение числа инцидентов безопасности в вычислительных системах достигается за счет определения значений параметров безопасности пользователей, характеризующих его атрибуты и действия, а также принадлежащие ему информационные связи, с последующим расчетом рисков информационной безопасности (ИБ) для всех событий, отражающих работу пользователя, и поиском возможных решений по снижению таких рисков.

Для этого выполняется сбор информации о событиях, составляющих инцидент безопасности, путем передачи с компьютеров пользователей на сервер данных из системных журналов и журналов событий, данных о существующих (созданных) профилях пользователей и другой информации, характеризующей возможные действия пользователей при работе на своем компьютере. Затем выполняется сортировка, подсчет, сопоставление числовых значений для каждой категории данных, и на основании их рассчитываются рейтинги (профили) для каждого признака, отражающего возможные риски.

Полученные расчетные значения рисков в дальнейшем используются для прогноза возникновения инцидентов и поиска возможных решений по снижению таких рисков, тем самым способствуя предотвращению инцидентов компьютерной безопасности.

Недостатком данного способа является отсутствие процедуры выявления взаимосвязей между разнородными событиями, что не позволяет использовать данный способ для обнаружения и расследования распределенных по времени и месту инцидентов безопасности, хотя многие информационные вторжения представляют собой именно цепочку событий, зачастую неявно связанных между собой.

В известных решениях [2, 3] достижение сокращения числа инцидентов компьютерной безопасности основывается на сборе информации об информационных рисках, связанных с действиями пользователя, и последующем обновлении политики безопасности, тем самым позволяя предотвращать аналогичные инциденты информационной безопасности.

Недостатком данных технологий является использование только данных о состоявшихся событиях, что не позволяет отслеживать текущие события безопасности, способные привести к инциденту.

Наиболее близким по технической сущности к заявленному и принятым за прототип является способ автоматического расследования инцидентов безопасности [4], в котором сокращение числа инцидентов безопасности осуществляется путем исключения повторения системных событий, определенных в качестве причин возникновения инцидентов компьютерной безопасности (нарушение политики безопасности, обнаружение вредоносной программы или некорректная работа средства защиты).

При этом на сервер загружаются данные о системных событиях с компьютерных устройств, подключенных к серверу администрирования, среди которых регистрируется то системное событие, которое привело к инциденту безопасности. Затем загруженные события анализируются на предмет выявления событий, предшествующих выявленному инциденту безопасности, и определяется, по меньшей мере, одно системное событие, являющееся причиной возникновения инцидента. Это позволяет сократить количество

инцидентов безопасности за счет исключения повторения системных событий, определенных в качестве причин возникновения данных инцидентов безопасности, путем принятия решения на изменение соответствующей политики безопасности.

Недостатком данного способа является реализация возможности отслеживания факта инцидента безопасности непосредственно средствами защиты из регистрационных данных только своих журналов или журналов установленной на этой ПЭВМ операционной системы. В способе не оговаривается процедура выявления возможных взаимосвязей между всеми происходящими событиями, влияющими на безопасность компьютера, что не позволяет эффективно идентифицировать инциденты безопасности, состоящие из совокупности распределенных событий безопасности.

Раскрытие изобретения

Техническим результатом является снижение количества необнаруженных инцидентов компьютерной безопасности.

Указанный технический результат достигается тем, что в отличие от известного способа автоматического расследования инцидентов безопасности, где сокращение инцидентов безопасности в информационной системе (ИС) достигается выполнением следующих этапов (фиг. 1):

• загрузки данных о системных событиях со всех компьютерных устройств на сервер администрирования;

• регистрации среди этих событий системного события, вызвавшего инцидент безопасности;

• анализа загруженных событий путем поиска предшествующих инциденту событий;

• определения одного системного события, являющегося причиной возникновения инцидента, авторизованного пользователя и компьютерного устройства, на котором было зафиксировано вызвавшее инцидент событие;

• последующего поиска и принятия решения на изменение политики безопасности с генерацией отчета, описывающего системные события, их хронологию и принятые решения,

дополнительно на этапе анализа загруженных данных о признаках событий выполняют корреляционный анализ этих данных с использованием специальных правил (сигнатур), включающий следующие действия:

• формируют исходное множество правил для выполнения корреляционного анализа;

• задают фоновые условия и уровень глубины анализа для каждого правила;

• производят отбор значимых правил в действующее множество, на основании которых и будет выполняться поиск взаимосвязей между распределенными событиями безопасности;

• выявляют и устраняют конфликты во вновь сформированном множестве;

• проверяют для каждого правила из действующего множества соответствие фактической глубины анализа заданной.

Сопоставительный анализ заявляемого решения с прототипом показывает, что предлагаемый способ отличается от известного введением отдельного этапа выявления корреляционных связей между признаками фиксируемых событий безопасности, на основе данных, полученных из всех журналов регистрации, как базовых средств, установленных на ПЭВМ, так и дополнительных средств защиты, а также специальной процедурой отбора для корреляции только значимых правил и устранения возможных конфликтов между ними.

Благодаря новой совокупности существенных признаков в способе реализована возможность расширения спектра обнаруживаемых инцидентов компьютерной

безопасности путем расследования не только простых событий деструктивного характера, но и составных, включающих разнесенные по времени и по месту события безопасности.

При этом эффективность выявления корреляционных связей между распределенными событиями обеспечивается формированием специального множества значимых правил корреляции, и реализованными в нем возможностями разрешения конфликтов при отборе таких правил.

Когда в вычислительной сети происходят некоторые события безопасности, которые могут нарушать политику безопасности и возможно являются угрозой для информации ПК и компьютерной сети в целом, установленные на компьютерах пользователей средства защиты выявляют и отслеживают инциденты безопасности. А специализированные программные агенты передают зафиксированные в журналах регистрации (лог-журналах) данные об этих событиях на сервер безопасности, который содержит:

- средство сбора данных, выполненное с возможностью загрузки данных о системных событиях, фиксируемых на компьютерах пользователей, при этом средство сбора данных связано со средством анализа инцидентов;
- средство регистрации инцидентов, выполненное с возможностью выделения, по меньшей мере, одного системного события из загруженных данных, вызвавшего инцидент безопасности, при этом средство регистрации инцидентов связано со средством анализа инцидентов и средством сбора данных;
- средство анализа инцидентов, выполненное с возможностью:
  - определения компьютера, на котором было зафиксировано событие, вызвавшее инцидент безопасности;
  - определения пользователя, авторизованного на компьютере пользователя;
  - поиска событий, предшествующих зарегистрированному инциденту безопасности;
  - определения, по меньшей мере, одного системного события, являющегося причиной возникновения инцидента;
- средство поиска решений, выполненное с возможностью поиска решения для устранения последствий и предотвращения повторений события, соответствующего зарегистрированному инциденту безопасности, при этом средство поиска решений связано со средством анализа инцидентов;
- средство создания отчетов, предназначенное для генерации отчета, содержащего, по меньшей мере, описание системных событий, взаимосвязь событий, хронологию событий, найденные решения и примененные решения.

На первом этапе (фиг. 1) со всех компьютерных устройств собирают данные о регистрируемых событиях безопасности (элемент с номером 100 на фиг. 1; далее ссылки на элементы рисунков указаны в обычных скобках). При этом элементарным событием безопасности считают единичную запись в журнале регистрации, содержащую полный набор данных о совершенном в компьютере действии, например, перехвате команд, функций (API-функций), чтении памяти и файлов, программ и любого другого возможного действия с объектами операционной и файловой систем. Под признаками события безопасности понимают тот набор данных из журналов регистрации, который однозначно идентифицирует тот или иной результат элементарного действия (процесса), служащего основой данного события безопасности (например, результат аутентификации пользователя, факт изменения прав доступа к файлу и др.).

Источниками информации для анализа выступают лог-журналы различных компонент ИС: операционных систем, прикладного и общего программного

обеспечения, а также средств защиты информации и др. Собираемые данные включают: записи программных и системных журналов (отчетов), которые ведут регистрацию действий пользователей, запросов программ, сетевых запросов и т.д.

Так как большинство лог-журналов имеют различный формат, то осуществляют приведение данных к единому виду агентом сбора данных, который представляет собой специализированное ПО, отдельно устанавливаемое на нужный хост (АРМ) и в режиме реального времени осуществляющее считывание из журналов релевантной информации. При этом выполняют нормализацию данных, т.е. перекодирование каждой текстовой строки журнала в бинарный вид, разделяя данные на две группы:

- в первую группу относятся признаки событий;
- во вторую - записи, которые несут в себе информацию о каком-либо внешнем действии: со стороны пользователя или системы.

Кроме того, все собираемые данные из журналов регистрации разбивают на категории, для каждой из которых определяют уровень приоритета. Это необходимо для привязки конкретного события безопасности к моделям защищенности ИС и уязвимостей ПО и определения весовых коэффициентов каждого признака, описывающего это событие.

На втором этапе (200) установленные в ИС средства защиты информации выявляют и отслеживают совокупности признаков происходящих в ИС локальных событий безопасности, способных составить инцидент безопасности.

Если средствами защиты информации на данном этапе среди произошедших в ИС локальных событий безопасности инцидент безопасности не идентифицирован (250), то на следующем этапе (300) дополнительно проводят процедуру корреляционного анализа данных по признакам распределенных событий безопасности. На этом этапе с помощью средства анализа инцидентов выполняют исследование регистрационных данных на предмет наличия скрытых отношений между разнородными событиями безопасности.

Это позволяет обнаруживать инциденты, состоящие из нескольких распределенных событий, в том числе, и происходившими в разное время и на разных узлах ИС. Временной период, за который проводится ретроспективный анализ данных, выбирает администратор безопасности. Например, злоумышленник в текущий момент пытается осуществлять инкрементное копирование базы данных с конфиденциальной информацией, при условии, что полную базу он уже скопировал заранее. Следовательно, в этом случае задаваемый временной интервал анализ целесообразно увеличить до нескольких недель или месяцев.

Таким образом, включение в способ расследования распределенных событий компьютерной безопасности процедуры корреляции позволяет обнаруживать скрытые отношения между распределенными событиями безопасности, имеющими единое целеполагание [5], например:

- атака со скомпрометированного узла;
- атака с одного узла на множество;
- распределенная DoS-атака;
- попытки установить соединение по закрытым портам.

В качестве основы для процедуры корреляции возможно использование сигнатурных методов (на основе задания правил) [6, 7]. В частности, RBR-метод (rule-based reasoning), в котором взаимосвязи между признаками событий и инцидентов безопасности определяются аналитиками в заранее заданных специфических правилах. При этом правила корреляции определяют, как отношения (сигнатуру) вида «условие-действие»,

что делает данный метод простым для реализации и сходным с привычной конструкцией «если - то». Для описания сигнатур в правилах корреляции используют структуру XML-директив, которые могут содержать несколько, возможно вложенных, правил.

Анализ данных с использованием сигнатурного метода корреляции можно представить следующим образом. После формирования действующего множества правил корреляции осуществляют последовательную проверку собранных агентами сбора данных из журналов регистрации. Для этого каждое правило загружают в память средства анализа инцидентов и сравнивают сигнатуру, описываемую этим правилом, с текущими данными, собранными с агентов сбора. Так, если произошло событие А (группа событий), т.е. среди зарегистрированных данных идентифицированы его признаки или совокупность признаков, а также выполнены фоновые условия для этого правила, тогда выполняют директиву В, которая может различного вида:

- добавить к обработке новое событие;
- произвести проверку некоторой части ИС;
- собирать дополнительные данные о регистрируемых событиях безопасности;
- сгенерировать сигнал оповещения об опасности.

Каждое новое событие сопоставляется со всеми директивами, и таким образом может генерироваться не одна тревога.

В случае совпадения только одного из признаков события безопасности, включают счетчик, который подсчитывает количество совершаемых однотипных событий. Счетчик предназначен для подсчета количества совпадений по одному и тому же правилу (признаку) на заданную глубину анализа. Например, пять попыток неудачного входа в операционную систему от имени одной учетной записи в течение пяти минут - инцидент.

Если совпадений не выявлено, загружают поочередно последующие правила и проверяют их сигнатуры на совпадение с анализируемыми данными.

Хотя задание правил обычно реализуется на интуитивно понятном уровне, выработка корректного набора правил по отношению к конкретной задаче достаточно затруднительна. Это связано с субъективностью задания правил администратором безопасности, необходимостью учета в разрабатываемых им правилах различных фоновых условий, а также невозможностью применять с прежней эффективностью готовые правила при возникновении новой (нестандартной) ситуации в ИС. При этом администратор безопасности должен описать столько правил (сигнатур), сколько необходимо для эффективной работы средства анализа, но количество случайных событий в ИС огромно, а количество возможных инцидентов постоянно растет. Все это приводит к конфликтам внутри самого множества правил, когда при последовательной обработке правил могут выдаваться незапланированные директивы, появляться пропуски или, наоборот, управляющий алгоритм будет попадать в петлю.

Поэтому в предлагаемом способе применяют дополнительные действия:

- задают фоновые условия и исходный уровень глубины выполняемого анализа правилами;
- формируют исходное множество правил для выполнения корреляционного анализа;
- производят отбор значимых правил в действующее множество;
- выявляют и устраняют конфликты среди отобранных правил;
- проверяют для каждого правила из действующего множества соответствие фактической глубины анализа заданной.

В качестве фоновых условий определяют обстоятельства, влияющие на учет (рассмотрение) тех или иных признаков событий безопасности при проверке правил корреляции. Каждому из фоновых условий администратор безопасности присваивает

коэффициент уверенности CF_i, $i = \overline{0,1}$.

Например, на компьютере пользователя существует учетная запись «Гость (Guest)», что позволяет в обычных условиях злоумышленнику обходить штатную систему разграничения доступа. Однако, на практике, данное фоновое условие может иметь высокий или низкий коэффициент уверенности, в зависимости от того, эта учетная запись разрешена (enable) - коэффициент уверенности $CF_i=1$, или запрещена (disable), тогда коэффициент уверенности $CF_i=0$, соответственно.

Примером набора фоновых условий может служить применение на сетевом устройстве (сервере) операционной системы Linux (коэффициент уверенности $CF_1=0,1$) с командным интерпретатором bash (коэффициент уверенности $CF_2=0,2$). При чем, если используется интерпретатор bash с версией 4.2 и 4.3 (коэффициент уверенности $CF_3=0,3$), а в ОС отсутствует соответствующий ему патч (коэффициент уверенности $CF_4=0,4$), то общий коэффициент уверенности CF_S для этого набора фоновых условий составит

$CF_S=CF_1+CF_2+CF_3+CF_4=1$,

в противном случае, при изменении любого из фоновых условий, соответствующий ему коэффициент уверенности CF_i устанавливается равным 0. В данном примере максимальный вес всех коэффициентов уверенности имеет CF_4, так как именно он оказывает самое существенное влияние возможность эксплуатации злоумышленником уязвимости CVE: 2014-6278. Фоновые условия, также как и признаки включаются в структуру правила (сигнатуру).

Кроме фоновых условий для каждого правила задают параметр глубины анализа $H_i = \langle T_i, V_i \rangle$, определяющий временной интервал T в течение которого с указанного источника данных собирается информация о событиях безопасности, и объем данных V, содержащий информацию об этих событиях. Использование параметра глубины анализа основано на той теоретической предпосылке, что одно событие, происходящее в течение определенного временного промежутка, может являться причиной другого события.

Как правило, единица измерения временного интервала T составляет 1 минуту, а типовой временной интервал сбора данных составляет 1 сутки. Ограничение временного интервала связано со следующим: около 70% правил корреляции работают с событиями, которые произошли в течение суток, 20% - до одной недели, 5% - не более месяца. Оставшиеся - в интервале квартал или полгода.

Объем данных V для правила определяется количеством значимых полей из журналов регистрации этого источника, используемых для корреляционного анализа признаков распределенных событий безопасности. На начальном этапе V задают минимального размера. Например, анализ данных из журнала безопасности операционной системы Windows 7 обычно имеет $V_i=2$ (табл. 1), что зачастую достаточно для анализа локальных инцидентов.

Таблица 1

№ п/п	Используемые поля из log-журнала (объем данных, V)	
	Код события	Ключевые слова
1	4624, Logon	Аудит успеха
2	4768, Account Logon	Kerberos Ticket Events
3	4688, Detailed Tracking	Process Creation

Это связано с тем, что в среднестатистической системе аудита нормальным считается поток событий равный 8000-10000 событий в секунду (Event per Second, EPS), при этом общее количество данных от 50-80 источников с учетом разных типов событий и набора учитываемых полей может достигать десятков тысяч EPS, что оказывает существенную нагрузку на систему.

В то же время для выявления распределенных инцидентов безопасности зачастую необходимо рассматривать расширенный состав полей журналов регистрации, и объем данных может быть существенно увеличен, например, до V=5 (табл. 2).

Таблица 2

Используемые поля из log-журнала (объем данных, V)				
Код события	Ключевые слова	Системное время	Пользователь	ID процесса
4672, Special Logon	Аудит успеха	2015-10-12T07:06:49.816368900Z	S-1-5-18	940

Параметр H для всех правил задается администратором безопасности. Основная цель - определить средние значения количества данных о распределенных событиях безопасности, которые необходимо получать для анализа от разных источников в различные временные интервалы (рабочий день, ночь, выходные и т.д.).

При необходимости на дальнейших этапах обработки данных глубина анализа для каждого правила может быть увеличена вплоть до максимальных значений, определяемых наибольшим количеством полей в журналах регистрации и наибольшим периодом времени за который отслеживаются события безопасности в ИС.

В процедуре формирования значимого множества правил корреляции (фиг. 2) на этапе развертывания системы защиты администратор по безопасности, исходя из своих знаний, задает исходное множество правил для выявления признаков деструктивных событий безопасности. Для этого формируют первоначальный список правил корреляции, содержащих совокупность возможных признаков (p) обнаруживаемого события или совокупности нескольких событий безопасности (310).

В общем случае, правила корреляции строятся на основе закономерностей и представляют собой выражения в виде

$B=A_1$ AND…AND A_n,

где $A_1 \ldots A_n$, B - предикаты,

при этом предикат B является целевой (THEN ACTION) частью, A_1 AND…AND A_n - условной (IF) частью, объединяющей признаки различных событий (совокупности событий) и фоновые условия для данной ИС.

При формировании правила используют булевы операторы (AND, OR, NOT).

Формирование правил исходного множества осуществляется администратором безопасности на основе информации о структуре и составе защищаемой информационной

системы, используемых в ней операционных системах, прикладном программном обеспечении и средствах защиты информации, т.е. о тех элементах, с которых будет вестись сбор данных. При этом могут быть использованы типовые правила корреляции, в том числе и разработанные ранее.

В качестве признаков событий безопасности, подлежащих обнаружению, определяют признаки тех событий, которые влияют на общую защищенность всей информационной системы или отдельного ее элемента. Например, к учитываемым в правилах корреляции событиям безопасности относят данные:

- о попытках изменения полномочий учетных записей;
- о входе одного пользователя под разными учетными записями;
- о превышении среднего времени соединения между узлами;
- о большом количестве узлов в сети организации, пытающихся соединится с одним и тем же внешним ресурсом.

В исходное (начальное) множество включают правила трех видов.

1. Правила, которые описывают признаки инцидента безопасности, состоящего из одиночного события безопасности. Например, правило осуществляет выдачу сигнала об опасности, если выполнена остановка (пауза) критичной службы, на отслеживаемом сервере:

Alert Event1 = device action {stoppet, paused}

AND matches filter {Windows/System Services and Auditing/Critical Services}

OR device vendor {Microsoft}, EventID {7036},

где *stoppet, paused* – признак полной или частичной остановки контролируемого сервиса;

Windows/System Services and Auditing/Critical Services – признак выявления совпадения с сервисом, который поставлен на контроль;

device vendor {Microsoft}, EventID {7036} – признак, указывающий на успешное завершение действия (переход в другое состояние) с учетом фонового условия, т.е. действие подлежит обязательному контролю, если работа ведется в среде ОС *Windows*.

2. Правила, которые описывают признаки инцидента безопасности, состоящего из нескольких последовательных событий безопасности, произошедших за определенный период времени. Например, если получают сигнал от средства антивирусной защиты и выявляют последующее сканирование сети с того устройства (хоста), на котором сработал антивирус. Чтобы идентифицировать такой инцидент безопасности, включающий распределенные события безопасности, в формируемом правиле необходимо связать признаки сканирования сети и обнаружения вируса:

Alert Event2 = select current_timestamp {'Critical' severity}, host_virus.host_ip

AND host_scan {src_ip = host_virus.host_ip}

AND timer: within {1 minute},

где *'Critical' severity* – признак срабатывания средства антивирусной защиты;

src_ip = host_virus.host_ip – признак выявления совпадения между инфицированным вирусом хостом, и АРМ, осуществляющим сканирование сети;

timer: within {1 minute} – признак учета временного интервала, в течение которого, после инфицирования хоста, может начаться процесс сканирования ЛВС.

3. Правила, которые идентифицируют признаки инцидента безопасности на основе выявления отклонений (аномалий) от средних значений активности того или иного устройства (программы) за определенный период времени. Например, правило отслеживает превышение среднего показателя срабатываний антивируса за квартал:

Alert Event3 = Current_Infected_Hosts {Host_Count_Threshold}

OR Current_Virus_Count {Virus_Count_Threshold},

где *Host_Count_Threshold* – признак, показывающий текущее значение «среднего показателя» срабатываний антивируса за квартал;

Virus_Count_ Threshold – признак, определяющий заданное администратором безопасности на основе статистики за предыдущие периоды среднее значение этого показателя.

На следующем шаге из исходного множества производят отбор значимых правил в действующее множество, на основании которых и будет выполняться поиск взаимосвязей между признаками событий безопасности.

Для этого выполняют оценку (311) количества правил в исходном множестве. Если в списке только одно правило, то для него сразу вычисляют (312) оценку Q, отражающую степень учета признаков события безопасности именно этим правилом

$$Q_i = \frac{p_i}{\sum_{i=1}^{n} p_i} \cdot \sum_{k=1}^{p_i} w_k^i \cdot CF_S^i ,$$

где n - общее количество правил корреляций, включенных в действующее множество;

m - общее количество признаков событий безопасности, учитываемых правилами из действующего множества;

p_i - количество признаков событий безопасности, учитываемых i-м правилом;

w_k^i - весовой коэффициент k-го признака, учитываемого i-м правилом;

CF_S^i - суммарный коэффициент уверенности для всех учитываемых правилом фоновых условий;

причем $\sum_{k=1}^{m} w_k = 1,\ i = \overrightarrow{0, n},\ k = \overrightarrow{0, m}$

Весовые коэффициенты признаков w_k^i определяются заранее экспертным методом при составлении правил администратором безопасности в зависимости от используемых моделей защищенности ИС и описаний уязвимостей программного обеспечения. Таким образом, чем большее количество признаков учитывает конкретное правило, и чем они значимее, тем более весомую оценку Q будет иметь данное правило.

Если в список включено несколько правил, то аналогичную оценку Q вычисляют для каждого из них (313), но для последующего отбора (318) выбирают правило (314), обладающее наивысшей оценкой среди проверяемых правил

$Q_i=\max(Q_1, \ldots, Q_n)$

Остальные правила дополнительно проверяют (315) на наличие фактического учета в сигнатуре правила фоновых условий. Если в правиле использованы фоновые условия, то их проверяют (316) на корректность и полноту описания для данной ИС. В случае неполноты учета требуемых фоновых условий сигнатурой правила, производят подключение дополнительных фоновых условий (317) и повторное вычисление (312) оценки Q. Подключение дополнительных фоновых условий осуществляет администратор безопасности экспертным методом.

Однако, некоторые правила могут включать в себя небольшое количество признаков, что может быть обусловлено как особенностью самой сигнатуры расследуемого события безопасности, так и малозначимостью самого правила. В последнем случае это приводит к необоснованному увеличению общего объема правил и, как следствие, снижению скорости анализа данных.

Поэтому для уменьшения в сформированном множестве количества малозначимых правил оценку всех отобранных правил Q дополнительно сравнивают (318) с пороговым уровнем $Q_{порог}$. Задание пороговой оценки производится администратором безопасности в пределах 40-70% от уровня максимально возможного значения (Q_{max}), что позволяет ограничить рост потребляемой памяти - ведь каждое анализируемая сигнатура события безопасности требует порождения отдельного процесса для своего обслуживания.

Также с пороговым уровнем сравнивают оценку правил, если их сигнатура вообще не требует использования фоновых условий (315) или уже корректно учитывает все требуемые для данной ИС фоновые условия (316).

При удовлетворении, оценкой степени учета признаков события безопасности для i-го правила корреляции заданному требованию (318), его включают в действующее множество правил (319), в противном случае удаляют из исходного множества (320). На следующем этапе между отобранными из исходного множества правил корреляции выявляют и устраняют возможные конфликты (фиг. 3). Это связано с необходимостью нивелирования субъективности администратора по безопасности при задании правил, а также для отбора в множество наиболее эффективных правил из числа сформированных ранее с учетом изменения конфигурации и структуры ИС.

Для этого из полученного после оценки учета признаков множества (319) выбирают те правила (331), которые одновременно содержат «одинаковые» признаки деструктивного события или совокупности событий безопасности, и формируют

конфликтное множество правил (332).

Для каждого i-го правила конфликтного множества оценивают (333) коэффициент «новизны» Z_i, отражающий близость признаков событий безопасности, рассматриваемых этим правилом, к признакам, учитываемых всеми другими правилами из этого множества. Для этого вычисляют произведение попарных коэффициентов совпадений признаков i-го правила с признаками каждого из l правил, включенных в конфликтное множество

$$Z_i = \prod_{j=1}^{l} \frac{2 p_{(j,i)}^{сов}}{p_i + p_j},$$

где p_i, p_j - количество признаков событий безопасности, учитываемых i-м и j-м правилом, соответственно,

$p_{(j,i)}^{сов}$ - количество совпадающих признаков, включенных одновременно в j-е и i-е правила корреляции,

l - количество правил корреляций, отобранных в конфликтное множество;

$j = \overline{0, l}$

Чем выше у правила значение коэффициента Z, тем больше в нем учитываемых признаков совпадает признаками, учитываемыми другими правилами. Приоритет отдают (334) правилам с наивысшим значением коэффициента Z, - эти правила доминируют над остальными и сохраняются в формируемом множестве (335).

В случае несоответствия правила данному требованию или когда несколько правил имеют равный приоритет (337), осуществляют сравнение (339) правил по критерию «специфики» S_i, отражающему количество признаков событий безопасности, загружаемых в рабочую память для проверки:

$$S_i = \frac{p_i}{\max(p_1, \ldots, p_n)},$$

где p_i - количество признаков событий безопасности, учитываемых i-м правилом,

$\max(p_1, \ldots, p_n)$ - наибольшее количество признаков, учитываемых одним из правил, входящим в действующее множество.

Здесь предпочтение отдают тому правилу, применение которого требует проверки наибольшего количества признаков событий безопасности (340), остальные правила удаляются из множества (338). Из отобранных правил формируют действующее (бесконфликтное) множество правил корреляции (336).

После устранения конфликтов в сформированном множестве осуществляют корректировку фактического значения глубины анализа H для всех его правил (фиг. 4). Так как параметр H задается администратором безопасности и определяет средние значения количества данных о распределенных событиях безопасности, получаемых для анализа от разных источников в различные временные интервалы, то такая процедура позволяет администратору безопасности контролировать и, при необходимости, уточнять приоритеты в расследовании распределенных событий компьютерной безопасности и, следовательно, повысить уверенность в обнаружении инцидентов ИБ.

На этом этапе выполняют проверку (341) фактического значения глубины анализа

H_i для i-го правила. Если правило имеет глубину анализа соответствующую заданному уровню (342), то его включают в действующее множество правил корреляции. Если проверяемое правило имеет глубину анализа менее заданного уровня, администратором безопасности увеличивается глубина анализа на один шаг $H_i + 1 = \langle T_i + 1\,\text{мин}, V_i + 1 \rangle$ и повторяют проверку (341) фактического значения глубины анализа H_i. При необходимости на дальнейших этапах обработки данных глубина анализа для каждого правила может увеличиваться вплоть до максимальных значений.

Затем (фиг. 1) для проведения корреляционного анализа данных случайным равновероятным способом из всего действующего множества правил выбирают одно значимое правило и проверяют взаимосвязанность признаков событий (300) как в пределах одного набора данных, так и из различных (в том числе и временных) наборов. Если обнаружены скрытые отношения между распределенными событиями безопасности (400), выдают сигнал оповещения об обнаружении инцидента информационной безопасности (500).

Если при проведении корреляционного анализа данных взаимосвязанность событий не выявлена, то применяют следующее правило корреляции из значимого множества.

После того как инцидент обнаружен производят анализ причин инцидента безопасности (600). Определяют данные, связанные с инцидентом: компьютерные и активные сетевые устройства, на котором были зафиксированы события, вызвавшие инцидент безопасности, и пользователь, авторизованный на данном компьютерном устройстве.

Таким образом, дополнительное применение корреляционного анализа позволяет на основе сформированного множества правил выявлять причинные, дополняющие, параллельные или взаимосвязанные отношения между различными событиями безопасности, производимыми с целью попыток несанкционированного доступа к защищаемым информационным ресурсам ИС либо нападения на них, тем самым снижая количество необнаруженных с помощью других способов инцидентов компьютерной безопасности. А введенные специализированные процедуры: отбора значимых правил, выявления и устранения конфликтов среди отобранных правил, а также проверки для каждого правила соответствия фактической глубины анализа заданной, позволяют формировать действующее множество значимых правил для данного этапа.

Далее производят поиск и применение решения для устранения последствий и предотвращения события (группы событий), определенного в качестве причины возникновения инцидента безопасности (700).

Решение для устранения последствий и предотвращения инцидента безопасности, соответствующего событию (группе событий), представляет собой, по меньшей мере, одну из мер:

- изменение политики безопасности;
- удаление вредоносного кода или резервное восстановление программного обеспечения;
- блокировка действий нарушителя;
- изменение конфигурации средств защиты компьютеров пользователей.

На завершающем этапе могут формировать отчет об инциденте компьютерной безопасности (800), включающий описание самого инцидента и событий, приведших к его возникновению, а также принятых и рекомендуемых мер по защите.

Краткое описание чертежей

На фиг. 1 показана блок-схема способа расследования распределенных событий в информационных системах с отдельным этапом корреляционного анализа данных о распределенных событиях безопасности.

На фиг. 2 показана блок-схема процедуры формирования значимого (действующего) множества правил для процедуры корреляции данных при расследовании распределенных инцидентов информационной безопасности.

На фиг. 3 показана блок-схема процедуры разрешения конфликтов в сформированном множестве правил расследования распределенных событий компьютерной безопасности.

На фиг. 4 показана блок-схема процедуры повышения уверенности в обнаружении инцидентов ИБ.

Осуществление изобретения

Рассмотрим пример реализаций предложенного способа в сетевой информационной системе, включающей сервер безопасности и компьютеры пользователей, а также активное коммутационное оборудование.

В качестве сервера безопасности может быть использован обычный компьютер или компьютер в серверном исполнении, имеющий увеличенный объем оперативной памяти и жесткого диска и серверную операционную систему.

Имеющиеся в составе сервера безопасности средства сбора данных с компьютеров пользователей, анализа событий безопасности, регистрации инцидентов безопасности и поиска решений выполнены программно и представляют собой комплекс прикладного программного обеспечения безопасности (КППОБ), инсталлированный на сервере. КППОБ обеспечивает необходимые функции, требуемые для реализации предложенного способа, и может быть разработано специалистом по программированию (программистом) на основе приведенных сведений о назначении функций.

Имеющиеся в составе компьютеров пользователей агенты сбора данных из журналов регистрации (ОС и средств защиты информации) и передачи их на сервер безопасности также выполнены программно и представляют собой прикладное программное обеспечение (ППО), инсталлированное на компьютер пользователя. ППО обеспечивает необходимые функции, требуемые для реализации предложенного способа, и может быть разработано специалистом по программированию (программистом) на основе приведенных сведений о назначении функций.

Для примера осуществления предложенного способа расследования распределенных событий компьютерной безопасности, рассмотрим применение процедуры корреляции данных для идентификации распределенного (сетевого) инцидента безопасности, основанного на эксплуатации уязвимостей CVE 2014-6271, CVE 2014-6277, CVE 2014-6278, CVE 2014-7169, CVE 2014-7186. Суть уязвимостей заключается в том, что командный интерпретатор bash позволяет задавать внутри себя переменные среды, которые задают определение функций. А после определения функции интерпретатор bash продолжает обрабатывать все команды. Вследствие чего злоумышленник получает возможность осуществить атаку с внедрением деструктивного кода на компьютер под управлением Unix-подобной ОС. Однако, данная атака не фиксируется отдельными средствами защиты информации, так как представляет собой распределенный инцидент безопасности, включая в себя несколько этапов реализации, в явном виде не имеющих внутренних логических связей.

На первом этапе предлагаемого способа расследования распределенных событий компьютерной безопасности для формирования исходного множества правил корреляции необходимо определение фоновых условий с соответствующими коэффициентами уверенности, поэтому в качестве таковых, например, выбирают

следующие:

1. Применение на сетевом устройстве (сервере, хосте) операционной системы Linux (ОС X, Unix и др.), коэффициент уверенности CF_1=0,1.

2. Использование в данной ОС командного интерпретатора bash, коэффициент уверенности CF_2=0,2.

3. Использование командного интерпретатора bash версии 4.2 или 4.3, коэффициент уверенности CF_3=0,3.

4. Отсутствие в установленной ОС патча, устраняющего уязвимость интерпретатора bash, коэффициент уверенности CF_4=0,4.

Далее определяют глубину анализа $H_i = \langle T_i, V_i \rangle$, выполняемого правилами. При этом могут быть выбраны:

временной интервал сбора данных: T=1 мин, так данная атака зачастую выполняется одномоментно, без разнесения во времени, и, следовательно, сразу задавать большую глубину нецелесообразно;

объем данных, получаемых из журналов регистрации ОС Linux (ОС X, Unix и др.), V=5. В зависимости от типа ОС поля соответствующих журналов регистрации могут быть разные, но они должны содержать информацию о выполнении процесса (например, запуск командного интерпретатора bash или изменение полномочий доступа к файлу):

Код события, Ключевые слова, Системное время, Пользователь, ID процесса

Затем формируют (фиг. 2) исходное множество правил (сигнатур) для корреляционного анализа путем задания множества совокупностей признаков распределенных деструктивных событий безопасности, описывающих эксплуатацию уязвимостей (310). В качестве таких признаков (с соответствующими весовыми коэффициентами w_k^i) могут быть определены:

• однократные последовательности символов исполняемого кода:

(1) для поиска уязвимости CVE 2014-6271 – `evn x=' ( ) { :;};` (весовой коэффициент w=0,1);

(2) для поиска уязвимости CVE 2014-7169 – `evn X=' ( ) { (a)=> \ '` (весовой коэффициент w=0,1);

(3) для поиска уязвимости CVE 2014-6277 – `( ) { x() { _; };` или `x( ) { _; } <<a; };` (весовой коэффициент w=0,1);

• многократные повторения

(4) для поиска уязвимости CVE 2014-7186 - символа «EOF» или слова «done» (весовой коэффициент w=0,1).

Кроме того, если инцидент имеет целью атаку на web-сервер, то в качестве признаков могут быть определены дополнительно:

(5) последовательность символов - «`HTTP_COOKIE- '`» (весовой коэффициент w= 0,05);

(6) IP адрес сервера, входящего в защищаемую ИС (весовой коэффициент w=0,05).

Если инцидент осуществляется через внедрение кода с использованием SMTP-протокола, то в качестве признаков могут быть определены дополнительно:

(7) кодовые последовательности - `"mail from:<>" и "rcpt to:<nobody>"` (весовой

коэффициент w=0,1).

Если инцидент безопасности заключается в исполнении активной нагрузки на компьютере пользователя, то в качестве признаков могут быть определены дополнительно сигнатуры команд

(8) на повышение полномочий для исполняемого файла - `chmod ... /var/tmp/fail.x` (весовой коэффициент w=0,2);

(9) на запуск данного файла на исполнение - `/var/tmp/fail.x` (весовой коэффициент w=0,1);

(10) на удаление файла после исполнения - `rm -rf /var/tmp/fail.x` (весовой коэффициент w=0,01).

Правила оформляют в любом формате, удобном для автоматической обработки, например, XML-формате.

Пусть на основе отобранных признаков в исходное множество правил корреляции включено 3 правила.

Правило №1 - типовое, ориентированное на выявление признаков любых событий безопасности, использующих данные уязвимости:

Alert Event1 = признак (1) OR признак (2) OR признак (3) OR признак (4)
AND {фоновое условие (1) AND фоновое условие (2) AND фоновое условие (3)},

глубина анализа $H_1 = \langle T_1 = 1\,\text{мин}, V_1 = 3 \rangle$.

Правило №2 - специализированное, направленное на выявление признаков распределенных событий безопасности, использующих данные уязвимости для заражения web-сервера (в т.ч. посредством почтовых сервисов):

Alert Event2 = признак (1) OR признак (2) OR признак (3)
AND {признак (5) AND признак (6) OR признак (7)}
AND {фоновое условие (1) AND фоновое условие (2) AND фоновое условие (3)},

глубина анализа $H_2 = \langle T_2 = 1\,\text{мин}, V_2 = 3 \rangle$.

Правило №3 - специализированное, направленное на выявление признаков распределенных событий безопасности, использующих данные уязвимости для внедрения и исполнения произвольного кода на компьютере пользователя:

Alert Event3 = признак (1) OR признак (2) OR признак (3) OR признак (4)
AND {признак (6) OR признак (7)} AND {признак (8) AND {признак (9) OR признак (10)}}
AND {фоновое условие (1) AND фоновое условие (2) AND фоновое условие (3)},

глубина анализа $H_3 = \langle T_3 = 1\,\text{мин}, V_3 = 3 \rangle$.

Далее администратором безопасности задается пороговое значение $Q_{порог}$=0,3, а для каждого правила вычисляют оценку Q, отражающую степень учета признаков событий безопасности именно этим правилом: Q_1=0,096, Q_2=0,18, Q_3=0,513.

Правило №3, как обладающее наивысшей оценкой, которая при этом превышает пороговое значение (318), сразу включают в действующее множество правил корреляции

(319).

Для остальных правил проводят проверку фактического учета в сигнатуре фоновых условий (315). В связи с тем, что оба правила (№1 и №2) уже содержат фоновые условия, то их дополнительно проверяют на корректность и полноту (316) описания фоновых условий для данной ИС. По результатам проверки к каждому из правил подключают фоновое условие №4 и повторно вычисляют оценку, отражающую степень учета признаков: Q_1=0,16, Q_2=0,3.

Оценка правила №2 после подключения дополнительного фонового условия, одновременно соответствует и условию (318), поэтому данное правило также включают в действующее множество правил корреляции.

В связи с тем, что оба правила (№2 и №3) содержат «одинаковые» признаки совокупности событий безопасности, из них формируют конфликтное множество правил (332) и оценивают коэффициент «новизны» Z для каждого из них (333). Но правил в конфликтном множестве всего два, поэтому оба имеют равный приоритет: Z_2=0,67, Z_3=0,67. И на следующем этапе осуществляют сравнение этих правил по критерию «специфики» (339): S_2=0,667, S_3=1.

По результатам оценки, отражающей количество признаков событий безопасности, загружаемых в рабочую память, предпочтение отдают правилу №3, а правило №2 удаляют из конфликтного множества (338).

После устранения конфликтов в сформированном множестве для отобранного правила осуществляют корректировку фактического значения глубины анализа H_3 (фиг. 4). Так как правило №3 имеет глубину анализа менее заданного уровня, то администратором безопасности увеличивается глубина анализа (344) на один шаг $H_3 + 1 = \langle T_3, V_3 = 3 + 1 \rangle$, и затем повторяют проверку (341) фактического значения глубины анализа H_3. Цикл повторяют два раза, чтобы достичь заданной глубины анализа $H_{зад}$. После чего правило включается в действующее множество значимых правил корреляции (343).

Основной этап реализации способа осуществляется следующим образом.

Сначала запускается информационная система.

После запуска установленные на компьютерах пользователей и активном сетевом оборудовании средства защиты информации самостоятельно выявляют и отслеживают на основе алгоритмов заложенных в них разработчиками известные им признаки локальных событий безопасности, способных составить инцидент безопасности. Одновременно агенты сбора данных из состава ППО на компьютерах пользователей и активного сетевого оборудования начинают загружать данные о системных событиях со всех компьютеров пользователей, сетевых устройств и средств защиты в средство сбора данных сервера безопасности (например, с использованием протокола Syslog).

Собранные данные предают в средство анализа данных для последующего анализа событий безопасности путем поиска предшествующих инциденту событий.

Все собираемые данные из журналов регистрации приводят к единому виду через нормализацию и разбивают на категории, для каждой из которых определяют уровень приоритета. Это необходимо для привязки конкретного события безопасности к моделям защищенности ИС и уязвим остей программного обеспечения.

В указанном случае (примере) приоритет получат данные из журналов регистрации сетевых средств защиты (межсетевой экран, средство обнаружения вторжений, т.е. анализирующих сетевой трафик), а также операционных систем, установленных на

web-сервере и компьютере пользователя.

Если инцидент безопасности зарегистрирован, то средство защиты информации, идентифицировавшее инцидент, посылает на сервер безопасности сигнал тревоги. А средством анализа событий безопасности из состава КППОБ производят определение одного системного события, являющегося причиной возникновения инцидента, авторизованного пользователя и компьютерного устройства, на котором было зафиксировано вызвавшее инцидент событие. А затем производят последующий поиск и принятие решения на изменение политики безопасности с генерацией отчета, описывающего системные события, их хронологию и принятые решения.

Если средствами защиты информации на данном этапе среди произошедших в ИС локальных событий безопасности инцидент безопасности не идентифицирован, то средством анализа событий безопасности дополнительно проводят процедуру корреляционного анализа собранных данных по правилам, включающим признаки распределенных событий безопасности.

Для этого используют значимое правило (№3), ранее включенное в действующее множество. Указанное правило загружают в память средства анализа инцидентов и сравнивают сигнатуры признаков, содержащиеся в этом правиле, с наборами данных, собранными из журналов регистрации.

В случае совпадения только одного из признаков события безопасности, включают счетчик, который подсчитывает количество совпадений по одному и тому же признаку (например, признак №4) в течение временного периода в соответствии с заданной глубиной анализа. Если за этот период совпадений признаков больше не выявлено счетчик обнуляется. При следующем совпадении счетчик включается вновь.

Если среди зарегистрированных данных идентифицированы все признаки, включенные в сигнатуру правила корреляции, а также выполнены все фоновые условия для этого правила, тогда средство анализа данных посылает сигнал оповещения об опасности.

Если совпадений не выявлено, загружают поочередно последующие правила и проверяют их сигнатуры на совпадение с анализируемыми данными.

После обнаружения распределенного инцидента компьютерной безопасности средством анализа событий безопасности из состава КППОБ производят определение всех системных событий, являющихся причиной возникновения инцидента безопасности, компьютерных устройств, на которых были зафиксированы вызвавшие инцидент события. А затем производят последующий поиск и принятие решения на изменение политики безопасности с генерацией отчета, описывающего системные события, их хронологию и принятые решения.

Следует отметить, что приведенные в описании сведения являются только примерами, которые не ограничивают объем настоящего изобретения, описанной формулой. Специалисту в данной области становится понятным, что могут существовать и другие варианты осуществления настоящего изобретения, согласующиеся с сущностью и объемом настоящего изобретения.

Источники информации

1. Патент РФ №2477929, 2011, МПК G06F 21/30

2. Патент США №7647622, 12.01.2010

3. Заявка США №20100125911, 20.05.2010

4. Патент РФ №2481633, 2009 г. МПК G06F 21/55

5. Kruegel Ch., Valeur F. Intrusion Detection and Correlation. Challenges and Solutions. Springer Science + Business Media, Inc., 2005. ISBN: 0-387-23398-9. [Режим доступа]: http://link.springer.com/book/10.1007%2Fb101493

6. Суслов В.И. Эконометрия, Новосибирск, СО РАН, 2005.

7. Mat Jani, H. Applying case reuse and rule-based reasoning (RBR) in object-oriented application framework documentation: Analysis and design. - Human System Interactions, 2008 Conference, pp. 597-602, ISBN: 978-1-4244-1542-7. [Режим доступа]: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4581508&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4581508

(57) Формула изобретения

1. Способ расследования распределенных событий компьютерной безопасности в информационной системе, включающей сервер безопасности и компьютеры пользователей, причем сервер безопасности содержит:

средство сбора данных, выполненное с возможностью загрузки данных о системных событиях, фиксируемых на компьютерах пользователей, при этом средство сбора данных связано со средством анализа инцидентов;

средство регистрации инцидентов, выполненное с возможностью выделения по меньшей мере одного системного события из загруженных данных, вызвавшего инцидент безопасности, при этом средство регистрации инцидентов связано со средством анализа инцидентов и средством сбора данных;

средство анализа инцидентов, выполненное с возможностью:

определения компьютера, на котором было зафиксировано событие, вызвавшее инцидент безопасности;

определения пользователя, авторизованного на компьютере пользователя;

поиска событий, предшествующих зарегистрированному инциденту безопасности;

определения по меньшей мере одного системного события, являющегося причиной возникновения инцидента;

средство поиска решений, выполненное с возможностью поиска решения для устранения последствий и предотвращения повторений события, соответствующего зарегистрированному инциденту безопасности, при этом средство поиска решений связано со средством анализа инцидентов;

средство создания отчетов, предназначенное для генерации отчета, содержащего по меньшей мере описание системных событий, взаимосвязь событий, хронологию событий, найденные решения и примененные решения;

причем способ заключается в том, что:

загружают данные о системных событиях из всех компьютеров пользователей на сервер безопасности;

регистрируют среди этих событий по меньшей мере одно системное событие, вызвавшее инцидент безопасности;

анализируют загруженные события путем поиска среди них таких, которые аналогичны событиям, предшествующим уже зарегистрированному инциденту безопасности;

проводят корреляционный анализ данных о событиях, распределенных по времени и месту, с использованием дополнительных правил, включающих следующие действия:

задают фоновые условия и уровень глубины анализа;

формируют исходное множество правил для выполнения корреляционного анализа;

производят отбор значимых правил в действующее множество;

выявляют и устраняют конфликты среди отобранных правил;

проверяют для каждого правила из действующего множества соответствие фактической глубины анализа заданной;

проводят поиск и применение решения для устранения последствий и предотвращения инцидента безопасности;

если корреляция между распределенными событиями выявлена, то проводят также поиск и применение решения для устранения последствий и предотвращения события или группы событий, определенных в качестве причины возникновения инцидента безопасности;

формируют отчет об инциденте безопасности, включающий описание самого инцидента и событий, приведших к возникновению инцидента безопасности, а также принятые и рекомендуемые меры.

2. Способ по п. 1, в котором данные о системных событиях, загружаемые с автоматизированных рабочих мест пользователей, хранятся на них в бинарном виде.

3. Способ по п. 1, в котором инцидентом безопасности является по меньшей мере одно из событий:

нарушение политик безопасности;

обнаружение вредоносного кода;

обнаружение несанкционированного доступа к информационным ресурсам;

попытки установить соединение по закрытым портам;

атака со скомпрометированного хоста.

4. Способ по п. 1, в котором дополнительно для проведения корреляционного анализа данных случайным равновероятным способом из всего действующего множества правил выбирают одно значимое правило и с его помощью проверяют взаимосвязь признаков событий как в пределах одного набора данных, так и из различных наборов.

5. Способ по п. 1, в котором, если при проведении корреляционного анализа данных взаимосвязанность событий не выявлена, то применяют следующее правило корреляции из действующего множества.

6. Способ по п. 1, в котором, если при проведении корреляционного анализа данных выявлена взаимосвязь между событиями безопасности, то фиксируют также их связь с возможным инцидентом безопасности.

7. Способ по п. 1, в котором решение для устранения последствий и предотвращения инцидента безопасности, соответствующего событию или группе событий, представляет собой по меньшей мере одну из мер:

изменение политики безопасности;

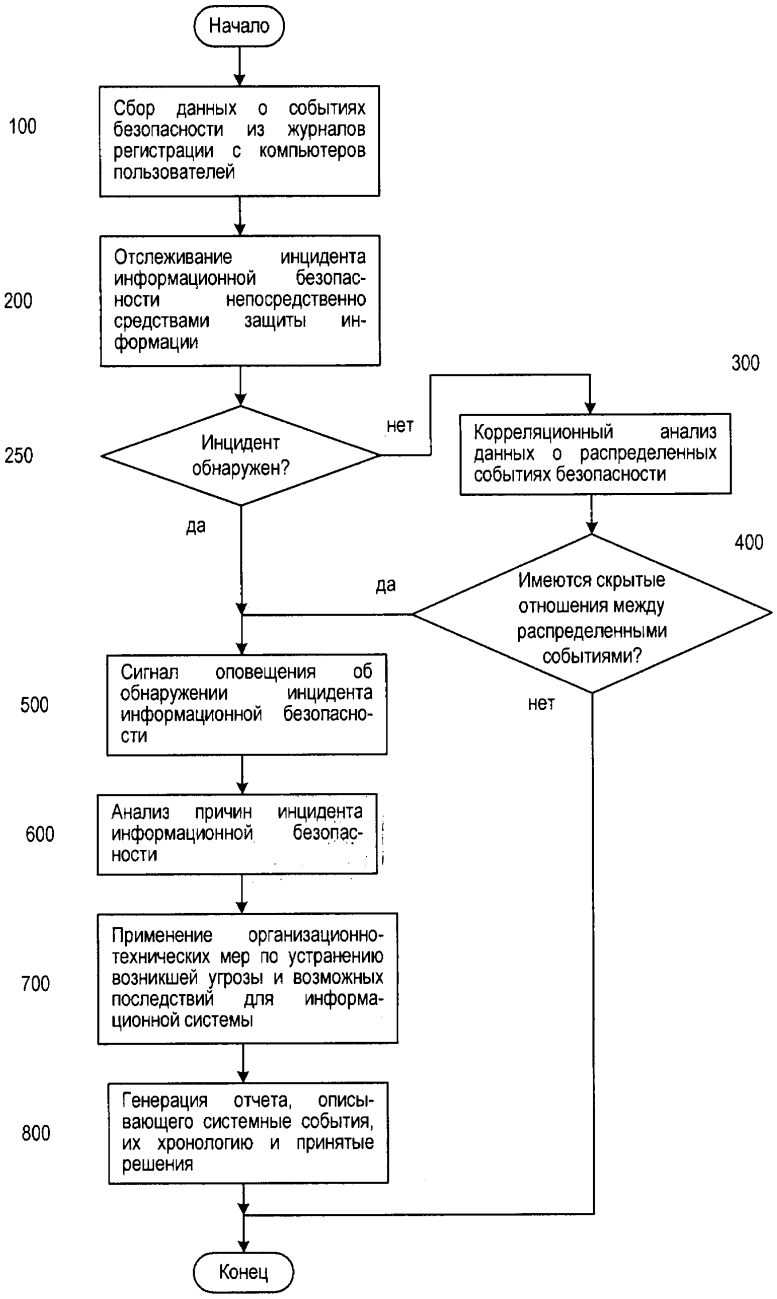
удаление вредоносного кода или резервное восстановление программного обеспечения;

блокировка действий нарушителя;

изменение конфигурации средств защиты на компьютерах пользователей.

1

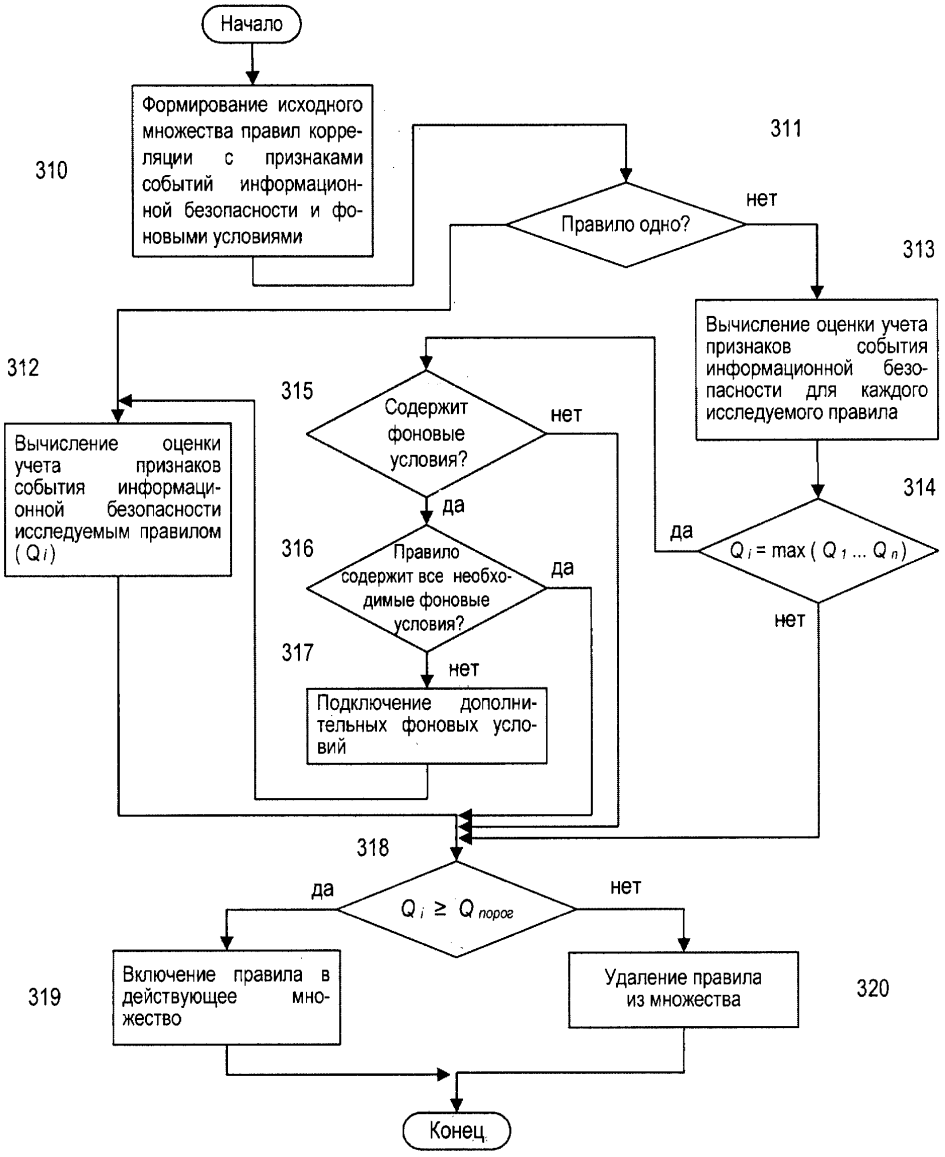
Способ расследования распределенных событий компьютерной безопасности



Фиг. 1

2

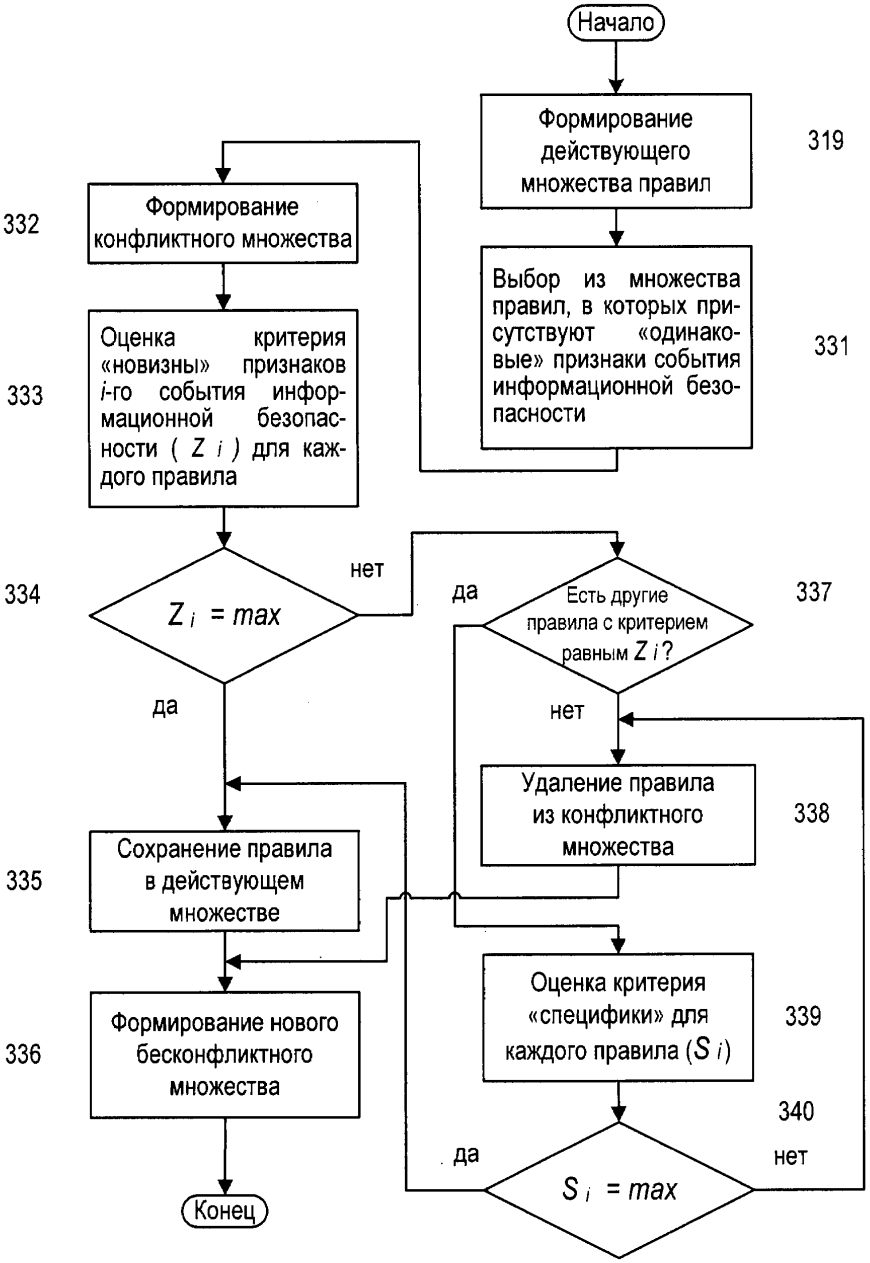
Способ расследования распределенных событий компьютерной безопасности



Фиг. 2

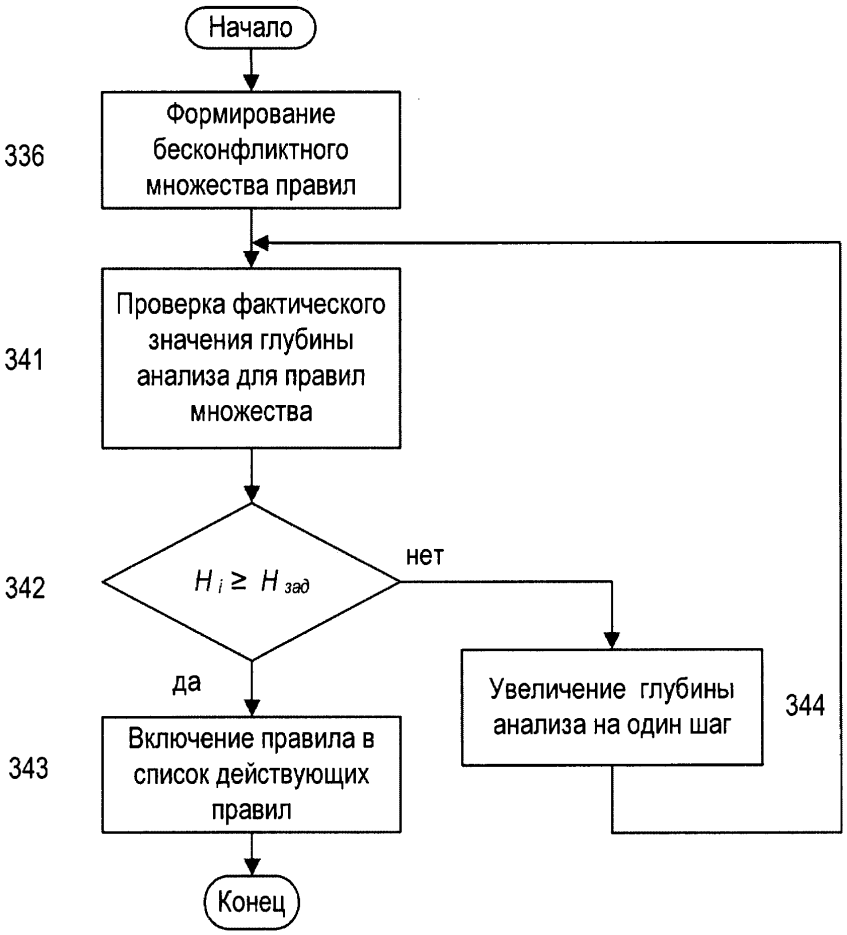
3

Способ расследования распределенных событий компьютерной безопасности



Фиг. 3

Способ расследования распределенных событий компьютерной безопасности



Фиг. 4