РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 481 633** (13) **C2**

(51) МПК
G06F 21/55 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2011132618/08, 04.08.2011**

(24) Дата начала отсчета срока действия патента:
04.08.2011

Приоритет(ы):
(22) Дата подачи заявки: **04.08.2011**

(45) Опубликовано: **10.05.2013** Бюл. № **13**

(56) Список документов, цитированных в отчете о поиске: **RU 96991 U1, 20.08.2010. Н.КУКАНОВА. Управление инцидентами информационной безопасности. Открытые системы. №10, 2006. 28.12.2006. [найдено 15.08.2012], найдено в Интернет по адресу URL: http: //www.osp.ru/ os/2006/l 0/3910101. RU 2390839 C1, 27.05.2010. US 6530024 B1, 04.03.2003. US 2009/0222876 A1, 03.09.2009.**

Адрес для переписки:
123060, Москва, 1-й Волоколамский пр-д, 10, корп.1, ЗАО Лаборатория Касперского, отдел по управлению интеллектуальной собственностью, Н.В. Кащенко

(72) Автор(ы):
Зайцев Олег Владимирович (RU)

(73) Патентообладатель(и):
Закрытое акционерное общество "Лаборатория Касперского" (RU)

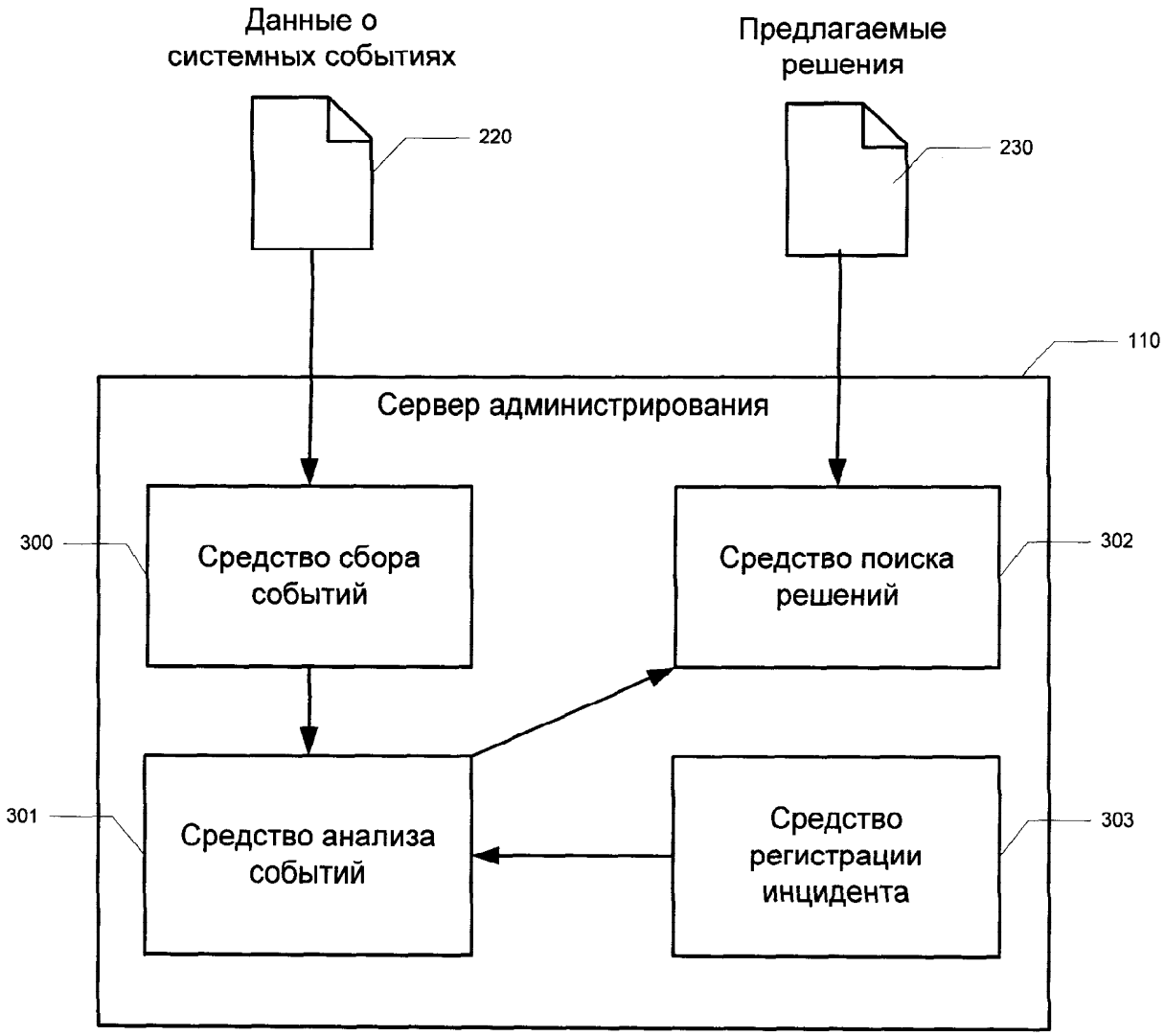
RU 2481633 C2

(54) СИСТЕМА И СПОСОБ АВТОМАТИЧЕСКОГО РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ

(57) Реферат:

Изобретение относится к вычислительной технике. Технический результат заключается в сокращении количества инцидентов безопасности за счет исключения повторения системных событий, определенных в качестве причин возникновения данных инцидентов безопасности. Система автоматического расследования инцидентов безопасности, выполненная в виде сервера администрирования, который содержит средство сбора данных, предназначенное для загрузки с подключенных к серверу администрирования компьютерных устройств данных о системных событиях, фиксируемых в упомянутых компьютерных устройствах; средство регистрации инцидентов, предназначенное для выделения, по меньшей мере, одного системного события из загруженных данных, вызвавшего инцидент безопасности; анализатор инцидентов, предназначенный для поиска событий, предшествующих зарегистрированному инциденту безопасности; определения, по меньшей мере, одного системного события, являющегося причиной возникновения инцидента; средство поиска решений, предназначенное для поиска решения для устранения последствий и предотвращения повторений инцидента безопасности соответствующего событию, определенному анализатором в качестве причины возникновения инцидента. 2 н. и 14 з.п. ф-лы, 9 ил.

RU 2481633 C2



Фиг. 3а

RU 2481633 C2

RU 2481633 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 481 633** (13) **C2**

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

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2011132618/08, 04.08.2011**

(24) Effective date for property rights:
04.08.2011

Priority:
(22) Date of filing: **04.08.2011**

(45) Date of publication: **10.05.2013 Bull. 13**

Mail address:
123060, Moskva, 1-j Volokolamskij pr-d, 10, korp.1, ZAO Laboratorija Kasperskogo, otdel po upravleniju intellektual'noj sobstvennost'ju, N.V. Kashchenko

(72) Inventor(s):
Zajtsev Oleg Vladimirovich (RU)

(73) Proprietor(s):
Zakrytoe aktsionernoe obshchestvo "Laboratorija Kasperskogo" (RU)

(54) SYSTEM AND METHOD FOR AUTOMATIC INVESTIGATION OF SAFETY INCIDENTS

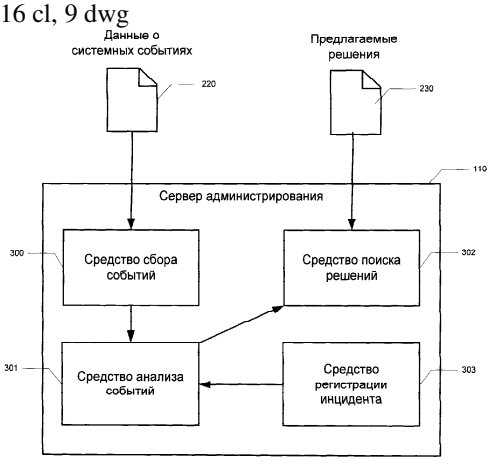
(57) Abstract:

FIELD: information technologies.

SUBSTANCE: system of automatic investigation of safety incidents made in the form of an administration server, which comprises: a data collection facility designed for download of data from computer devices connected to the administration server about system events fixed in the specified computer devices; a facility of incidents registration, intended to separate at least one system event from downloaded data that caused a safety incident; an analyser of incidents designed for: searching for events preceding the registered safety incident; determination of at least one system event, which is the reason for incident occurrence; a facility for solution finding, which is designed to search for a solution to eliminate consequences and to prevent recurrence of the safety incident corresponding to the event determined by the analyser as the reason for the incident occurrence.

EFFECT: reduction of a number of safety incidents due to exclusion of recurrence of system events determined as reasons for occurrence of these safety incidents.

16 cl, 9 dwg



Фиг. 3а

RU 2481633 C2

RU 2481633 C2

Область техники

Настоящее изобретение относится к системам и способам обеспечения информационной безопасности и более конкретно к системам и способам автоматического расследования инцидентов безопасности в компьютерных сетях.

Уровень техники

Безопасность вычислительных сетей и входящих в их состав компьютерных систем приобретает особую важность в корпоративной среде. Утечка информации, хранящейся и обрабатываемой в компьютерной сети компании, может привести к убыткам, не сравнимым с убытками от потери личной информации пользователей. Именно поэтому к системам безопасности компаний предъявляется больше требований, и уровень техники, применимой в данной области, быстро растет.

Для персонала службы безопасности и правоохранительных органов необходимо наличие функции расследования происшествий в системе безопасности с целью предотвращения подобных случаев в будущем и применение административных мер по отношению к виновным лицам. Расследование несанкционированных действий проводится по инцидентно-ориентированному принципу. Суть данного принципа заключается в выборке исходных данных, предшествующих и вызвавших инцидент, сортировке этих данных, их анализе с целью определения причин возникновения инцидента и выработке решений по устранению инцидента и недопущению его повторения. Проведение расследования должно быть оперативным и простым в управлении.

В заявке US 20040260947 A1 описывается система для сбора инцидентов безопасности, которая осуществляет сбор информации в несколько этапов - первичный сбор и дополнительный. После того как собрана необходимая информация о сети и ее компонентах, производится анализ и определяется инцидент. Однако данная система не позволяет определить причины и источник заражения.

В патенте US 7159237 описана система мониторинга безопасности компьютерной сети. Данная система не способна вырабатывать решения автоматически без участия аналитика, что сильно замедляет реакцию на инцидент.

В заявках WO 2001025935 A1 и US 20020019945 A1 описывается процесс хранения и представления информации об инциденте в доступном для управления формате.

Системы, которые существуют на данный момент, позволяют собирать информацию о событиях на компьютерах пользователей, выделять из событий те, которые могут нанести вред, и представлять отчеты службе безопасности. Однако существует ряд проблем, которые остаются нерешенными. Одна из таких проблем заключается в представлении данных в виде несвязных событий, например «обнаружен вирус» или «отказ в работе антивируса». Эта информация не позволяет восстановить цепочку и предысторию событий.

Другой проблемой известных систем является то, что они не позволяют выделять некоторые события среди других - ранжировать их. Такая возможность позволила бы удалять из журнала ненужную информацию и сохранять как можно дольше особо важные события. Опыт показывает, что для расследования некоторых инцидентов необходимо изучить события, произошедшие несколько лет (2-3 года) назад. Эта проблема приводит к тому, что при расследовании текущего инцидента специалисты не могут опираться на данные по похожим инцидентам или пользоваться историей событий.

Еще одним недостатком является непригодность систем к интеграции в вычислительные сети с большим количеством персональных компьютеров (ПК), т.к.

текущий протокол событий в результате превращается в большой неупорядоченный набор данных, анализ которых неспециалистом невозможен, а у специалиста займет большое количество времени.

Данное изобретение позволяет более эффективно и результативно решить задачу расследования инцидентов безопасности в компьютерной сети.

Сущность изобретения

Настоящее изобретение предназначено для решения проблемы расследования инцидентов безопасности в компьютерных сетях, исправления их последствий и предотвращения их повторений.

Техническим результатом настоящего изобретения является сокращение количества инцидентов безопасности за счет исключения повторения системных событий, определенных в качестве причин возникновения данных инцидентов безопасности. Описанные далее система и способ позволяют обнаруживать подозрительные события в компьютерной сети, анализировать их, восстанавливать историю событий, предшествующих инциденту безопасности, находить решения по исправлению последствий событий и настраивать систему для предотвращения повторения события.

Краткое описание прилагаемых чертежей

Сопровождающие чертежи, которые включены для обеспечения дополнительного понимания изобретения, и составляют часть этого описания, показывают варианты осуществления изобретения и совместно с описанием служат для объяснения принципов изобретения.

Заявленное изобретение поясняется следующими чертежами, на которых:

Фиг.1 показывает принятую схему системы расследования инцидентов безопасности.

Фиг.2 отображает функциональную схему обмена данными между сервером администрирования и ПК пользователя.

Фиг.3а показывает структурную схема системы автоматического расследования инцидентов безопасности.

Фиг.3б демонстрирует работу средства поиска решений.

Фиг.4а содержит модель нечетко-логической системы.

Фиг.4б показывает функцию принадлежности в нечетко-логической системе.

Фиг.5 описывает способ автоматического расследования инцидентов безопасности.

Описание предпочтительных вариантов осуществления

Система безопасности, как правило, содержит центральную часть, называемую сервером безопасности (СБ), к которой подключены ПК пользователей. При этом топология сети не имеет значения. Сервер безопасности предназначен для осуществления контроля действий, производимых в каждом ПК сети и между ними, а также для удаленного управления ПК и его настройки.

Описываемое изобретение может быть реализовано в качестве сервера безопасности или его надстройки.

Когда на компьютере пользователя происходит некоторое событие, попадающее под понятие инцидента, автоматически применяются меры по его исправлению и предотвращению. Настройка системы позволяет установить в качестве инцидента любое действие, которое полезно для расследования, например обнаружение вредоносного программного обеспечения, обнаружение сетевой атаки, обнаружение критических нарушений в работе антивируса и т.д.

На Фиг.1 изображена принятая схема системы расследования инцидентов безопасности. В состав системы входят следующие компоненты: сервер

администрирования 110, база данных администрирования 120, база данных инцидентов 130, база данных экспертной системы 140 и сервер антивирусной лаборатории 150. К системе подключены ПК пользователей 100 и консоль администрирования 160.

Когда в компьютерной сети ПК пользователей 100 обнаружен инцидент, данные об инциденте передаются на сервер администрирования 110 и сохраняются в базе данных администрирования 120. Сохраненные данные, в том числе обнаруженные инциденты обрабатывает специалист. Данные могут поступать как в реальном времени, так и загружаться с некоторой периодичностью, например, раз в сутки. Администратор безопасности, с одной стороны, может обращаться к базе данных администрирования 120, с другой - к базе данных инцидентов 130, которые уже были проанализированы. В своей работе администратор основывается на экспертных данных, которые хранятся в базе данных экспертной системы 140. Данная база, как правило, является обновляемой - обновление происходит с серверов антивирусной лаборатории 150. Проанализировав события, администратор группирует события в инциденты и заносит описание каждого инцидента в базу инцидентов 140. Взаимодействие администратора с системой осуществляется через консоль администрирования 160. База данных инцидентов заполняется информацией с гораздо меньшей скоростью, нежели аналогичная база данных событий, в результате чего появляется возможность хранить отчеты об инцидентах несколько лет. Некоторые из предложенных экспертной системой решений можно воплотить в жизнь автоматически. Если специалист согласится с этими решениями, то он подтверждает их выполнение, серверу администрирования 110 передаются необходимые команды, которые передаются на ПК пользователя 100. Команды могут быть не для одного ПК, а представлять собой глобальные решения, например отключение автозапуска на уровне группы или всех ПК. Ответ о принятых мерах заносится в описание инцидента. Статистические данные об инцидентах и принятых или отклоненных мерах анонимно могут передаваться на сервер антивирусной лаборатории для накопления статистики и последующей корректировки правил базы экспертной системы.

Анализ данных администраторами безопасности в масштабах крупной корпоративной вычислительной сети неэффективен из-за больших объемов информации. Далее будет описана система, позволяющая оптимизировать процесс разбора инцидента, а также позволяющая сократить объем хранимой информации. Процесс управления ПК пользователей на сервере администрирования более детально показан на Фиг.2. Для защиты информации на компьютерах пользователей 100 устанавливаются средства защиты 210. Состав этих средств может быть различным, но необходимым средством защиты является антивирус, который сканирует систему на наличие вредоносных компонент и лечит зараженные файлы. Средства защиты обладают набором параметров, которые управляются с помощью сервера администрирования. Например, доступ к нежелательному или опасному веб-ресурсу может быть заблокирован в сетевом экране настройкой правил фильтрации сетевого графика. Встроенный в операционную систему сервис безопасности также является средством защиты 210 и может поддерживать политику безопасности в сети. Средства защиты 210 постоянно в процессе работы ведут журналы и создают отчеты работы 220. Эта информация 220 может быть представлена в различном формате данных: текст, файл, запись в базе данных и содержит системное время события, код ошибки или тип инцидента. Собранные в ПК 100 данные 220 передаются в сервер администрирования, где происходит первичный анализ. Затем сервер запрашивает

дополнительную информацию, если она необходима. Например, при возникновении событий типа «обнаружен вирус» или «обнаружена атака» на сервер администрирования передается расширенная информация - тип; серийный номер и дата подключения сменных носителей, если вирус найден на них; данные о том, как создается зараженный объект в общедоступной папке, если речь идет о вирусе в этой папке; данные о подключенных модемах, сетевых адаптерах в случае сетевых инцидентов. Необходимо учесть, что дополнительные системные данные могут быть запрошены также с ПК, отличного от того, на котором обнаружен инцидент. ПК, с которого дополнительно загружаются системные данные, может быть, например, связан с первым ПК по средствам передачи данных. После анализа данных и формирования решений и рекомендаций 230 последние передаются от анализатора инцидентов на сервер администрирования, где применяются. Некоторые решения 230 могут быть автоматически применены и отосланы на один или несколько компьютеров 100. Примером автоматического применения рекомендаций может служить инцидент, связанный с заражением компьютера с флеш-карты памяти. В таком случае система настраивается на автоматическую блокировку флеш-карт с данным серийным номером на всех или выбранных ПК. Возможны также другие варианты рекомендаций для применения в автоматическом режиме - это блокировка всех носителей информации на заданном ПК, выполнение расширенного сканирования и т.д.

В случае отсутствия системы анализа инцидентов отчеты, которые представлялись администратору безопасности 170 на сервере администрирования 110, выглядят следующим образом:

09-BUH-5 2009-08-13 10:12:09.000 E:\.System\S-1-6-21-2434476501-1644491937-600003330-1213\Autorun.exe Trojan.Win32.Buzus.arrw

Как можно заметить, эти данные очень сложно верно интерпретировать неспециалисту. Даже если администратор безопасности хорошо разбирается в защите компьютеров от вредоносных программ и атак, он не всегда может знать как восстановить систему в случае заражения. Именно эту проблему решает система автоматического расследования инцидентов. Обработав исходные данные и запросив дополнительную информацию, система способна на основе знаний, хранимых в базах данных инцидентов и экспертной системы, сгенерировать отчет, который будет понятен специалисту среднего уровня, и в некоторых случаях позволит решить проблему в автоматическом режиме. Отчеты об инцидентах будут иметь качественно новое представление:

13.08.2009 в 10:10 к ПК 09-BUH-5 (IP=192.168.0.114, бухгалтер Сидорова) был подключен Flash-накопитель Transcend JetFlash V30 (емкость 4 Гб, SN:1234567890), не значащийся в базе служебных Flash-накопителей.
Проверка антивирусным монитором показала, что накопитель заражен вредоносной программой Trojan.Win32.Buzus.arrw (был заражён файл: E:\System\S-1-6-21-2434476501-1644491937-600003330-1213\Autorun.exe).
Вредоносная программа была успешно нейтрализована монитором.
На данном ПК зафиксировано уже 4 подобных инцидента, ближайший – 12.08.2009 [подробнее].
11.08.2009 указанный выше Flash-накопитель фигурировал в инциденте на ПК 09-GLBUH [подробнее].
Рекомендации:

1. *Заблокировать возможность подключения накопителя Transcend JetFlash V30 SN:1234567890 на ПК 09-BUH-5 [выполнить], на всех ПК группы «1» [выполнить] или создать глобальное правило на запрет работы с данным накопителем для всех групп [выполнить]*
2. *Отключить на ПК 09-BUH-5 возможность работы с Flash-накопителями [выполнить]*

Выполненные мероприятия:

1. *Проверка Flash-накопителя на вирусы с лечением [выполнено - подробнее]*

В квадратных скобках данного примера показаны интерактивные элементы, например гиперссылки, нажатие которых приводит к выполнению неких действий по настройке или отображению дополнительной информации. Данный отчет использует те же данные, как и в предыдущем примере, дополнительную информацию и историю инцидентов. Представление содержит консолидированные данные в доступном человеку формате, которые отображают суть инцидента, время происшествия, его причины. Наиболее важным дополнением являются действия, которые предлагается произвести или применить. В случае выполнения действий отчет может перестраиваться - появится позиция «Выполненные мероприятия» с интерактивной функцией «отменить». Кроме того, в описании инцидента содержится список действий, сделанных человеком и добавляемых им по мере выполнения. Это сделано для ведения административной отчетности, например «запрошена объяснительная записка от пользователя», «получена объяснительная записка», «вынесено решение сократить премию пользователя на 10% за вирусный инцидент» и т.д.

На Фиг.3а показана схема системы автоматического расследования инцидентов безопасности. Система состоит из четырех основных элементов: средства сбора событий 300, поиска решений 302, регистрации инцидента 303 и анализа событий 301.

Система может быть установлена на сервер администрирования 110 и вместе с ним подключена к компьютерной сети.

Основным назначением средства сбора событий 300 является загрузка данных о системных событиях 220 с компьютерных устройств пользователей, подключенных к серверу администрирования. Загружаемыми данными являются записи программных и системных журналов и отчетов, которые ведут записи действий пользователей, запросы программ, сетевые запросы и т.д. Загрузка данных может производиться в несколько этапов: сначала могут быть загружены события высокого уровня, а затем, если есть необходимость, события низкого уровня. К событиям высоко уровня относятся такие действия, как действие с файлами, изменение прав доступа, запуск программ. К событиям низкого уровня относятся команды программ и передаваемые сетевые пакеты, например обращение к памяти процесса, блокирование входящего пакета данных и т.д.

Средство регистрации инцидента 303 обнаруживает или регистрирует факт возникновения инцидента. Данное средство может являться антивирусным средством, сетевым экраном или другим средством защиты или получать от данного средства информацию об инциденте. Например, в случае если антивирус обнаружит вредоносную активность, средство регистрации 303 отметит событие, на которое сработал антивирус, как инцидент. После чего направит инцидент в средство анализа событий.

Средства защиты реагируют уже на случившийся факт заражения или нарушения политики. Решением для данного случая может являться лишь восстановление системы или лечение файла. Однако проблема лежит глубже, в том, почему данный инцидент смог произойти. Если антивирус обнаружил вредоносное программное обеспечение, то необходимо понять откуда оно было загружено или кем заражено. И искать решение для исходной проблемы, а не только для той, которая была обнаружена. Расследование инцидента является назначением средства анализа событий 301. После того как инцидент был зарегистрирован, он попадает в средство анализа 301, где для данного события собираются все связанные с ним события. События могут храниться в базе данных администрирования или в любом другом доступном средстве хранения информации. За сбор событий отвечает средство сбора событий 300, однако для анализа понадобятся не все записи.

Для каждого инцидента, зафиксированного на компьютере пользователя, загружаются предшествующие ему события и сортируются в хронологическом порядке. Далее средство анализа выстраивает цепочку событий, которые связаны с объектом инцидента. Объектом инцидента является объект операционной системы (файл, процесс, сетевой пакет, учетная запись, память, запись системного реестра, подключенное физическое устройство и другие). С исследуемого компьютерного устройства загружают дополнительную информацию по связанным событиям. Цепочка событий для каждого компьютера имеет, по меньшей мере, одно начальное событие и одно конечное событие. Конечным событием является событие, зарегистрированное средством регистрации инцидента, а начальным событием является событие, произошедшее раньше остальных. После того как цепочка событий в компьютерном устройстве построена, средство анализа событий проверяет наличие в цепи ветвей событий, которые связаны с другими компьютерными устройствами корпоративной сети или внешними устройствами (карты памяти, внешние диски, мобильные устройства). Примером ветви является передача файла по почте, копирование файла в общий доступ, запись файла на съемную карту памяти. Если ветви обнаружены, то аналогичная цепочка событий строится на связанном компьютере сети, после чего цепочки событий объединяются. Связанными считаются

компьютеры, которые участвовали в передаче или доступе к объекту инцидента. Например, компьютерные устройства, к которым был подключен один и тот же внешний диск или компьютеры, между которыми передавался объект инцидента. Процесс анализа продолжается до тех пор, пока все ветви не будут проанализированы или пока не будут обработаны все сохраненные в базе данных события. Результирующая цепочка может иметь несколько начальных событий. Как правило, начальным событием является загрузка файла с вредоносного сайта, получение и открытие почтового сообщения с вредоносным вложением, подключение зараженного внешнего носителя и т.д.

В другом варианте реализации причинно-следственная связь событий сохраняется изначально в системном журнале. В этом случае журнал выполнен в виде таблицы или базы данных, в которой определены причинно-следственные связи между записями, например наследование объектов, хронологическая последовательность записей и специальные идентификаторы. Например, если фиксируется факт запуска файла и определяется его вредоносный характер, начинается расследование со следующими исходными данными: полное имя файла, его контрольная сумма, дата изменения и другие параметры в зависимости от операционной системы. Таблица или база данных содержит информацию о пользователе, запустившем файл, приложении, которое его обрабатывало. Неизвестное приложение будет являться новой отправной точкой - параллельной цепочкой расследования, целью которого будет определить максимально информацию о происхождении приложения и уровне доверия, например определить у скольких пользователей оно есть и как часто запускается, откуда было загружено или скопировано.

Если обрабатывающее приложение известно и доверено, то расследование переходит к поиску загрузок данного файла из сети, затем к поиску операции копирования этого файла.

Если файл находится на сменном носителе, то производится проверка данного носителя: ищется в сети компьютерная система, зафиксировавшая подключение данного устройства.

Результат каждой проверки может являться отправной точкой для новой цепочки расследования (являться входным параметром расследования).

Некоторые цепочки приведут к событиям, которые не влияют на безопасность компьютерной системы (не могут быть оценены для модификации политики безопасности). К таким событиям относятся:

- работа доверенных приложений;
- работа с новыми устройствами, сетевыми ресурсами и объектами (устройства, ресурсы и объекты, информация о которых отсутствует в базе данных системных событий и экспертной базе данных);
- события, которые не были зафиксированы в системный журнал в результате поздней установки системы расследования или в результате специальной настройки ведения журналов.

В случае когда процесс расследования завершается одним из приведенных событий, анализ продолжается по временным интервалам. Из базы данных системных событий считываются события, приближенные к конечному событию по времени: сетевые соединения, запуск программ и другие, после чего расследование инцидента идет по новым цепям событий, начинающихся с обнаруженных во временном интервале событий.

В одном из вариантов технический результат достигается за счет использования

еще одного подхода в поиске источников угроз безопасности. Если на компьютере обнаружен подозрительный объект и необходимо произвести его анализ, но на данном компьютерном устройстве сети расследование не дает результатов, можно произвести расследование по данному объекту на другом компьютере сети или на нескольких компьютерах сети, получить и сравнить результаты расследования по данному объекту. Например, обнаружен вирус, но на данном компьютере нет возможности проанализировать системные журналы и таблицы. Производится поиск компьютерных систем, на которых был обнаружен данный объект, и далее цепочки событий строятся на найденном компьютере. Масштаб системы может быть ограничен одним компьютером, локальной сетью, а может распространяться на глобальную сеть с использованием центральных серверов и прямой связи пользователей.

Начальные события определяются в качестве причин возникновения инцидента безопасности, и именно для них требуется найти решение, которое предотвратит в дальнейшем повторение инцидента и исправит его последствия. Более подробно пример работы средства поиска решений 302 будет описан далее.

На Фиг.3б изображена функциональная схема средства поиска решений 302. Менеджер аналитики 310 - средство, которое консолидирует информацию о событиях и инциденте 220 из баз данных администрирования 120 и инцидентов 130 и экспертные данные 311 из базы данных экспертной системы 140. В составе средства поиска решений 302 находится несколько аналитических модулей 320, в которых реализуется алгоритм принятия решения по какому-либо признаку (или по набору признаков). Эти алгоритмы могут быть изменены путем обновления базы данных экспертной системы 140 без изменений структуры средства 302 целиком. На выходе аналитического модуля 320 получается решение, которое попадает в систему принятия решений 330. Каждый анализатор обладает приоритетом для однозначного определения решения. Исходя из приоритета выбирается решение. Некоторые аналитические модули 320 используют в качестве параметров различные данные и решения могут не пересекаться, а дополняться. Например, в случае если первый аналитический модуль принял решение о карантине, второй аналитический модуль 320 может принять решение уже о том, стоит ли послать файл на проверку на сервер антивирусной лаборатории 150, третий аналитический модуль 320 принимает решения об автоматическом применении предыдущих решений. Обработав все решения, система принятия решений генерирует предлагаемые действия 230 и включает их в отчет об инциденте, который сохраняется в базе данных инцидентов 130 и направляется в сервер администрирования 110 после того как специалист одобрит рекомендуемые действия или выберет наиболее подходящее в консоли администрирования 160. Система может быть настроена также на автоматическое выполнение рекомендаций. В этом случае стадия проверки и одобрения специалистом будет отсутствовать.

Алгоритм аналитического модуля 320 может быть различным. В качестве примера алгоритм одного из модулей построен на нечеткой логике. Данный аналитический модуль должен определить, следует ли отправить исследуемый файл на карантин и послать его аналитикам на сервер антивирусной лаборатории 150. Модуль представляет собой нечетко-логическую систему Мамдани. В данном случае входными сигналами являются сведения, найденные по метаданным объекта: полное имя, размер, информация об авторе, время последнего изменения, атрибуты. В данном примере входными данными 410 аналитического модуля 320 являются:

- qr_nc_count - количество файлов с похожими метаданными, которые ранее удалось успешно отправить на карантин;

- qr_err_count - количество файлов с похожими метаданными, которые ранее система отправляла на карантин, но безуспешно (подобная ситуация возникает в случае, если объектом является запись реестре, или файл, который защищен от копирования специальным методами);

- qr_malware_count - количество файлов с похожими метаданными, которые ранее успешно отправлены на карантин (автоматически или пользователем) и после изучения были признаны вредоносными;

- qr_new_malware_count - количество файлов с похожими метаданными, которые ранее успешно отправлены на карантин, автоматическими эвристиками не обнаруживались и после изучения были признаны вредоносными;

- qr_good_count - количество файлов с похожими метаданными, которые ранее успешно отправлены на карантин и после анализа были признаны легитимными.

Как несложно заметить, ни один из показателей не позволяет однозначно принять решение, и в большинстве случаев появляется конкуренция - ситуация, в которой большинство указанных показателей не равны нулю. Например, файл ранее многократно встречался, признавался чистым, в других случаях признавался вредоносным, и в каждом случае картина уникальна и необходимо принять единственно верное решение. Отправлять в таких случаях файл на карантин неразумно. Это можно объяснить тем, что на каждый инцидент будет собрано очень большое количество файлов, которые очень сложно обработать. При этом интерес представляют только несколько файлов (2-3) из них.

На Фиг.4б представлены функции принадлежности. Для каждой из входных переменных 460 определены лингвистические переменные, а для каждой переменной определены термы 450. Например, «Очень низкий», «Низкий», «Средний», «Высокий», «Очень высокий», и для каждого терма определены функции принадлежности 440. С помощью функций принадлежности 440 можно произвести операцию, называемую фаззификацией, т.е. приведением к нечетким переменным. Если для файла с такими метаданными обнаружено сорок новых вредоносных программ, то это соответствует уровню «СРЕДНИЙ». Эксперт строит правила вида:

ЕСЛИ {количество новых вредоносных программ высокое},

ТО {потребность в карантине очень высокая}.

Правила просты и записаны на естественном языке, поэтому эксперт без труда может формулировать подобные правила, их легко анализировать и проверять. Более того, высоким количеством вредоносных программ на данный момент считается количество в размере пяти, а спустя некоторые время это значение может увеличиться до пятисот. Это необходимо учитывать на стадии фаззификации. Функции принадлежности 440 легко править для их соответствия текущим обстоятельствам, не изменяя правил, и наоборот. В системе правила выглядят следующим образом:

If (qr-nc-count is vis) then (qr-priority is niz) [**0.15**]
If (qr-nc-count is och-vis) then (qr-priority is niz) [**0.15**]
If (qr-err-count is och-niz) then (qr-priority is vis) [**0.6**]
If (qr-err-count is niz) then (qr-priority is sredn) [**0.6**]
If (qr-err-count is sredn) then (qr-priority is niz) [**0.1**]
If (qr-err-count is vis) then (qr-priority is niz) [**0.1**]
If (qr-malware-count is och-niz) then (qr-priority is niz) [**1**]
If (qr-malware-count is niz) then (qr-priority is niz) [**1**]
If (qr-malware-count is sredn) then (qr-priority is sredn) [**1**]
If (qr-malware-count is vis) then (qr-priority is och-vis) [**1**]
If (qr-malware-count is och-vis) then (qr-priority is och-vis) [**1**]
If (qr-new-malware-count is och niz) then (qr-priority is niz) [**0.25**]
If (qr-new-malware-count is niz) then (qr-priority is sredn) [**0.25**]

Цифры в квадратных скобках - это весовые коэффициенты, показывающие приоритетность и значимость правил. В системе обычно двадцать - тридцать правил, на основании которых ведется принятие решения. Затем производится обратная операция - дефаззификация 430, в процессе которой рассчитывается четкое число, например, от «0» до «100». Число «0» означает, что в карантине нет необходимости, а противоположное значение «100» означает, что необходимо отправить файл на карантин и изучить его с высшим приоритетом.

На Фиг.5а и 5б показан способ автоматического расследования инцидентов, реализуемый на стороне клиента и сервера соответственно.

Расследование инцидентов предполагает сбор системных данных о действиях пользователя, программ на ПК и начинается с инициализации 500, т.е. установки и запуска средств защиты 210 на ПК. Средства защиты 210 записывают системные данные - ведут журнал данных, обрабатываемых средствами защиты или другими службами (встроенными в операционную систему). Под обработкой данных понимается перехват команд, функций (API-функций), чтение памяти и файлов программ и любое другое возможное действие с объектами операционной системы. Основной функцией средств защиты 210 является выявление и отслеживание 510 инцидентов безопасности - событий, которые нарушают политику безопасности и являются угрозой для информации ПК и компьютерной сети в целом.

Если на шаге 515 обнаружен инцидент, то в журналах осуществляется выборка 520 тех записей о событиях, которые связаны с данным инцидентом по критериям. Сопоставленные (выбранные) события могут быть сохранены в отдельный файл, промаркированы флагами или выделены другим образом. На шаге 525 полученные данные на этапе 520 отправляются на сервер. В качестве альтернативы данные могут быть выложены в сетевой папке или доступ к файлам разрешен для сервера администрирования, чтобы последний в любой момент мог загрузить данные.

Помимо внутренних событий отслеживаются сетевые запросы от сервера 530. Клиент может получить от сервера рекомендации 535 для исправления последствий инцидентов и команду обновления 545. Когда от сервера получены рекомендации - обновленная политика безопасности, файл настройки средства защиты, исполняемый файл, скрипт файл или решение, в другом поддерживаемом формате, клиент исполняет 540 (применяет) данные рекомендации. Рекомендации могут быть также направлены пользователю в аудио-визуальном формате для ручной настройки или исполнения.

Если от сервера приходят обновления, содержащие новые/измененные критерии детектирования инцидентов, правила детектирования, правила сбора и фильтрации событий, клиент сохраняет 550 их в средства защиты, что позволяет удаленно изменять работу системы расследования инцидентов безопасности на ПК.

Обнаружение инцидента может произойти в первую очередь на сервере в результате корреляции системных отчетов, собранных с множества ПК. После того как обнаружен инцидент 555 (на сервере или на клиентес помощью множества детекторов установленных на ПК пользователей 100 в модулях защиты 210) производится сбор данных об инциденте 560. Первичные данные содержат лишь небольшой набор данных, таких как время обнаружения инцидента, наименование ПК в сети, имя авторизованного пользователя, тип инцидента и его параметр, как это было описано ранее. Далее в базе данных известных инцидентов выбираются связанные инциденты 565: зарегистрированные на этом компьютере; произошедшие по вине данного пользователя; с тем же типом инцидента; обнаружена та же вредоносная программа, зарегистрированные на компьютере, осуществлявшим обмен данными с ПК, на котором обнаружен инцидент. После этого производится анализ данных 570, который определяет достаточность полученных данных, сравнивает инцидент со связанными событиями и определяет причины возникновения инцидента 580. На шаге 570 может возникнуть потребность в дополнительных данных 575, например журнал последних действий в системе, номера подключенных внешних устройств и журнал посещения веб-сайтов, для более точного установления причин нарушения политики безопасности. После определения инцидента и сбора всех необходимых параметров запускается поиск рекомендаций и решений 585. Данный процесс протекает в средстве поиска решений 302 с учетом экспертных данных. Причинно-следственные алгоритмы, реализованные в аналитических модулях 320, могут быть построены на разных методах - статистических, логических, нечеткой логики, функциональных и других. Опционально составляется отчет об инциденте, включающий описание инцидента, события, повлекшие к возникновению инцидента, принятые и рекомендуемые меры. Характерной чертой генерируемого отчета является его доступная для восприятия форма, отличающая отчет от аналогов и возможная благодаря средству анализа событий. Информация о найденных решениях и рекомендациях добавляется в отчет об инциденте, упрощая его восприятие администратором безопасности. Далее идет шаг проверки 595 данной рекомендации, выбор наиболее подходящего решения, если существует альтернатива, и их применение. Установка решений и применение рекомендаций может происходить в автоматическом режиме, если это отмечено в настройках системы, или запускаться администратором безопасности из отчета об инциденте. В завершении отчет об инциденте сохраняется в базе данных инцидентов. Результирующий отчет содержит собранные данные об инциденте, дополнительную информацию, рекомендации, выполненные действия и проведенные административные мероприятия.

Фиг.6 представляет пример компьютерной системы общего назначения, персональный компьютер или сервер 20, содержащий центральный процессор 21, системную память 22 и системную шину 23, которая содержит разные системные компоненты, в том числе память, связанную с центральным процессором 21. Системная шина 23 реализована, как любая известная из уровня техники шинная структура, содержащая в свою очередь память шины или контроллер памяти шины, периферийную шину и локальную шину, которая способна взаимодействовать с любой другой шинной архитектурой. Системная память содержит постоянное

запоминающее устройство (ПЗУ) 24, память с произвольным доступом (ОЗУ) 25. Основная система ввода/вывода (BIOS) содержит основные процедуры, которые обеспечивают передачу информации между элементами персонального компьютера 20, например, в момент загрузки операционной системы с использованием ПЗУ 24.

Персональный компьютер 20 в свою очередь содержит жесткий диск 27 для чтения и записи данных, привод магнитных дисков 28 для чтения и записи на сменные магнитные диски 29 и оптический привод 30 для чтения и записи на сменные оптические диски 31, такие как CD-ROM, DVD-ROM и иные оптические носители информации. Жесткий диск 27, привод магнитных дисков 28, оптический привод 30 соединены с системной шиной 23 через интерфейс жесткого диска 32, интерфейс привода магнитных дисков 33 и интерфейс оптического привода 34 соответственно. Приводы и соответствующие компьютерные носители информации представляют собой энергонезависимые средства хранения компьютерных инструкций, структур данных, программных модулей и прочих данных персонального компьютера 20.

Настоящее описание раскрывает реализацию системы, которая использует жесткий диск, сменный магнитный диск 29 и сменный оптический диск 31, но следует понимать, что возможно применение иных типов компьютерных носителей информации, которые способны хранить данные в доступной для чтения компьютером форме (твердотельные накопители, флеш карты памяти, цифровые диски, память с произвольным доступом (ОЗУ) и т.п.).

Компьютер 20 имеет файловую систему 36, где хранится записанная операционная система 35 и дополнительные программные приложения 37, другие программные модули 38 и программные данные 39. Пользователь имеет возможность вводить команды и информацию в персональный компьютер 20 посредством устройств ввода (клавиатуры 40, манипулятора «мышь» 42). Могут использоваться другие устройства ввода (не отображены): микрофон, джойстик, игровая консоль, сканнер и т.п. Подобные устройства ввода по своему обычаю подключают к компьютерной системе 20 через последовательный порт 46, который в свою очередь подсоединен к системной шине, но могут быть подключены иным способом, например, при помощи параллельного порта, игрового порта или универсальной последовательной шины (USB). Монитор 47 или иной тип устройства отображения также подсоединен к системной шине 23 через интерфейс, такой как видеоадаптер 48. В дополнение к монитору 47 персональный компьютер может быть оснащен другими периферийными устройствами вывода (не отображены), например колонки, принтер и т.п.

Персональный компьютер 20 способен работать в сетевом окружении, при этом используется сетевое соединение с другим или несколькими удаленными компьютерами 49. Удаленный компьютер (или компьютеры) 49 являются такими же персональными компьютерами или серверами, которые имеют большинство или все упомянутые элементы, отмеченные ранее при описании существа персонального компьютера 20, представленного на Фиг.6. В вычислительной сети могут присутствовать также и другие устройства, например, маршрутизаторы, сетевые станции, пиринговые устройства или иные сетевые узлы.

Сетевые соединения могут образовывать локальную вычислительную сеть (LAN) 51 и глобальную вычислительную сеть (WAN) 52. Такие сети применяются в корпоративных компьютерных сетях, внутренних сетях компаний и, как правило, имеют доступ к сети Интернет. В LAN- или WAN-сетях персональный компьютер 20 подключен к локальной сети 51 через сетевой адаптер или сетевой интерфейс 53. При

использовании сетей персональный компьютер 20 может использовать модем 54 или иные средства обеспечения связи с глобальной вычислительной сетью 52, такой как Интернет. Модем 54, который является внутренним или внешним устройством, подключен к системной шине 23 посредством последовательного порта 46. Следует уточнить, что сетевые соединения являются лишь примерными и не обязаны отображать точную конфигурацию сети, т.е. в действительности существуют иные способы установления соединения техническими средствами связи одного компьютера с другим.

В заключение 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.

Формула изобретения

1. Система автоматического расследования инцидентов безопасности, выполненная в виде сервера администрирования, который содержит

(а) средство сбора данных, хранящееся в памяти и исполняемое на процессоре сервера администрирования, предназначенное для загрузки с подключенных к серверу администрирования компьютерных устройств данных о системных событиях, фиксируемых в упомянутых компьютерных устройствах, при этом средство сбора данных связано с анализатором инцидентов;

(б) средство регистрации инцидентов, хранящееся в памяти и исполняемое на процессоре сервера администрирования, предназначенное для выделения, по меньшей мере, одного системного события из загруженных данных, вызвавшего инцидент безопасности, при этом средство регистрации инцидентов связано с анализатором инцидентов и средством сбора данных;

(в) анализатор инцидентов, хранящийся в памяти и исполняемый на процессоре сервера администрирования, предназначенный для

поиска событий, предшествующих зарегистрированному инциденту безопасности;

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

(д) средство поиска решений, хранящееся в памяти и исполняемое на процессоре сервера администрирования, предназначенное для поиска решения для устранения последствий и предотвращения повторений инцидента безопасности соответствующего событию, определенному анализатором в качестве причины возникновения инцидента, при этом средство поиска решений связано с анализатором инцидентов.

2. Система по п.1, в которой данные о системных событиях, загружаемые с компьютерных устройств, хранятся на компьютерных устройствах в виде системных журналов или программных отчетов.

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

нарушение политики безопасности;

обнаружение вредоносной программы;

некорректная работа средства защиты.

4. Система по п.1, в которой решение представляет собой, по меньшей мере, одну из мер:

изменение политики безопасности;

обновление программного обеспечения;

рекомендация пользователю, записанная в обрабатываемом на компьютерном устройстве формате.

5. Система по п.1, в которой анализатор инцидентов предназначен также для определения компьютерного устройства, на котором было зафиксировано событие, вызвавшее инцидент безопасности.

6. Система по п.5, в которой анализатор инцидентов предназначен также для определения пользователя, авторизованного на упомянутом компьютерном устройстве.

7. Система по п.1, которая дополнительно содержит сервер антивирусной лаборатории, предназначенный для обработки зарегистрированных инцидентов и загрузки нового решения в средство поиска решений.

8. Система по п.1, которая дополнительно содержит средство создания отчетов, предназначенное для генерации отчета, содержащего, по меньшей мере, описание системных событий, взаимосвязь событий, хронологию событий, найденные решения, примененные решения.

9. Способ автоматического расследования инцидентов безопасности, в котором

(а) загружают данные о системных событиях с компьютерных устройств, подключенных к серверу администрирования;

(б) регистрируют, по меньшей мере, одно системное событие из загруженных данных, вызвавшее инцидент безопасности;

(в) анализируют загруженные события путем поиска событий, предшествующих зарегистрированному инциденту безопасности;

(г) определяют, по меньшей мере, одно системное событие, являющееся причиной возникновения инцидента;

(д) производят поиск и применение решения для устранения последствий и предотвращения повторений инцидента безопасности соответствующего событию, определенному в качестве причины возникновения инцидента.

10. Способ по п.9, в котором данные о системных событиях, загружаемые с компьютерных устройств, хранятся на компьютерных устройствах в виде системных журналов или программных отчетов.

11. Способ по п.9, в котором инцидентом безопасности является, по меньшей мере, одно из событий:

нарушение политики безопасности;

обнаружение вредоносной программы;

некорректная работа средства защиты.

12. Способ по п.9, в решение представляет собой, по меньшей мере, одну из мер:

изменение политики безопасности;

обновление программного обеспечения;

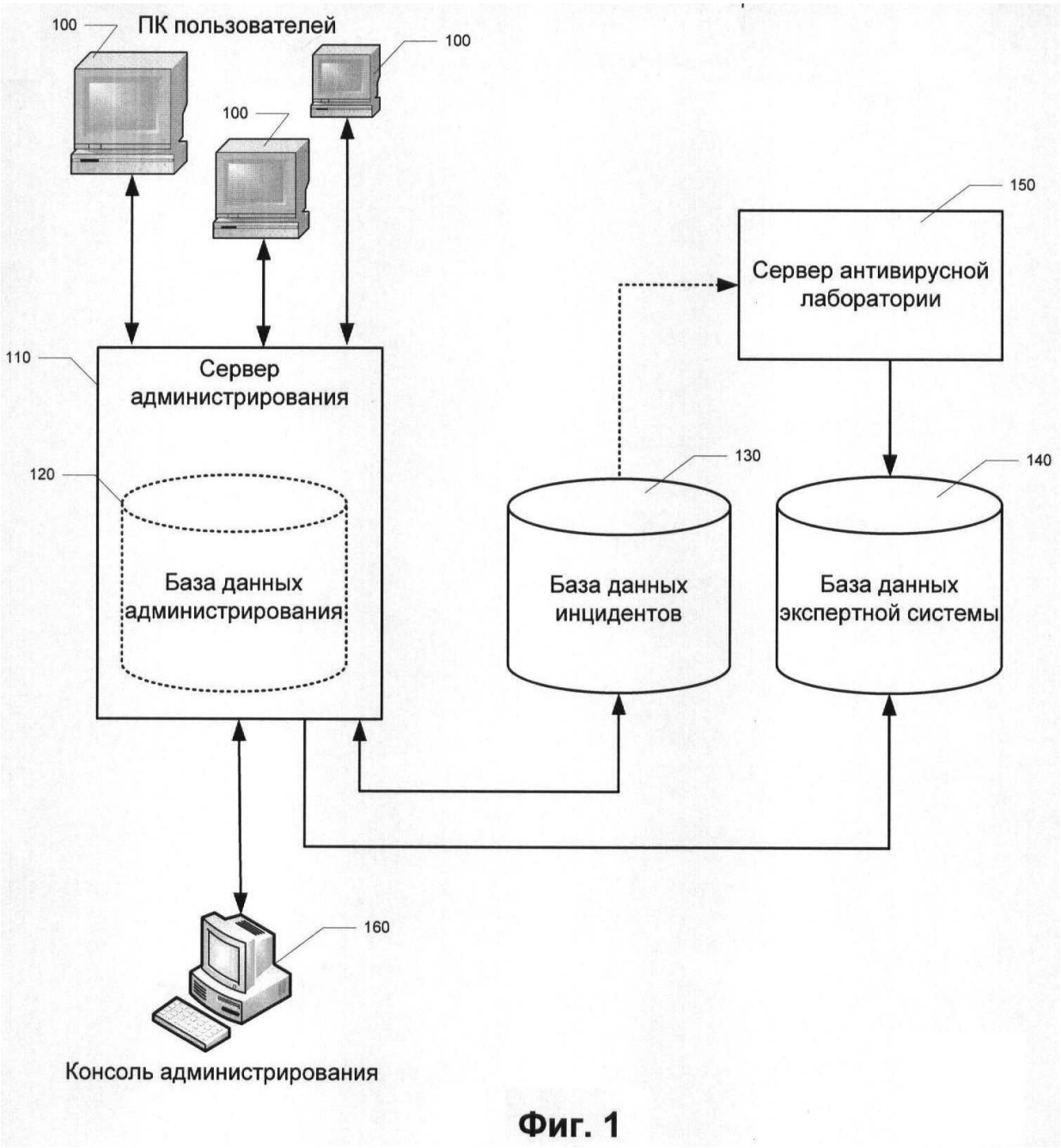
рекомендация пользователю, записанная в обрабатываемом на компьютерном устройстве формате.

13. Способ по п.9, который дополнительно содержит этап, на котором анализатор инцидентов определяет компьютерное устройство, на котором было зафиксировано событие, вызвавшее инцидент безопасности.

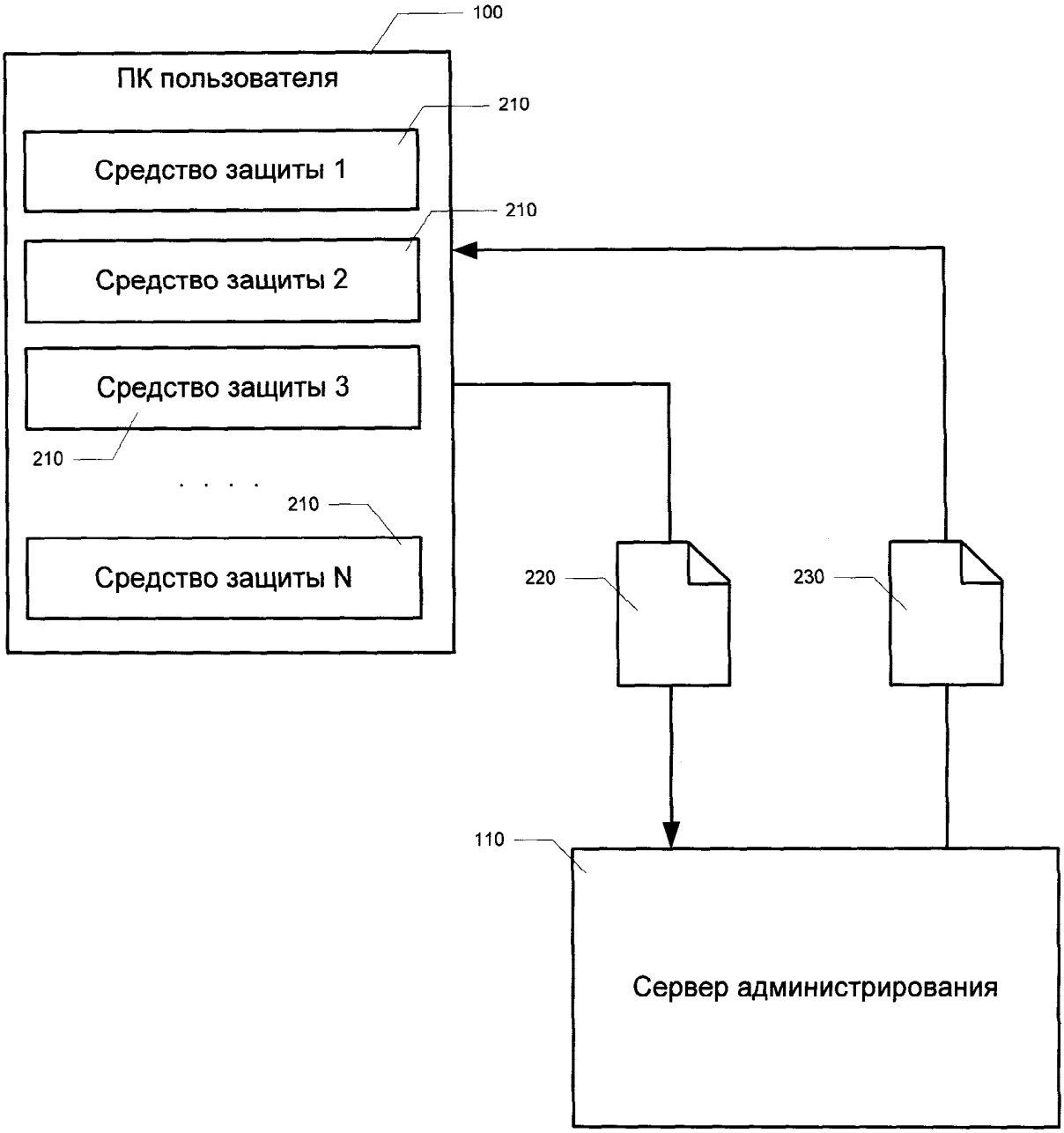
14. Способ по п.13, который дополнительно содержит этап, на котором анализатор инцидентов определяет пользователя, авторизованного на упомянутом компьютерном устройстве.

15. Способ по п.9, который дополнительно содержит этап, на котором генерируют отчет, содержащий, по меньшей мере, описание системных событий, взаимосвязь событий, хронологию событий, найденные решения, примененные решения.

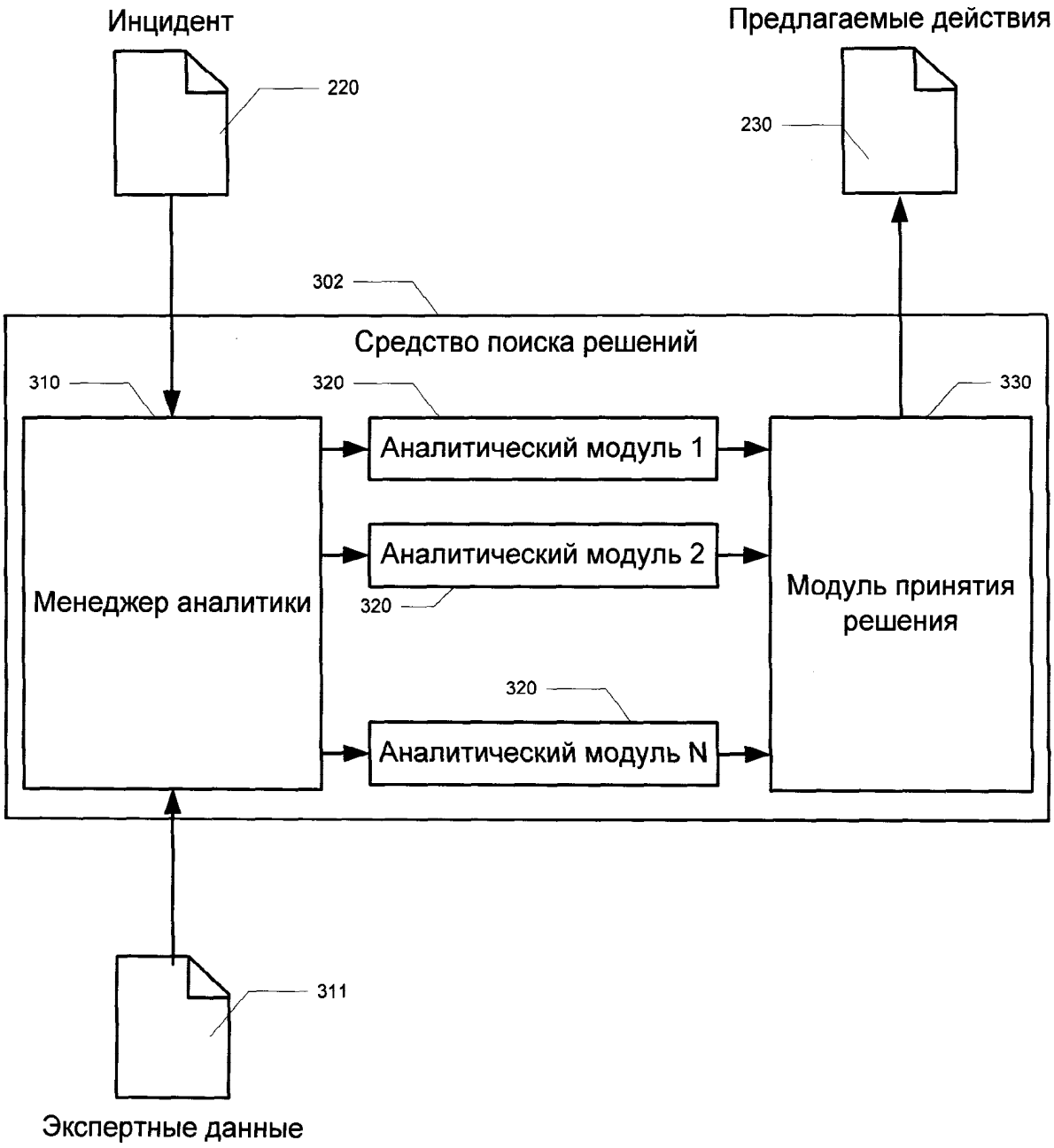
16. Способ по п.9, который запускается на выполнение с заданной периодичностью.


100
ПК пользователей
100
100
150
Сервер антивирусной лаборатории
110
Сервер администрирования
120
130
140
База данных администрирования
База данных инцидентов
База данных экспертной системы
160
Консоль администрирования

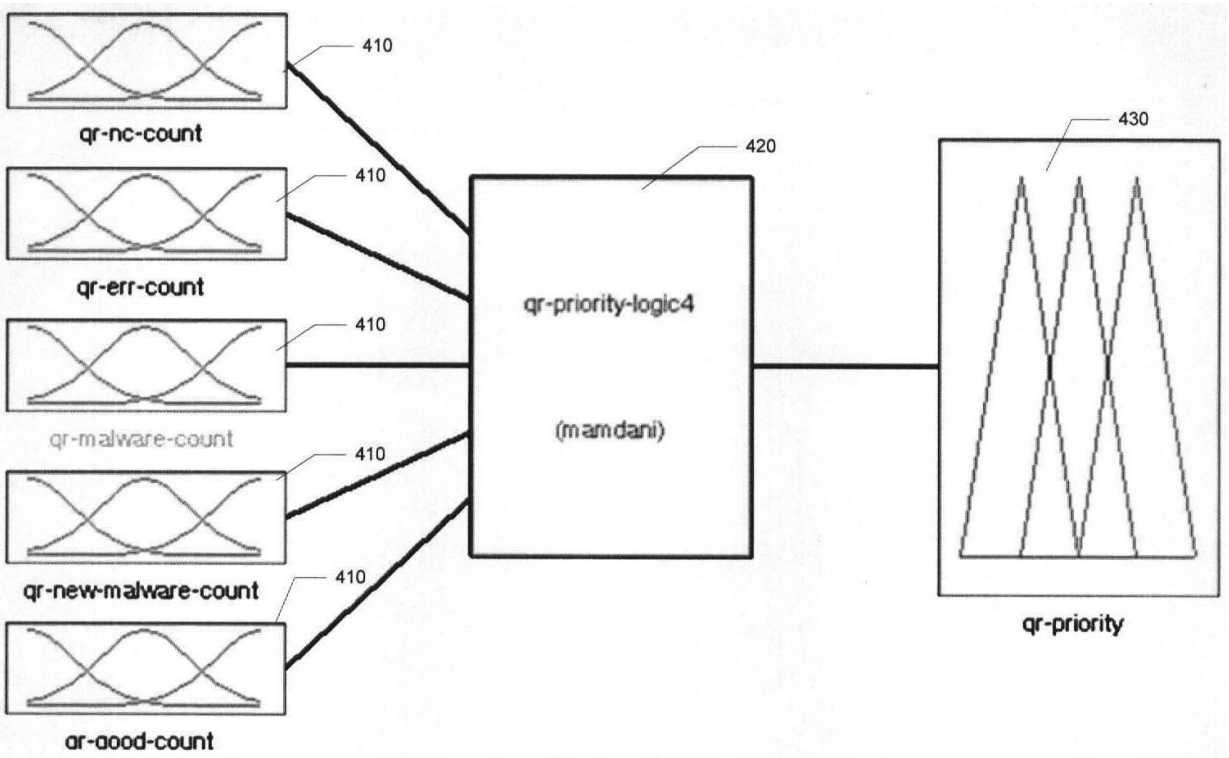
Фиг. 1


100
ПК пользователя
210
Средство защиты 1
210
Средство защиты 2
Средство защиты 3
210
210
Средство защиты N
220
230
110
Сервер администрирования

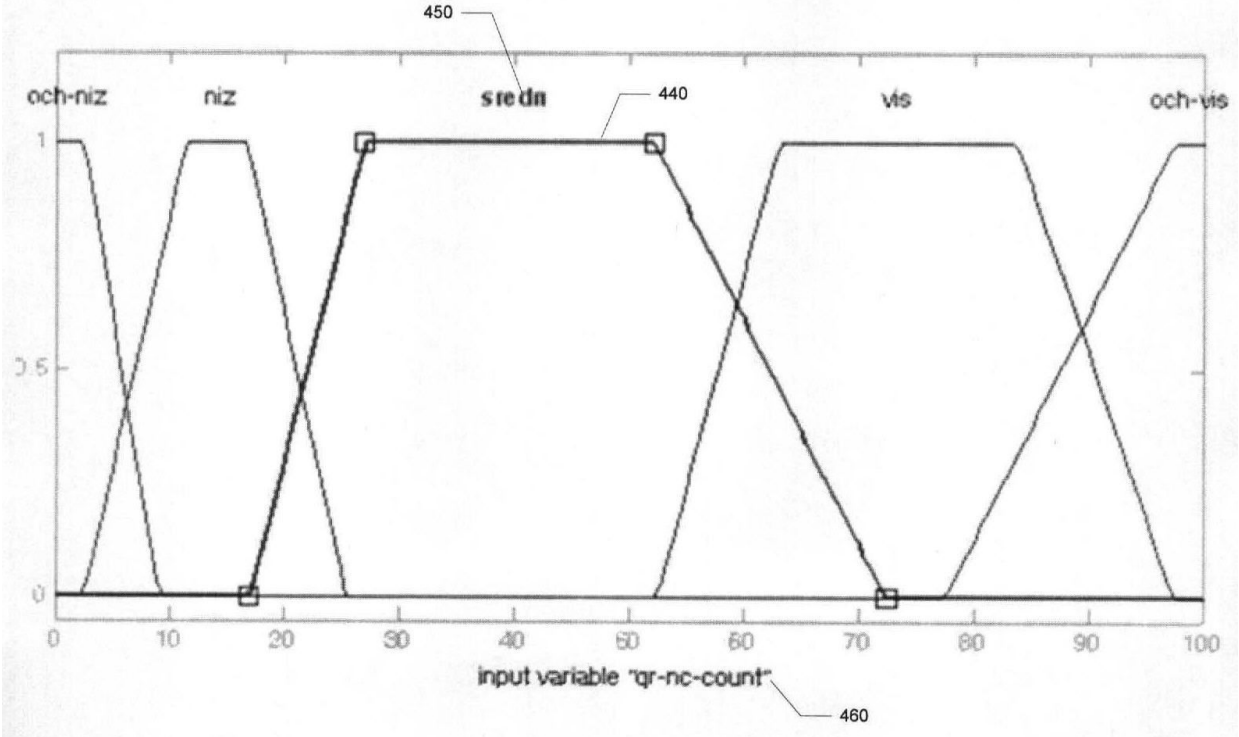
Фиг. 2


Инцидент
220
Предлагаемые действия
230
302
Средство поиска решений
310
320
330
Аналитический модуль 1
Аналитический модуль 2
320
Менеджер аналитики
Модуль принятия решения
320
Аналитический модуль N
311
Экспертные данные

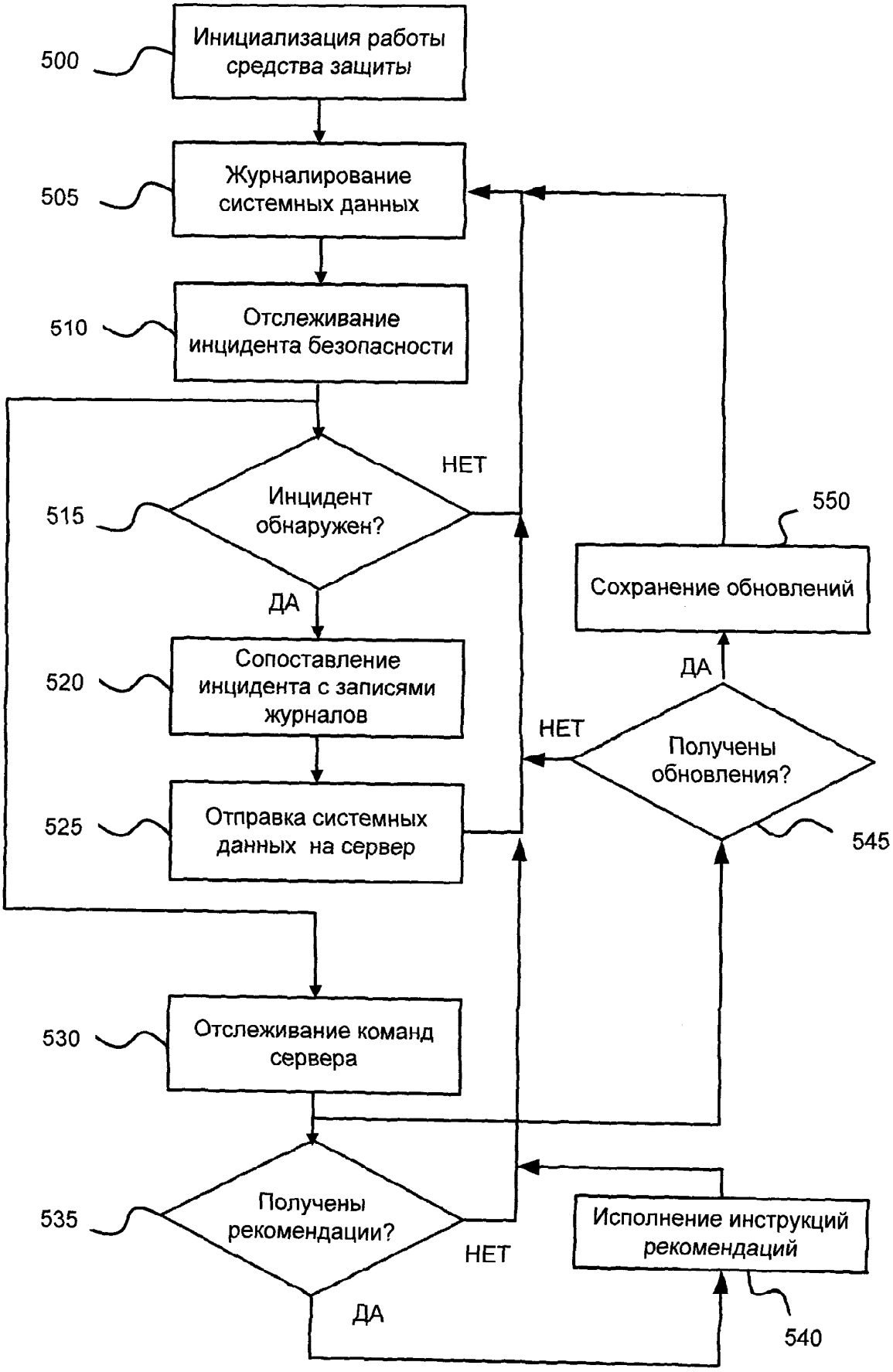
Фиг. 3б


410
qr-nc-count
410
qr-err-count
410
qr-malware-count
410
qr-new-malware-count
410
qr-good-count
420
qr-priority-logic4
(mamdani)
430
qr-priority

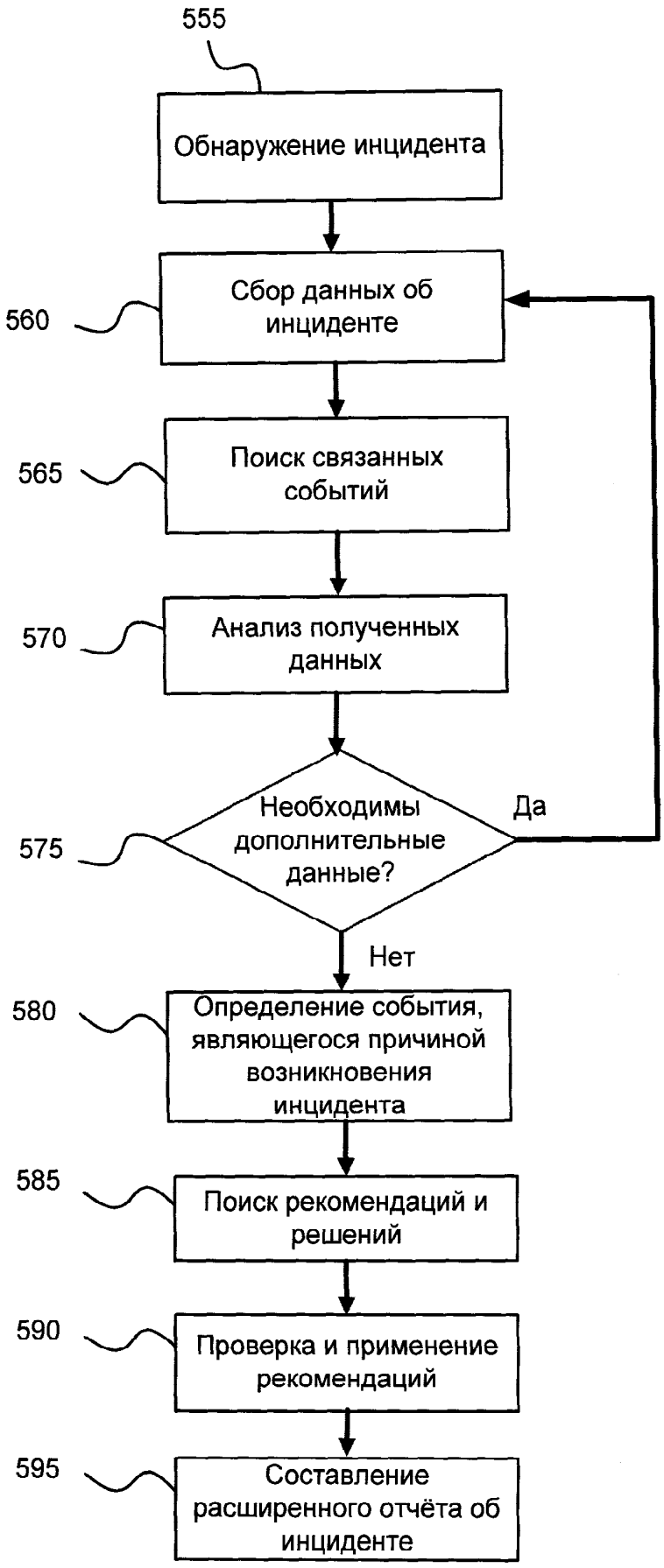
Фиг. 4а


450
och-niz
niz
sredn
440
vis
och-vis
1
0.5
0
0
10
20
30
40
50
60
70
80
90
100
input variable "qr-nc-count"
460

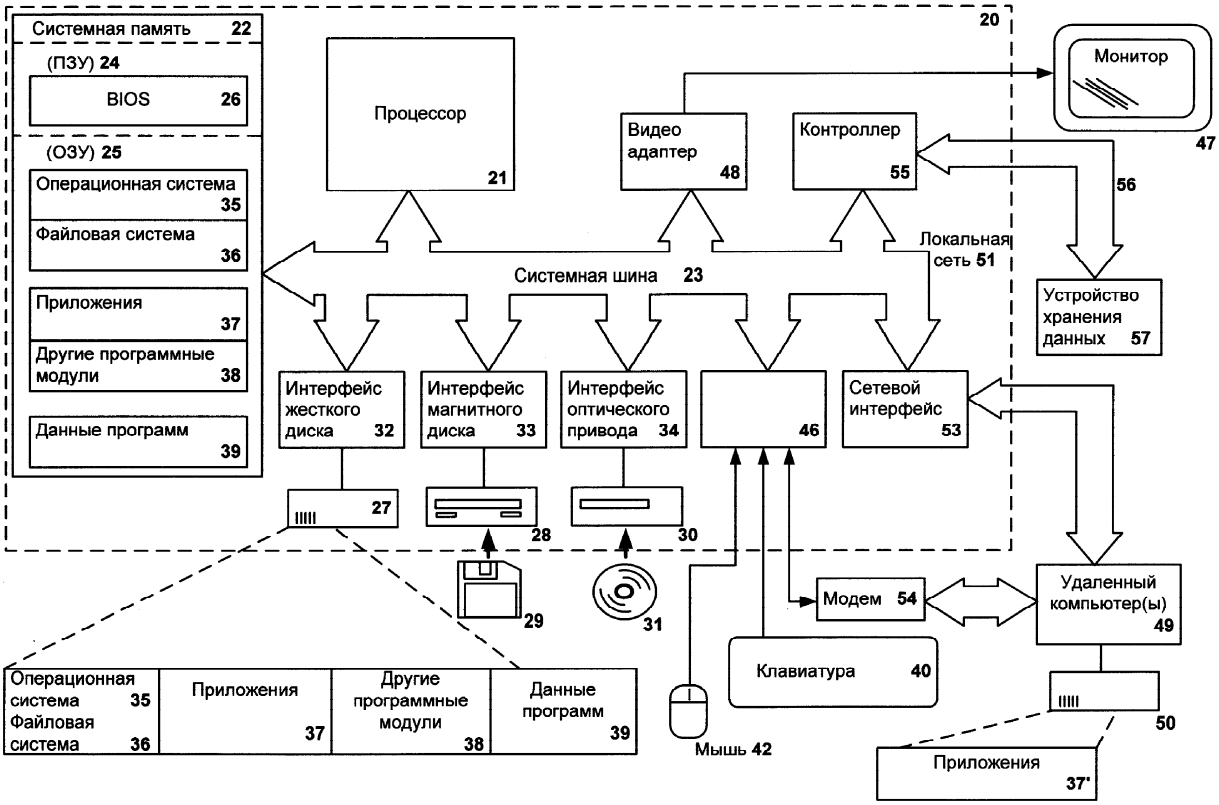
Фиг. 4б


500
Инициализация работы средства защиты
505
Журналирование системных данных
510
Отслеживание инцидента безопасности
515
Инцидент обнаружен?
НЕТ
ДА
520
Сопоставление инцидента с записями журналов
525
Отправка системных данных на сервер
530
Отслеживание команд сервера
535
Получены рекомендации?
НЕТ
ДА
540
Исполнение инструкций рекомендаций
545
Получены обновления?
НЕТ
ДА
550
Сохранение обновлений

Фиг. 5а


555
Обнаружение инцидента
560
Сбор данных об инциденте
565
Поиск связанных событий
570
Анализ полученных данных
575
Необходимы дополнительные данные?
Да
Нет
580
Определение события, являющегося причиной возникновения инцидента
585
Поиск рекомендаций и решений
590
Проверка и применение рекомендаций
595
Составление расширенного отчёта об инциденте

Фиг. 5б


20
Системная память 22
(ПЗУ) 24
BIOS 26
(ОЗУ) 25
Операционная система 35
Файловая система 36
Приложения 37
Другие программные модули 38
Данные программ 39
Процессор 21
Видео адаптер 48
Контроллер 55
Монитор
47
56
Локальная сеть 51
Системная шина 23
Устройство хранения данных 57
Интерфейс жесткого диска 32
Интерфейс магнитного диска 33
Интерфейс оптического привода 34
46
Сетевой интерфейс 53
27
28
30
29
31
Модем 54
Удаленный компьютер(ы) 49
Клавиатура 40
50
Мышь 42
Приложения 37'
Операционная система 35
Файловая система 36
Приложения 37
Другие программные модули 38
Данные программ 39

Фиг. 6