РОССИЙСКАЯ ФЕДЕРАЦИЯ



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 758 041** (13) **C2**

(51) МПК
G06F 21/55 (2013.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/55 (2021.08)

(21)(22) Заявка: **2019126640, 22.01.2018**

(24) Дата начала отсчета срока действия патента:
22.01.2018

Дата регистрации:
25.10.2021

Приоритет(ы):
(30) Конвенционный приоритет:
30.01.2017 US 15/419,933

(43) Дата публикации заявки: **01.03.2021** Бюл. № **7**

(45) Опубликовано: **25.10.2021** Бюл. № **30**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **30.08.2019**

(86) Заявка PCT:
US 2018/014606 (22.01.2018)

(87) Публикация заявки PCT:
WO 2018/140335 (02.08.2018)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, стр. 3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
ЛО, Пэнчэн (US),
БРИГГС, Ривз Хопп (US),
АХМАД, Навид (US)

(73) Патентообладатель(и):
МАЙКРОСОФТ ТЕКНОЛОДЖИ ЛАЙСЕНСИНГ, ЭлЭлСи (US)

(56) Список документов, цитированных в отчете о поиске: **US 2015067857 A1, 05.03.2015. US 8776229 B1, 08.07.2014. US 2009300765 A1, 03.12.2009. US 2006230289 A1, 12.10.2006. RU 2523114 C2, 20.07.2014.**

(54) ПОСТОЯННОЕ ОБУЧЕНИЕ ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ

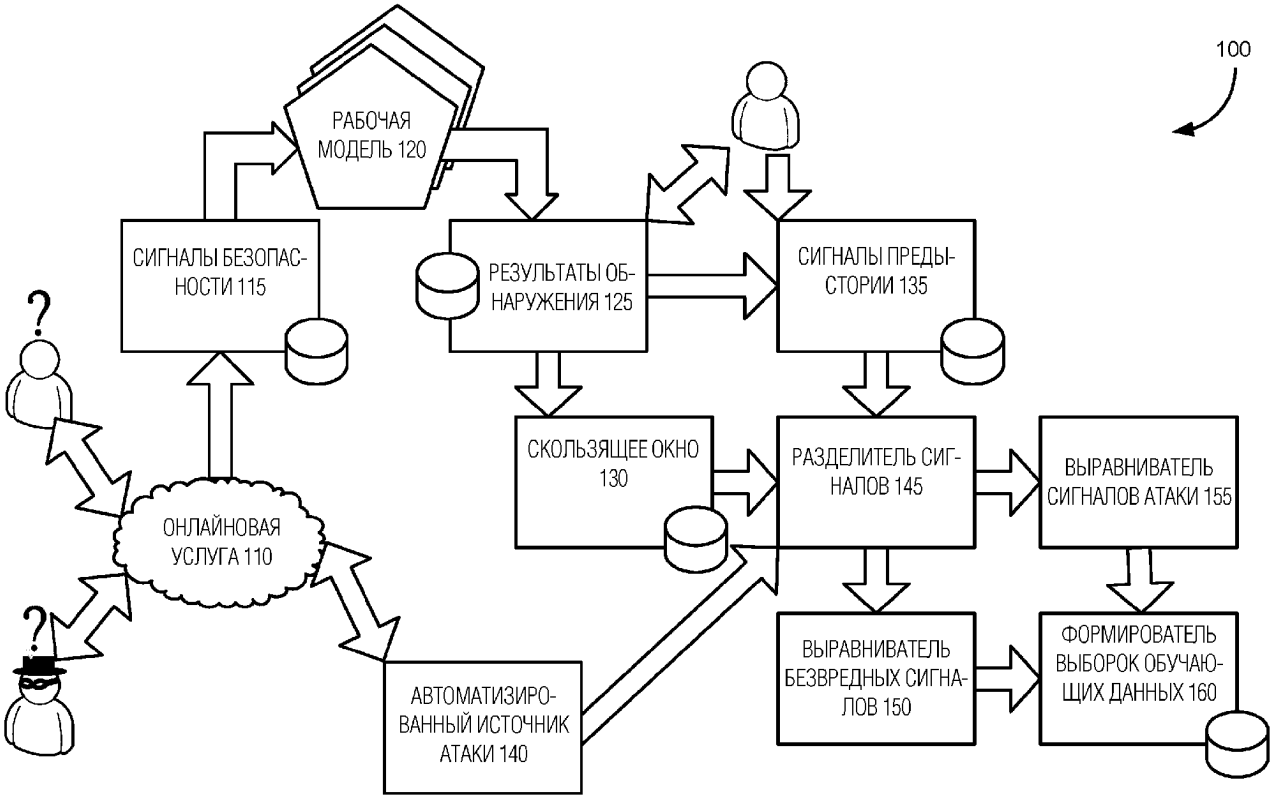
(57) Реферат:

Данное изобретение относится к области обеспечения безопасности сети. Технический результат заключается в обеспечении более надежной и быстрой идентификации новых форм атак, повышения безопасности сети, а также снижения ресурсов обработки, используемых для защиты сети от злоумышленных сторон. Такой результат достигается за счет способа обеспечения безопасности онлайновой услуги, предоставляемой через сеть, посредством модели с постоянным обучением, содержащего: сбор набора сигналов безопасности от онлайновой услуги, причем набор сигналов безопасности собирают в скользящем окне времени; идентификацию того, является ли каждый сигнал безопасности из набора сигналов безопасности вредоносным или безвредным; создание сбалансированного обучающего набора данных для скользящего окна времени посредством: обеспечения баланса вредоносных сигналов из набора сигналов безопасности на основе типа атаки, идентифицированного для каждого вредоносного сигнала, обеспечения баланса безвредных сигналов из набора сигналов

RU 2758041 C2

RU 2758041 C2

безопасности, чтобы создать сбалансированный обучающий набор данных на основе типа устройства, от которого принят каждый безвредный сигнал, и обеспечения баланса вредоносных сигналов с безвредными сигналами посредством перекрестного соединения вредоносных сигналов с безвредными сигналами; и создание предсказательной модели на основе сбалансированного обучающего набора данных, причем, в ответ на прием дополнительного сигнала безопасности, связанного с новым сетевым сеансом, от онлайновой услуги, предсказательная модель применяется для определения того, является ли этот дополнительный сигнал безопасности вредоносным или безвредным. 3 н. и 17 з.п. ф-лы, 5 ил.



ФИГ. 1А

RU 2758041 C2

RU 2758041 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 758 041** (13) **C2**

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

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/55 (2021.08)

(21)(22) Application: **2019126640, 22.01.2018**

(24) Effective date for property rights:
22.01.2018

Registration date:
25.10.2021

Priority:
(30) Convention priority:
30.01.2017 US 15/419,933

(43) Application published: **01.03.2021** Bull. № **7**

(45) Date of publication: **25.10.2021** Bull. № **30**

(85) Commencement of national phase: **30.08.2019**

(86) PCT application:
US 2018/014606 (22.01.2018)

(87) PCT publication:
WO 2018/140335 (02.08.2018)

Mail address:
129090, Moskva, ul. B. Spasskaya, 25, str. 3, OOO "Yuridicheskaya firma Gorodisskij i Partnery"

(72) Inventor(s):
LUO, Pengcheng (US),
BRIGGS, Reeves Hoppe (US),
AHMAD, Naveed (US)

(73) Proprietor(s):
MICROSOFT TECHNOLOGY LICENSING, LLC (US)

RU 2758041 C2

(54) CONSTANT TRAINING FOR INTRUSION DETECTION

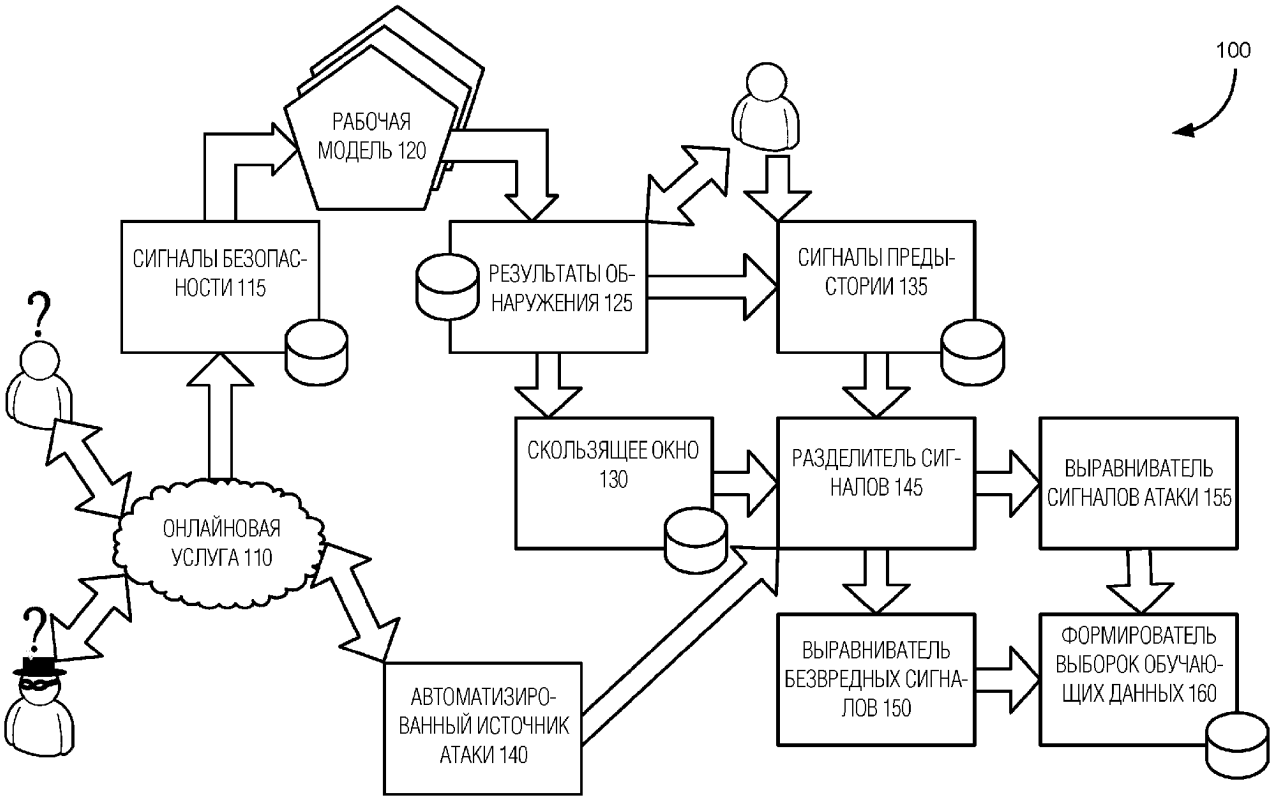
(57) Abstract:

FIELD: network security.

SUBSTANCE: method for ensuring the security of an online service provided through a network, by means of a model with constant training, contains: collecting a set of security signals from the online service, wherein the set of security signals is collected in a sliding time window; identifying, whether each security signal from the set of security signals is malicious or harmless; creating a balanced training dataset for the sliding time window by: balancing malicious signals from the set of security signals based on an attack type identified for each malicious signal, balancing harmless signals from the set of security signals to create the balanced training dataset based on a type of device from which each harmless signal is received, and balancing malicious signals with harmless signals by cross-linking malicious signals with harmless signals; and creating a predictive model based on the balanced training dataset, wherein, in response to receiving an additional security signal associated with a new network session from the online service, the predictive model is used to determine, whether this additional security signal is malicious or harmless.

EFFECT: providing more reliable and fast identification of new forms of attacks, increase in network security, as well as reduction in processing resources used to protect the network from malicious parties.

RU 2758041 C2



ФИГ. 1А

RU 2758041 C2

RU 2758041 C2

ПРЕДШЕСТВУЮЩИЙ УРОВЕНЬ ТЕХНИКИ

[0001] Компьютерные сети находятся под постоянной угрозой от злоумышленных сторон, осуществляющих попытки несанкционированного доступа к системам, размещенным на них. Тактика, используемая злоумышленными сторонами для злонамеренного действия на сети, и тактика, используемая администраторами сети для защиты от злонамеренных действий, постоянно развиваются с учетом друг друга; к арсеналу средств злоумышленных сторон добавляются новые эксплойты, и неэффективные эксплойты удаляются. Реализация контрмер, однако, часто является реагирующей на действия, причем администраторы сети должны ожидать идентификации новейшего эксплойта до развертывания контрмеры и определения, когда останавливать развертывание контрмеры, если соответствующий эксплойт более не используется. Идентификация корректно и блокирование новейших эксплойтов часто представляют сложность для администраторов сети, особенно когда эксплойт еще не является широко распространенным или ведет атаку на небольшое количество услуг, предлагаемых в сети.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

[0002] Эта краткое описание приведено, чтобы в упрощенной форме ввести подборку понятий, которые дополнительно описаны ниже в разделе Подробного описания изобретения. Эта краткое описание не предназначено идентифицировать все ключевые или существенные признаки заявленного изобретения, и при этом оно также не подразумевается поддержкой в определении объема заявленного изобретения.

[0003] Системы, способы и компьютерные устройства хранения данных, включающие в себя команды, предлагаются здесь, чтобы обеспечивать постоянное обучение для обнаружения вторжения. Множество моделей машинного обучения постоянно повторно обучаются на сигналах сети на основе собранных от машин и устройств в сети сигналов, представляющих злонамеренные действия и безвредное поведение. Скользящее окно используется, чтобы собирать сигналы, так что модели используют самые новые данные, чтобы идентифицировать атаки, и модели постоянно переводят с повышением и понижением, чтобы защищать сети, если их способности точно обнаруживать атаки повышаются и понижаются в ответ на состав новейших данных. Модели, развернутые в активных сетях производственного предприятия, предоставляют свои обнаружения почти в реальном времени специалистам-аналитикам по безопасности, которые обеспечивают обратную связь по доле правильных результатов (accuracy) моделей (например, пропущенных вторжений/ ложно отрицательных результатов, ложно утвердительных результатов, неудачно идентифицированных вторжений), чтобы дополнительно уточнять, каким образом модели обучаются.

[0004] Для повышения надежности обучающего набора данных, используемого, чтобы постоянно повторно обучать и уточнять модели обнаружения, и тем самым улучшать модели, обеспечивают баланс сигналов атаки, чтобы решить проблему их недостаточного количества по сравнению с безвредным сигналом и в отношении конкретных типов атак. Безвредные сигналы перекрывают сигналами атаки различных типов от других машин, чтобы обеспечить сбалансированный обучающий набор для обучения и уточнения моделей. Среди сигналов атаки в сбалансированном обучающем наборе сигналы различных типов атаки также сбалансированы, чтобы гарантировать, что модель одинаково обучается на всех типах атак. Признаки (features) сигналов динамически выделяют при посредстве текстовой конфигурации, таким образом, повышая гибкость моделей, чтобы реагировать на различные наборы признаков, указывающие атаку на сеть.

[0005] В различных аспектах, атаки имитируются посредством известного внутреннего «источника атаки», чтобы повышать готовность сети и генерировать добавочные сигналы атаки. Подобным образом, исторически значимые сигналы атаки используются в некоторых аспектах с тем, что даже если сигналы атаки конкретного типа не наблюдались в скользящем окне, эти сигналы представляются на модели.

[0006] Путем обеспечения для сети моделей обнаружения вторжения с постоянным обучением, функциональные возможности устройств и программного обеспечения в сети улучшаются. Новые формы атак идентифицируют быстрее и более надежно, таким образом, решая сцентрированную на компьютере проблему, каким образом повысить безопасность сети. Кроме того, вычислительные ресурсы не расходуются непроизводительно в попытке обнаруживать исключенные формы атаки, таким образом, снижая ресурсы обработки, используемые для защиты сети от злоумышленных сторон.

[0007] Примеры реализованы в виде процесса компьютера, вычислительной системы, или в виде изделия такого как устройство, компьютерный программный продукт или читаемый компьютером носитель. Согласно аспекту, компьютерный программный продукт является компьютерным носителем данных, который считывается компьютерной системой и на котором закодирована компьютерная программа, содержащая команды для выполнения компьютерного процесса.

[0008] Подробности одного или более аспектов изложены на сопроводительных чертежах и в описании ниже. Другие признаки и преимущества будут очевидны из рассмотрения последующего подробного описания и анализа связанных с ним чертежей. Должно быть понято, что последующее подробное описание является лишь пояснительным и не является ограничительным для формулы изобретения.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0009] Сопроводительные чертежи, которые включены в это раскрытие и составляют его часть, иллюстрируют различные аспекты. На чертежах:

Фиг.1А - примерная система обеспечения безопасности, с помощью которой может быть практически осуществлено настоящее раскрытие;

Фиг.1В - примерная система обучения и выбора модели для использования с примерной системой обеспечения безопасности по Фиг.1А, с помощью которой может быть практически осуществлено настоящее раскрытие;

Фиг.2 - структурная схема, показывающая общие этапы, включенные в примерный способ для разработки обучающего набора данных, посредством которого обучать предсказательные модели для использования в обеспечении безопасности онлайновой услуги;

Фиг.3 - структурная схема, показывающая общие этапы, включенные в примерный способ для обучения и выбора предсказательных моделей для использования в обеспечении безопасности онлайновой услуги; и

Фиг.4 - структурная схема, иллюстрирующая примерные физические компоненты вычислительного устройства.

ПОДРОБНОЕ ОПИСАНИЕ СУЩНОСТИ ИЗОБРЕТЕНИЯ

[0010] Следующее подробное описание ссылается на сопроводительные чертежи. По возможности, на чертежах используются одинаковые ссылочные позиции, и следующее описание ссылается на такие же или подобные элементы. Хотя примеры могут быть описаны, являются возможными модификации, адаптации и другие реализации. Например, замены, дополнения или модификации могут делаться по отношению к элементам, иллюстрируемым на чертежах, и способы, описанные здесь, могут модифицироваться путем замещения, изменения порядка следования или

добавления этапов к раскрытым способам. Соответственно, следующее подробное описание не является ограничительным, а взамен, надлежащий объем определяется прилагаемой формулой изобретения. Примеры могут принимать форму аппаратной реализации, или полностью программной реализации, или реализации, объединяющей аспекты программного и аппаратного обеспечения. Следующее подробное описание, следовательно, не должно пониматься в ограничительном смысле.

[0011] Здесь рассматриваются системы, способы и машиночитаемые устройства хранения данных, включающие в себя команды, чтобы обеспечивать улучшенную безопасность сети при посредстве моделей обнаружения вторжения с постоянным обучением. Путем обеспечения для сети моделей обнаружения вторжения с постоянным обучением, функциональные возможности устройств и программного обеспечения в сети улучшаются. Новые формы атак идентифицируют быстрее и более надежно, таким образом, решая сцентрированную на компьютере проблему, каким образом повысить безопасность сети. Кроме того, вычислительные ресурсы не расходуются непроизводительно в попытке обнаруживать исключенные формы атаки, таким образом, снижая ресурсы обработки, используемые для защиты сети от злоумышленных сторон.

[0012] Фигура Фиг.1А являет собой примерную систему 100 обеспечения безопасности, с помощью которой может быть осуществлено настоящее раскрытие. Как показано на Фиг.1А, онлайновая услуга 110 подключается различными пользователями - который может быть безвредным или злоумышленным - и системой 100 обеспечения безопасности. Онлайновая услуга 110 представляет организованный в сеть набор вычислительных устройств, таких как облачный центр обработки данных, который предоставляет различным пользователям "облачные" услуги, включая, но без ограничения указанным: Инфраструктуру как услугу (IaaS), где пользователь обеспечивает операционную систему и программное обеспечение, работающие на устройствах онлайновой услуги 110; Платформу как услугу (PaaS), где пользователь обеспечивает программное обеспечение, и онлайновая услуга 110 обеспечивает операционную систему и устройства; или Программное обеспечение как услугу (SaaS), где онлайновая услуга 110 обеспечивает и операционную систему, и программное обеспечение для работы на устройствах для пользователей. Пользователи, которые добиваются доступа к онлайновой услуге 110, могут быть легальными пользователями или злоумышленными сторонами, которые используют уязвимости системы обеспечения безопасности для проникновения в онлайновую услугу 110, чтобы исполнять несанкционированные процессы и/или осуществлять поиск и выборку данных из онлайновой услуги 110 без легальной авторизации.

[0013] Для определения, являются ли пользователи безвредными или злоумышленными, или являются ли устройства безвредными (не посылающими вредоносные сигналы) или скомпрометированными (посылающими вредоносные сигналы), различные сигналы 115 безопасности от онлайновой услуги 110 собирают и подают в рабочие (production) модели 120, чтобы создать результаты 125 обнаружения, указывающие, является ли данный сеанс злоумышленным или безвредным. Сигналы 115 безопасности включают в себя журналы регистрации событий, трассы состояний сети, системные команды и подобное, каковые анализируются посредством рабочих моделей 120 относительно характеристик, и значения их признаков определяются посредством обучения рабочих моделей 120, чтобы являться указателем злоумышленного или безвредного поведения. С целью настоящего раскрытия конкретные сигналы 115 безопасности именуются являющимися "вредоносными" (malicious) или "безвредными" (benign) на основе действий в онлайновой услуге 110,

связанных с генерацией конкретного сигнала 115 безопасности. Кроме того, как используется здесь, термин "признак" является числовым атрибутом, получаемым исходя из одного или более входных сигналов, относящихся к характеристике или поведению, наблюдаемым в сети, которые воспринимаются "моделью", являющейся алгоритмом, который воспринимает набор признаков (также именуемых признаками модели), задаваемый аналитиком, чтобы преобразовывать значения признаков в прогнозную оценку или достоверность, указывают ли признаки вредоносную или безвредную активность.

[0014] Сигналы 115 безопасности предоставляются на рабочие модели 120, чтобы выделять различные признаки из сигналов 115 безопасности, для какового рабочие модели 120 были обучены идентифицировать вредоносные активности на онлайновой услуге 110. Сигнал 115 безопасности являет собой совокупность из одного или более связанных событий, происходящих на устройствах в рамках онлайновой услуги 110, и может включать в себя несколько признаков (например, используемый порт, подключенный IP-адрес, идентификационные данные/тип устройства, от которого сигнал принимается, пользователь, предпринятое действие), из какового выделяют подмножество для исследования посредством данной рабочей модели 120 для определения, является ли сигнал 115 безопасности безвредным или вредоносным. Признаки от одного или более сигналов 115 безопасности объединяют в вектор признаков для анализа, и в различных аспектах, признаки могут быть оценены, чтобы обеспечивать численный анализ этого признака для ввода в рабочие модели 120.

[0015] Например, данный IP (Протокол Internet) адрес может оцениваться на основе его частоты использования, где более частое использование данного IP-адреса во время скользящего окна 130 будет изменять значение, предоставляемое на рабочую модель 120, по сравнению с менее частым использованием. Напротив, если осуществляется доступ к секретному файлу, предпринимается запрещенное действие, обращаются к занесенному в черный список IP-адресу, и т.д., двоичная оценка, указывающая, что имело место опасное состояние, может предоставляться на рабочую модель 120 в сигнале 115 безопасности. Рабочие модели 120 не основываются на «белых» списках или «черных» списках, и их обучение, являющееся относительным по отношению к признакам, наблюдаемым в сигналах 115 безопасности, рассматривается более подробно со ссылкой на фигуры Фиг. 1B, 2, и 3, каковому можно обучиться во времени без директивы черного списка или белого списка признаков, которые являются указателем вторжения в онлайновую услугу 110.

[0016] Для данного сигнала 115 безопасности, определение посредством рабочих моделей 120 устанавливает, является ли рассматриваемый сигнал 115 безопасности безвредным или вредоносным. Эти результаты 125 обнаружения связываются с сигналами 115 безопасности, чтобы идентифицировать их либо как вредоносные, либо как безвредные. В некоторых аспектах, по меньшей мере, некоторые из этих результатов 125 обнаружения (например, результаты 125 обнаружения вредоносных) предоставляются пользователю-аналитику, который может действовать на результатах 125 обнаружения, чтобы развернуть контрмеры против злоумышленного пользователя или атаки, или определить, что результаты 125 обнаружения обеспечивают оценку другую, чем указывают рабочие модели 120. Например, когда для вредоносного сигнала рабочей моделью 120 был указан ложно отрицательный результат, аналитик может дать оценку, что сигнал является фактически вредоносным, и указать действие, которое следует предпринять. В другом примере, когда для безвредного сигнала был указан ложно положительный результат, аналитик может дать оценку, что сигнал является

фактически безвредным, и указать, что никакое действие не следует предпринимать. В другом примере, когда для вредоносного действия был указан ложно положительный результат, аналитик может указать, что никакое действие или действие, отличающееся от рекомендуемого системой 100 обеспечения безопасности, не должно быть предпринято). Коррекции от аналитиков, таким образом, используются в дальнейшем обучении и улучшении моделей.

[0017] Результаты 125 обнаружения также подаются, в различных аспектах, в базу данных, сохраняющую скользящее окно 130 наблюдаемых сигналов 115 безопасности за последние *d* дней (где *d* допускает возможность настройки пользователем-аналитиком или другим администратором сети, например, как два дня, десять, пятнадцать и т.д. дней), и базу данных, сохраняющую сигналы 135 предыстории для сигналов 115 безопасности, которые должны использоваться для обучения независимо от того, наблюдали ли их в последние *d* дней. Сигналы 135 предыстории курируются пользователем-аналитиком для включения сигналов 115 безопасности, связанных с известными внешними атаками. В дополнительных аспектах, пользователь-аналитик курирует сигналы 135 предыстории для включения безвредных сигналов, которые могут выглядеть подозрительными, или иначе возвращать ложно положительные результаты относительно вторжения в сеть, чтобы гарантировать, что предсказательные модели обучаются корректно отвечать на сигналы, которые исторически оказались трудными, чтобы корректно идентифицировать.

[0018] Автоматизированный источник 140 атаки использует известные шаблоны атак и эксплойты, чтобы проверять обеспечение безопасности онлайновой услуги 110 и предоставлять известные результаты для использования вместе с результатами 125 обнаружения, выдаваемыми рабочими моделями 120. Когда результаты 125 обнаружения для сигнала 115 безопасности, то есть, результат атаки от автоматизированного источника 140 атаки не указывает, что атака была вредоносной, сигнал 115 безопасности будет рассматриваться вредоносным, поскольку автоматизированный источник 140 атаки означает, что он был вредоносным. В различных аспектах автоматизированный источник 140 атаки является необязательным компонентом системы 100 обеспечения безопасности или онлайновой услуги 110.

[0019] Сигналы 115 безопасности (включая таковые в скользящем окне 130 и сигналы 135 предыстории, если доступны) подаются на разделитель 145 сигналов наряду с результатами 125 обнаружения от рабочих моделей 120 (и коррекциями от пользователя-аналитика), указывающими, был ли сигнал 115 безопасности определен являющимся безвредным или вредоносным. Подобным образом в аспектах, в которых развернут автоматизированный источник 140 атаки, идентификационные данные «безвредный/вредоносный» для сигналов 115 безопасности, сгенерированных исходя из его действий на онлайновой услуге 110, обеспечиваются на разделитель 145 сигналов. Разделитель 145 сигналов сконфигурирован, чтобы разделять сигналы 115 безопасности на безвредные сигналы, обеспечиваемые на выравниватель 150 безвредных сигналов, и вредоносные сигналы, обеспечиваемые на выравниватель 155 сигналов атаки.

[0020] Выравниватель 150 безвредных сигналов и выравниватель 155 сигналов атаки дорабатывают набор сигналов 115 безопасности, используемый для заполнения набора данных, используемого формирователем 160 выборок обучающих данных, чтобы обеспечить сбалансированные безвредные и вредоносные сигналы, посредством которых обучать модели для обнаружения новейших эксплойтов онлайновой услуги 110. Формирователь 160 выборок обучающих данных удаляет безвредные сигналы, принятые от скомпрометированных устройств в онлайновой услуге 110, оставляя только

вредоносные сигналы от скомпрометированных устройств. Выполняется перекрестное соединение безвредных сигналов от чистых устройств с вредоносными сигналами от скомпрометированных устройств, приводящее к $B \times M$ примерам атаки, где B представляет число «безвредных» примеров и M - число «вредоносных» примеров. Это дает расширенный набор данных, который налагает примеры атаки на безвредные примеры, как если бы атаки имели место на чистых устройствах.

[0021] Поскольку чистые устройства имеют различные вариации безвредных сигналов, и скомпрометированные устройства имеют различные вариации сигналов атаки, перекрестное соединение обоих наборов данных создает большое число сценариев со значительной вариацией. Однако если сценарии отбираются случайно, как например, посредством автоматизированного источника 140 атаки, в обучающем наборе может присутствовать неравное количество каждого типа атак, каковое может исказить обучение моделей (приводя к предсказанию некоторых атак лучше, чем других). Примеры атак, следовательно, уравнивают по отношению к сценариям атак, чтобы гарантировать, что имеется по существу равное количество (например, ±5%) каждого примера атаки в обучающем наборе. В различных аспектах, в недостаточно представленных типах атаки (то есть, типах атаки в количестве ниже равновесного числа) имеются существующие вредоносные сигналы, размноженные, чтобы повысить их относительное число, и/или в чрезмерно представленных типах атаки (то есть, типах атаки в количестве выше равновесного числа) имеются существующие вредоносные сигналы, удаленные или замененные/перекрытые примерами недостаточно представленных типов атаки, чтобы добиться сбалансированного набора примеров атаки.

[0022] Подобно вредоносным сигналам, безвредные сигналы уравниваются относительно друг друга в отношении типа или роли устройства, от которого сигналы были приняты, так что данный тип или роль устройства не является чрезмерно представленным в обучающем наборе данных (приводя к предсказанию некоторых атак на данных типах/ролях устройства лучше, чем других). Безвредные примеры, следовательно, уравниваются по отношению к имеющемуся типу устройства, чтобы гарантировать, что имеется по существу равное (например, ±5%) количество каждого типа устройства, обеспечивающего безвредные примеры. В различных аспектах, в недостаточно представленных типах устройства (то есть, типах устройства в количестве ниже равновесного числа) имеются существующие безвредные сигналы, размноженные для повышения их относительного числа, и/или в чрезмерно представленных типах устройства (то есть, типах устройства в количестве выше равновесного числа) имеются существующие безвредные сигналы, удаленные или замененные/перекрытые безвредными примерами из недостаточно представленных типов устройства, чтобы добиться сбалансированного набора безвредных примеров.

[0023] Фиг.1В являет собой примерную систему 105 обучения и выбора модели для использования с примерной системой 100 обеспечения безопасности по Фиг.1А, с помощью которой может быть осуществлено настоящее раскрытие. Сбалансированный набор данных безвредных и вредоносных сигналов от формирователя 160 выборок обучающих данных обеспечивается на разделитель 165 обучение/испытание, чтобы и обучать, и оценивать различные модели, посредством чего обеспечивать безопасность онлайновой услуги 110. Набор данных разделяется на k подмножеств, где k-1 имеющихся подмножеств (например, две трети) используются, чтобы обучать модели, и одно подмножество набора данных (например, одна треть) зарезервировано, чтобы оценивать модели. В различных аспектах предусматриваются различные доли для разделения

набора данных на подмножества обучения и оценивания, которые предоставляются на блок 170 обучения модели и блок 175 оценивания модели, соответственно.

[0024] Блок 170 обучения модели сконфигурирован, чтобы обучать множество соответствующих стадии разработки (development) моделей 180 с помощью одного или более способов машинного обучения при помощи обучающего подмножества сбалансированных данных. Способы машинного обучения обучают модели точно делать предсказания на данных, подаваемых в модели (например, являются ли сигналы 115 безопасности безвредными или вредоносными; является ли имя существительное человеком, местом или предметом; на что будет походить погода завтра). В ходе фазы обучения, модели разрабатываются по отношению к обучающему набору данных известных входов (например, выборки *A*, выборки *B*, выборки *C*), чтобы оптимизировать модели для корректного предсказания выхода для данного входа. Обычно фаза обучения может быть контролируемой, полуконтролируемой или неконтролируемой; означая убывающий уровень на который "корректные" выходы обеспечиваются в соответствии с обучающими входами. В контролируемой фазе обучения все из выходов обеспечиваются на модель, и моделью руководят для разработки общего правила или алгоритма, который отображает вход на выход. Напротив, в неконтролируемой фазе обучения, требуемый выход не обеспечивается для входов, так что модель может разработать свои собственные правила для обнаружения связей в рамках обучающего набора данных. В полуконтролируемой фазе обучения, обеспечивается не полностью помеченный обучающий набор, с некоторыми из выходов известными и некоторыми неизвестными для обучающего набора данных.

[0025] Модели могут исполняться по отношению к обучающему набору данных для нескольких циклов, в которых обучающий набор данных повторно подается в модель для уточнения ее результатов. Например, в контролируемой фазе обучения, модель разрабатывается, чтобы предсказывать выход для данного набора входов, и оценивается по нескольким циклам, чтобы более надежно обеспечивать выход, который обозначается как соответствующий данному входу для наибольшего числа входов для обучающего набора данных. В другом примере, для неконтролируемой фазы обучения, модель разрабатывается для кластеризации набора данных на *n* групп и оценивается по нескольким циклам, насколько непротиворечиво она помещает данный вход в данную группу и насколько надежно она создает *n* требуемых кластеров по каждому циклу.

[0026] В различных аспектах, перекрестная проверка применяется поверх каждой обучающей фазы, где порция обучающего набора данных используется в качестве набора данных для оценивания. Например, обучающий набор данных может быть разделен на *k* сегментов, где (*k*-1) сегментов используются в обучающих циклах, и оставшийся сегмент используется для определения, насколько хорошо выполнены обученные модели. Таким образом, каждая модель обучается по отношению к каждой имеющейся комбинации входных параметров, так что каждая модель обучается *k* раз, и параметры лучшей модели выбирают на основе их средних рабочих характеристик по циклам.

[0027] Как только цикл исполняется, модели оцениваются, и значения их переменных корректируются, чтобы добиться лучшего уточнения модели. В различных аспектах, оценки являются смещенными к ложным отрицательным, смещенными к ложным положительным или равномерно смещенными по отношению к общей точности модели. Значения могут корректироваться несколькими способами в зависимости от используемой методики машинного обучения. Например, в генетическом или эволюционном алгоритме, значения для моделей, которые являются наиболее

успешными в предсказании требуемых выходов, используются для разработки значений для моделей, чтобы использовать в ходе последующего цикла, каковое может включать в себя случайное изменение/мутацию, чтобы обеспечить добавочные точки данных. Средний специалист в данной области техники будет знать несколько других алгоритмов машинного обучения, которые могут применяться с настоящим раскрытием, включая обучение с применением линейной регрессии, случайных лесов, дерева решений, нейронных сетей и т.д.

[0028] Модель разрабатывает правило или алгоритм по нескольким циклам путем изменения значений одной или более переменных, влияющих на входы, чтобы более близко отображать на требуемый результат, но поскольку обучающий набор данных может быть изменен и является предпочтительно очень большим, совершенные метрики доли правильных результатов и точности могут не быть достижимыми. Число циклов, которые составляют фазу обучения, следовательно, может задаваться в виде заданного числа пробных испытаний или фиксированного временного/вычислительного ресурса, или может быть прекращено до достижения этого числа/ресурса, когда доля правильных результатов данной модели является достаточно высокой или достаточно низкой, или была достигнута стабилизация доли правильных результатов. Например, если обучающая фаза спроектирована, чтобы исполнять *n* циклов и создавать модель с, по меньшей мере, долей правильных результатов в 95%, и если такая модель создается до n-го цикла, фаза обучения может окончиться преждевременно и использовать созданную модель, удовлетворяющую конечному целевому порогу точности. Подобным образом, если данная модель является достаточно неточной, чтобы удовлетворять произвольному случайному порогу (например, модель является точной только 55% в определении выходов истина/ложь для данных входов), фаза обучения для этой модели может быть завершена преждевременно, хотя другие модели, находящиеся в фазе обучения, могут продолжать обучение. Подобным образом, когда данная модель продолжает обеспечивать одинаковую точность или ее результаты колеблются по множеству циклов - достигнув плоского участка рабочей характеристики - фаза обучения для данной модели может завершиться до достижения числа циклов/вычислительного ресурса.

[0029] Как только фаза обучения является завершенной, модели приводят в окончательную форму. Приведенные к окончательным модели оценивают по отношению к критериям проверки. В первом примере тестовый набор данных, который включает в себя известные выходы для своих входов, подается в окончательные модели, чтобы определить точность моделей в обработке данных, на которых они не обучались. Во втором примере, относительное число ложноположительных, относительное число ложно отрицательных результатов могут использоваться, чтобы оценивать модели после приведения в окончательную форму. В третьем примере используется очерчивание между образованиями кластеров, чтобы выбирать модель, которая дает самые четкие границы для своих кластеров данных. В других примерах оцениваются добавочные метрики моделей, такие как площади под кривыми точности и полноты.

[0030] Модели 180 стадии разработки (и, следовательно, рабочие модели 120) являются предсказательными моделями, которые первоначально разрабатываются посредством конфигуратора 185 признаков модели на основе отборов, выполненных административным пользователем. Административный пользователь отбирает один или более признаков сигнала 115 безопасности, которые подлежат прослушиванию на устройствах онлайновой услуги 110, и каким способом эти признаки должны анализироваться, чтобы выразить, является ли данный сигнал 115 безопасности вредоносным или безвредным. В различных аспектах, признаки предоставляются в

структурированных текстовых файлах (например, с использованием меток Расширяемого языка разметки гипертекста (XML) или нотации Объектов JavaScript (JSON)), из которых административный пользователь может отбирать для задания набора признаков для новой модели 180 стадии разработки. На основе конфигурации признаков, признаки динамически выделяют в виде вектора признаков из данного набора сигналов безопасности для устройства. Различные признаки могут быть выделены для различных моделей на основе их соответственной конфигурации признаков. Структурированные текстовые файлы, следовательно, позволяют административному пользователю добавлять к модели или модифицировать признаки и то, каким образом их исследуют, без необходимости добавлять код к базе кодов или модифицировать таковой; структурированный текстовый файл позволяет вызывать сегменты кода из базы кодов, которая может быть расширена или модифицирована разработчиком, чтобы доставлять административному пользователю новые типы признаков для отбора из них. Например, административный пользователь может отбирать в качестве признака тип исследования для использования с данным параметром или поле данных из сигналов 115 безопасности: общее число различных значений в наборе данных (Count), максимальное значение в наборе данных (Max), подсчет наиболее часто встречающегося значения в списке (MaxCount), максимальную сумму значений в списке, которая не превышает предельное значение (MaxSum), и т.д. Примеры полей данных/параметров для наблюдения в сигналах безопасности, включают в себя, но без ограничения: виды сигналов (например, утечка данных, попытки входа в систему, запросы доступа к заданным файлам), используемые порты, байты, используемые в процессе/связи, байты, переданные по данному IP-адресу (протокола Internet) /от него и запись порта, идентификатор пользователя, находится ли данный IP-адрес или действие в черном списке или белом списке, и т.д.

[0031] Блок 175 оценивания модели сконфигурирован для оценивания моделей 180 стадии разработки для определения, какие модели должны использоваться в качестве рабочих моделей 120 в системе 100 обеспечения безопасности. В различных аспектах, рабочие модели 120 повторно включаются в модели 180 стадии разработки для оценивания, или пороги точности рабочих моделей 120 используются для определения, заменять ли данную рабочую модель 120 моделью 180 стадии разработки. В других аспектах, модели 180 стадии разработки сравнивают с рабочими моделями 120 в отношении других метрик, таких как, например, доля правильных результатов, площади под кривыми точности и полноты, и т.д., в которых лучшие модели отбирают в качестве продвигаемых моделей 190 для использования в качестве рабочих моделей 120. Модели могут постоянно переводиться с повышением из моделей 180 стадии разработки в рабочие модели 120 (и с понижением из рабочих моделей 120 в модели 180 стадии разработки), по мере того, как блок 175 оценивания модели определяет их эффективность в корректной идентификации вредоносных сигналов как вредоносные и безвредных сигналов как безвредные. В различных аспектах, первые *n* наиболее точных моделей 180 стадии разработки или все модели 180 стадии разработки с превышением порога точности переводятся как продвигаемые модели 190 в рабочие модели 120. В других аспектах административный пользователь может вручную переводить модель 180 стадии разработки в рабочую модель 120, как, например, когда никакая другая модель не осуществляет мониторинг данного признака сигналов 115 безопасности.

[0032] Система 100 обеспечения безопасности, система 105 обучения и выбора модели, и их соответственные составляющие элементы являются иллюстративными для множества вычислительных систем, включая, без ограничения, системы настольных

компьютеров, проводные и беспроводные вычислительные системы, мобильные вычислительные системы (например, мобильные телефоны, нетбуки, компьютеры планшетного или сверхтонкого типа, блокнотные компьютеры и переносные компьютеры), ручные устройства, мультипроцессорные системы, микропроцессорную или программируемую бытовую электронику, миникомпьютеры, принтеры, и большие ЭВМ. Аппаратные средства этих вычислительных систем рассматриваются более подробно в отношении Фиг.4.

[0033] Хотя составляющие элементы системы 100 обеспечения безопасности и системы 105 обучения и выбора модели показаны удаленно друг от друга в иллюстративных целях, следует отметить, что являются возможными несколько конфигураций из одного или более этих устройств, размещенных локально по отношению к другому иллюстрируемому устройству, и каждое иллюстрируемое устройство может представлять множество экземпляров этого устройства. Различные серверы и посредники, известные средним специалистам в данной области техники, могут находиться между составляющими элементами, иллюстрируемыми на фигурах Фиг. 1А и 1В, для маршрутизации передач между этими системами, которые не проиллюстрированы, чтобы не отвлекать от аспектов новизны настоящего раскрытия.

[0034] Фиг.2 являет собой структурную схему, показывающую общие этапы, включенные в примерный способ 200 для разработки обучающего набора данных, посредством которого обучать предсказательные модели для использования в обеспечении безопасности онлайновой услуги 110. Способ 200 начинается с ОПЕРАЦИИ 210, где собирают сигналы 115 безопасности. В различных аспектах, сигналы 115 безопасности могут приниматься в реальном времени (или почти в реальном времени, учитывая задержки обработки и передачи) или могут приниматься и кэшироваться в базе данных для периодического анализа, такого как, например, в периодическом процессе для анализа событий безопасности каждые m минут. Сигналы 115 безопасности включают в себя прослушиваемые события и параметры различных действий, имеющих место на машинах в онлайновой услуге 110.

[0035] Прослушиваемые события и параметры используются в ОПЕРАЦИИ 220, чтобы идентифицировать, соответствует ли данный сигнал 115 безопасности действию, которое является вредоносным или безвредным. В различных аспектах, собранные сигналы 115 безопасности подаются на предсказательные модели, обозначенные для использования с оперативными онлайновыми услугами 110 (то есть, рабочие модели 120), чтобы определить, является ли каждый сигнал 115 безопасности вредоносным или безвредным. Эти определения представляют пользователям-аналитикам, которые могут действовать на основе определений, чтобы защитить онлайновую услугу 110 от злоумышленной стороны, но могут также отменять определение, сделанное предсказательными моделями; указывая, что определение является ложноположительным или ложно отрицательным результатом. Подобным образом в аспектах, где автоматизированный источник 140 атаки используется для имитации атаки на онлайновую услугу 110, автоматизированный источник 140 атаки обеспечивает уведомление, которое идентифицирует сигналы 115 безопасности, созданные в ответ на атаку, как вредоносные, так что эти сигналы 115 безопасности рассматриваются вредоносными независимо от результатов обнаружения от предсказательных моделей.

[0036] В ОПЕРАЦИИ 230 задается скользящее окно 130, чтобы определить временной интервал от текущего момента времени, в котором анализировать сигналы 115 безопасности, релевантные для новейших эксплойтов и атак, исполняемых на онлайновую услугу 110. Скользящее окно 130 определяет набор сигналов 115

безопасности, попадающих в обозначенный интервал времени от текущего момента времени; причем сигналов 115 безопасности, собранных в рамках последних *d* дней. Окно из нескольких дней используется для обучения и предсказания медленных атак, выполняемых за несколько дней, чтобы избегать обнаружения посредством обычных систем обеспечения безопасности. По мере того, как сигналы 115 безопасности собирают, самые недавние сигналы безопасности добавляются к набору сигналов 115 безопасности для скользящего окна 130, и сигналы 115 безопасности, которые были собраны до обозначенного периода времени для скользящего окна 130, постоянно удаляются из набора сигналов 115 безопасности.

[0037] В некоторых аспектах, сигналы 135 предыстории необязательно принимаются в ОПЕРАЦИИ 240. Сигналы 135 предыстории курирует пользователь-аналитик на основе предварительно полученных наблюдением сигналов 115 безопасности, чтобы включить исторически значимые сигналы 115 безопасности, которые представляют некоторые типы атак или безвредные варианты использования, которые обозначены для целей обучения, независимо от того, были ли замечены подобная атака или вариант использования во временной интервал скользящего окна 130. В одном примере, у исторически опасного эксплойта могут иметься сигналы 115 безопасности, связанные с его обнаружением, добавленные к сигналам 135 предыстории, чтобы постоянно оставаться на защите от этого эксплойта. В другом примере, разработчик может выявить эксплойт «нулевого дня» и не знать, используют ли его еще злоумышленные стороны, и обеспечить примерный сигнал 115 безопасности, имитирующий действия эксплойта «нулевого дня», для использования в качестве сигнала 135 предыстории, чтобы упреждающе защищать от эксплойта, даже если его никогда не замечали. В еще дополнительном примере, сигнал 115 безопасности, который часто приводит к ложным положительным результатам, может добавляться к сигналам 135 предыстории, чтобы гарантировать, что предсказательные модели обучаются по отношению к этому конкретному сигналу 115 безопасности. Сигналы 135 предыстории, если имеются, добавляются к набору сигналов 115 безопасности, собранных внутри скользящего окна 130.

[0038] Переходя к ОПЕРАЦИИ 250, способ 200 обеспечивает баланс собранных вредоносных и безвредных сигналов, которые попадают в скользящее окно 130, и каких-либо сигналов 135 предыстории, добавленных к набору в необязательной ОПЕРАЦИИ 240. При обеспечении баланса вредоносных сигналов, тип атаки каждого сигнала определяют так, что относительные количества сигналов, представляющих каждый тип атаки, приводятся в равновесие (то есть, выравниваются) с тем, чтобы никакой данный тип атаки не был чрезмерно представлен или недостаточно представлен в совокупности вредоносных сигналов. При обеспечении баланса безвредных сигналов, безвредные сигналы, принятые от устройств, которые сгенерировали вредоносные сигналы в скользящем окне 130, отбрасываются, и относительные количества безвредных сигналов, принятых от каждого типа устройства в онлайновой услуге 110, приводятся в равновесие, так что никакой данный тип устройства не является чрезмерно представленным или недостаточно представленным в совокупности безвредных сигналов.

[0039] Кроме того, поскольку ожидается, что набор вредоносных сигналов будет меньшим по количеству, чем набор безвредных сигналов, порция набора безвредных сигналов может быть отобрана в ОПЕРАЦИИ 260 для перекрестного соединения с вредоносными сигналами, чтобы создать новый, больший набор вредоносных сигналов, так что два набора будут содержать требуемое соотношение вредных к безвредным

сигналам. В различных аспектах, как только набор вредоносных сигналов и набор безвредных сигналов приведены в требуемое соотношение (например, равновесие), два набора используются вместе в качестве обучающего набора.

[0040] В ОПЕРАЦИИ 270 обучающий набор различных сценариев атаки, составленный из сбалансированных вредоносных и безвредных сигналов, имеющих место в скользящем окне 130 (и какие-либо сигналы 135 предыстории), делают доступным для обучения предсказательных моделей. Например, рабочие модели 120, используемые, чтобы анализировать сигналы 115 безопасности, постоянно повторно обучаются и/или заменяются другими предсказательными моделями по мере обновления во времени содержания скользящего окна 130, чтобы лучше оценивать атаки и эсплойты, активно используемые против онлайновой услуги 110. Способ 200, следовательно, может завершаться после ОПЕРАЦИИ 270 или возвращаться к ОПЕРАЦИИ 210 для продолжения сбора сигналов 115 безопасности, чтобы периодически или постоянно восполнять обучающий набор данных на основе скользящего окна 130.

[0041] Фигура Фиг.3 являет собой структурную схему, показывающую общие этапы, включенные в примерный способ 300 для обучения и выбора предсказательных моделей для использования в обеспечении безопасности онлайновой услуги 110. Способ 300 начинается с ОПЕРАЦИИ 310, где принимается обучающий набор данных сбалансированных вредоносных и безвредных сигналов, такой как разработанный по способу 200. В различных аспектах, способ 300 вызывается на периодической основе (например, каждые *h* часов), в ответ на обновление скользящего окна 130 (и, следовательно, обучающего набора данных) или команду пользователя.

[0042] Переходя к ОПЕРАЦИИ 320, обучающий набор данных разделяется на подмножество для оценивания и подмножество для обучения. В различных аспектах размер подмножества оценивания относительно обучающего набора данных может изменяться, но обычно меньше по размеру, чем подмножество обучения. Например, подмножество оценивания может быть одной третью первоначального обучающего набора, и подмножество обучения, следовательно, будет оставшимися двумя третями первоначального обучающего набора. Средний специалист в данной области техники оценит, что другие доли обучающего набора данных могут отщепляться для использования в качестве подмножества оценивания.

[0043] В ОПЕРАЦИИ 330 принимают признаки конфигурации, чтобы создавать модели 180 стадии разработки в качестве потенциальных предсказательных моделей для использования в производственной деятельности (то есть, в качестве рабочих моделей 120), чтобы обеспечивать безопасность онлайновой услуги 110. Административный пользователь, такой как аналитик по безопасности, отбирает один или более параметров, внесенных в список для онлайновой услуги 110, при посредстве сигналов 115 безопасности и типа признака, по которым исследовать эти признаки. Сигналы 115 безопасности включают в себя, но без ограничения: журналы регистрации событий, трассы состояний сети, отчеты об ошибках, отчеты приемника специальных событий, атомарное обнаружение и комбинации этого, и параметры для выбранных функций могут включать в себя любой из элементов, включенных в сигналы 115 безопасности.

[0044] Например, когда сигналы 115 безопасности включают в себя трассы состояний сети, параметр пары адресов отправитель/приемник может выбираться и оцениваться согласно типу признака "общее количество" (count), так что число раз, которое пара встречается в обучающем наборе, увеличивает счет/значение, чтобы оценивать этот признак. В другом примере, когда сигналы 115 безопасности включают в себя трассы

состояний сети, параметр числа байтов, переданных между парой отправитель/приемник, обеспечивается в виде значения/количества, чтобы оценивать этот признак. В дополнительном примере параметр баланса передач между парой отправитель/приемник, чтобы указывать относительное отношение загрузка/выгрузка, обеспечивается как значение/счет, чтобы оценивать этот признак. Средний специалист в данной области техники признает вышеуказанное неограничительными примерами; другие параметры и другие типы признаков этих параметров, по которым они могут оцениваться посредством предсказательных моделей, предусматриваются для использования с настоящей заявкой.

[0045] Переходя к ОПЕРАЦИИ 340, модели 180 стадии разработки создаются на основе принятой конфигурации признаков и уточняются в соответствии с подмножеством обучения с помощью одного или более алгоритмов машинного обучения. Каждая предсказательная модель создается, чтобы воспринимать конкретный вектор признаков (указывающий признаки, отобранные административным пользователем), где каждый признак, составляющий вектор признаков, ассоциируется с коэффициентом. Каждый вектор признаков динамически выделяется из сигналов 115 безопасности на основе конфигурации признаков. Значения коэффициентов корректируются по нескольким циклам алгоритма машинного обучения, так что когда данная модель 180 стадии разработки принимает ввод вектора признаков, взаимодействия между различными значениями признаков могут быть скорректированы, чтобы надежно генерировать выход «вредоносный или безвредный» для соответствия выходам, обозначенным в подмножестве обучения.

[0046] Переходя к ОПЕРАЦИИ 350, предсказательные модели, уточненные в отношении обучающего набора данных в ОПЕРАЦИИ 340, оцениваются по отношению к подмножеству оценивания, отщепленному из обучающего набора данных в ОПЕРАЦИИ 320. Подмножество оценивания включает в себя входы (сигналы 115 безопасности, накопленные от онлайновой услуги 110) с известными выходами, является ли сигнал вредоносным или безвредным. Кроме того, пары вход/выход из подмножества оценивания не использовались, чтобы напрямую обучать на них модели 180 стадии разработки, и таким образом обеспечивают проверку, обеспечивают ли модели 180 стадии разработки общее функциональное правило для определения, является ли неизвестный сигнал вредоносным или безвредным.

[0047] Пороговое значение перевода применяется к моделям 180 стадии разработки для определения, переводить ли данную модель 180 стадии разработки в рабочую модель 120. Пороговые значения перевода предписывают, насколько точной модели 180 стадии разработки требуется быть в предсказании, являются ли сигналы вредоносными или безвредными, на основе вектора признаков, выделенного из сигналов 115 безопасности. В некоторых аспектах, пороговое значение перевода задается в виде константы, такой как, например, по меньшей мере, доля правильных результатов в $n\%$, заданная площадь под кривой точности и полноты на тестовых данных, и т.д. В других аспектах пороговое значение перевода задается долей правильных результатов текущей рабочей модели 120 для данного вектора признаков или типа атаки, так что для того, чтобы модели 180 стадии разработки заменить рабочую модель 120 в системе 100 обеспечения безопасности, модель 180 стадии разработки должна быть более точной, чем текущая рабочая модель 120.

[0048] В ОПЕРАЦИИ 360 модели 180 стадии разработки и повторно оцененные рабочие модели 120, которые действуют лучшим образом согласно подмножеству оценивания и пороговому значению перевода, переводят для использования системой

100 обеспечения безопасности, чтобы защищать онлайновую услугу 110. Рабочие модели 120, которые более не удовлетворяют пороговому значению перевода или были замещены моделями 180 стадии разработки, могут быть удалены или переведены в модели 180 стадии разработки для дополнительного обучения и коррекции, и для последующего повторного оценивания. Способ 300 может затем завершиться.

[0049] Хотя реализации были описаны в общем контексте программных модулей, которые исполняются в сочетании с прикладной программой, которая работает в операционной системе на компьютере, специалисты в данной области техники признают, что аспекты также могут реализовываться в комбинации с другими программными модулями. Обычно, программные модули включают в себя подпрограммы, программы, компоненты, структуры данных и другие виды структур, которые выполняют особые задачи или реализуют особые абстрактные типы данных.

[0050] Аспекты и функциональные возможности, описанные здесь, могут работать при посредстве множества вычислительных систем, включая, без ограничения, системы с настольным компьютером, проводные и беспроводные вычислительные системы, мобильные вычислительные системы (например, мобильные телефоны, нетбуки, компьютеры планшетного или сверхтонкого типа, блокнотные компьютеры и портативные компьютеры), ручные устройства, мультипроцессорные системы, микропроцессорную или программируемую бытовую электронику, миникомпьютеры и большие ЭВМ.

[0051] Кроме того, согласно аспекту, аспекты и функциональные возможности, описанные здесь, работают на распределенных системах (например, облачных вычислительных системах), где функциональностью приложения, памятью, хранением и поиском данных и различными функциями обработки управляют удаленно друг от друга по распределенной вычислительной сети, такой как сеть Интернет или внутрикорпоративная сеть. Согласно аспекту, пользовательские интерфейсы и информация различных типов отображаются посредством встроенных устройств отображения вычислительного устройства или посредством удаленных устройств отображения, связанных с одним или более вычислительными устройствами. Например, пользовательские интерфейсы и информацию различных типов отображают и с ними взаимодействуют на поверхности стены, на которую проецируются пользовательские интерфейсы и информация различных типов. Взаимодействие с множеством вычислительных систем, с помощью которых реализации осуществляются на практике, включает в себя ввод нажатия клавиши, ввод с сенсорного экрана, речевой или другой аудио ввод, жестовый ввод, где связанное вычислительное устройство оснащено функциональностью обнаружения (например, камерой) для ввода с оцифровкой и интерпретации жестов пользователя, чтобы управлять функциональностью вычислительного устройства, и подобное.

[0052] Фигура Фиг.4 и связанное с ней описание обеспечивают рассмотрение множества операционных сред, в которых примеры осуществляются практически. Однако, устройства и системы, иллюстрируемые и рассматриваемые относительно Фиг.4, приведены с целью примера и иллюстрации, и не являются ограничительными для большого количества конфигураций вычислительных устройств, которые используются для осуществления на практике аспектов, описанных здесь.

[0053] Фигура Фиг.4 является блок-схемой, иллюстрирующей физические компоненты (то есть, аппаратные средства) вычислительного устройства 400, с помощью которого могут быть осуществлены на практике примеры настоящего раскрытия. В базовой конфигурации вычислительное устройство 400 включает в себя, по меньшей мере, один

блок 402 обработки и системную память 404. Согласно аспекту, в зависимости от конфигурации и типа вычислительного устройства 400, системная память 404 является устройством памяти, которое содержит, но без ограничения указанным, энергозависимую память (например, оперативную память), энергонезависимую память (например, постоянную память), флэш-память или какую-либо комбинацию таких памятей. Согласно аспекту, системная память 404 включает в себя операционную систему 405 и один или более программных модулей 406, подходящих для исполнения программно-реализованного приложения 450. Согласно аспекту, системная память 404 включает в себя систему 100 обеспечения безопасности, систему 105 обучения и выбора модели, и любые модели, используемые или создаваемые посредством этого. Операционная система 405, например, является подходящей для управления работой вычислительного устройства 400. Кроме того, аспекты осуществляются на практике в сочетании с графической библиотекой, другими операционными системами, или любой другой прикладной программой, и не ограничиваются каким-либо конкретным приложением или системой. Эта базовая конфигурация иллюстрируется на Фиг. 4 этими компонентами внутри пунктирной линии 408. Согласно аспекту, вычислительное устройство 400 имеет добавочные технические характеристики или функциональность. Например, согласно аспекту, вычислительное устройство 400 включает в себя добавочные устройства хранения данных (съемные и/или несъемные) такие как, например, на магнитных дисках, оптических дисках или магнитной ленте. Такое добавочное запоминающее устройство проиллюстрировано на Фиг. 4 съемным запоминающим устройством 409 и несъемным запоминающим устройством 410.

[0054] Как изложено выше, согласно аспекту, ряд программных модулей и файлов данных сохраняются в системной памяти 404. При исполнении в блоке 402 обработки, программные модули 406 (например, система 100 обеспечения безопасности, система 105 обучения и выбора модели) выполняют процессы, включающие в себя, но без ограничения, один или более этапов из способов 200 и 300, проиллюстрированных на фигурах Фиг. 2 и 3, соответственно. Согласно аспекту, другие программные модули используются в соответствии с примерами и включают в себя приложения, такие как приложения электронной почты и контактов, приложения обработки текстов, приложения обработки электронных таблиц, приложения баз данных, приложения презентации слайдов, прикладные программы графические или автоматизированного проектирования, и т.д.

[0055] Согласно аспекту, вычислительное устройство 400 имеет одно или несколько устройств 412 ввода, таких как клавиатура, мышь, перо, устройство звукового ввода, устройство сенсорного ввода, и т.д. Устройство(а) 414 вывода, такое как устройство отображения, динамики, принтер, и т.д. также включаются в состав согласно аспекту. Вышеупомянутые устройства являются примерами, и могут использоваться другие. Согласно аспекту, вычислительное устройство 400 включает в себя одно или более соединений 416 связи, позволяющих обмен информацией с другими вычислительными устройствами 418. Примеры подходящих соединений 416 связи включают в себя, но без ограничения, схему радиочастотного (RF) передатчика, приемника и/или приемопередатчика; универсальную последовательную шину (USB), параллельный и/или последовательный порты.

[0056] Термин «читаемые компьютером носители данных», как используется здесь, включает в себя компьютерные носители данных. Компьютерные носители данных включают в себя энергозависимые и энергонезависимые, съемные и несъемные носители, реализованные любым способом или технологией для хранения информации, такой

как читаемые компьютером команды, структуры данных или программные модули. Системная память 404, съемное запоминающее устройство 409 и несъемное запоминающее устройство 410 - все являются примерами носителей данных компьютера (то есть, запоминающего устройства). Согласно аспекту, носители данных компьютера включают в себя оперативную память (RAM), постоянную память (ROM), электрически стираемую программируемую постоянную память (EEPROM), флэш-память или память по другой технологии, ПЗУ на компакт-диске (CD-ROM), цифровые многофункциональные диски (DVD) или другие оптические ЗУ, магнитные кассеты, магнитную ленту, накопитель на магнитных дисках или другие ЗУ на магнитном носителе, или любое другое изделие, которое может использоваться для хранения информации, и к которому может осуществлять доступ вычислительное устройство 400. Согласно аспекту, любые такие носители данных компьютера являются частью вычислительного устройства 400. Носители данных компьютера не включают в себя несущую или другой распространяемый сигнал данных.

[0057] Согласно аспекту, носители передачи данных осуществляются читаемыми компьютером командами, структурами данных, программными модулями или другими данными в модулированном сигнале данных, таком как несущая или другой механизм переноса, и включают в себя любые носители доставки информации. Согласно аспекту, термин "модулированный сигнал данных" описывает сигнал, у которого имеется одна или более характеристик, задаваемых или измененяемых таким образом, чтобы закодировать информацию в сигнале. В качестве примера, а не ограничения, носители передачи данных включают в себя проводные носители, такие как проводная сеть или прямое проводное соединение, и беспроводные носители, такие как акустические, радиочастотные (RF), инфракрасного излучения и другие беспроводные носители.

[0058] Реализации, например, описываются выше со ссылкой на блок-схемы и/или операционные иллюстрации способов, систем и компьютерных программных продуктов согласно аспектам. Функции/действия, отмеченные в блоках, могут происходить не в порядке следования, как показано на какой-либо структурной схеме. Например, два блока, показанные последовательно, фактически могут исполняться по существу параллельно, или блоки иногда могут исполняться в обратном порядке в зависимости от подразумеваемой функциональности/действий.

[0059] Описание и иллюстрация одного или более примеров, приведенных в этой заявке, не предназначены для установления границ или ограничения каким-либо образом объема, как заявлено в формуле изобретения. Аспекты, примеры и подробности, приведенные в этой заявке, считаются достаточными, чтобы передавать права на владение и давать возможность другим выполнять и использовать лучший вариант осуществления изобретения. Реализации не следует толковать как ограничиваемые каким-либо аспектом, примером или подробностью, приведенной в этой заявке. Независимо от того, показаны ли или описаны в комбинации или отдельно, подразумевается, что различные признаки (и структурные, и методологические) будут выборочно включаться или опускаться, чтобы получить пример с конкретным набором признаков. При предоставлении описания и иллюстрации настоящей заявки, специалист в данной области техники сможет представить себе изменения, модификации и альтернативные примеры, входящие в рамки существа более широких аспектов общей идеи изобретения, осуществленной в этой заявке, которые не выходят за рамки более широкого объема.

(57) Формула изобретения

1. Способ обеспечения безопасности онлайновой услуги, предоставляемой через сеть, посредством модели с постоянным обучением, содержащий:

сбор набора сигналов безопасности, связанных с одним или более сетевыми сеансами, от онлайновой услуги, причем набор сигналов безопасности собирают в скользящем окне времени;

идентификацию того, является ли каждый сигнал безопасности из набора сигналов безопасности вредоносным или безвредным;

создание сбалансированного обучающего набора данных для скользящего окна времени посредством:

обеспечения баланса вредоносных сигналов из набора сигналов безопасности на основе типа атаки, идентифицированного для каждого вредоносного сигнала,

обеспечения баланса безвредных сигналов из набора сигналов безопасности, чтобы создать сбалансированный обучающий набор данных на основе типа устройства, от которого принят каждый безвредный сигнал, и

обеспечения баланса вредоносных сигналов с безвредными сигналами посредством перекрестного соединения вредоносных сигналов с безвредными сигналами; и

создание предсказательной модели на основе сбалансированного обучающего набора данных, причем, в ответ на прием дополнительного сигнала безопасности, связанного с новым сетевым сеансом, от онлайновой услуги, предсказательная модель применяется для определения того, является ли этот дополнительный сигнал безопасности вредоносным или безвредным.

2. Способ по п.1, в котором идентификация того, является ли каждый сигнал безопасности из набора сигналов безопасности вредоносным или безвредным, дополнительно содержит:

исследование каждого сигнала безопасности в рабочей модели, причем рабочая модель создается посредством блока обучения модели в соответствии со сбалансированным обучающим набором данных и сконфигурирована, чтобы давать результат обнаружения того, является ли конкретный сигнал безопасности вредоносным или безвредным;

передачу результата обнаружения пользователю-аналитику; и

в ответ на прием действия от пользователя-аналитика в отношении результата обнаружения, обновление результата обнаружения, чтобы указать, является ли упомянутый конкретный сигнал безопасности вредоносным или безвредным.

3. Способ по п.2, в котором автоматизированный источник атаки имитирует атаку на онлайновую услугу, при этом идентификация того, является ли каждый сигнал безопасности из набора сигналов безопасности вредоносным или безвредным, дополнительно содержит:

прием от автоматизированного источника атаки уведомления, идентифицирующего сигналы безопасности, сгенерированные в ответ на атаку; и

интерпретацию сигналов безопасности, сгенерированных в ответ на атаку, как вредоносных независимо от результата обнаружения.

4. Способ по п.2, в котором идентификация того, является ли каждый сигнал безопасности из набора сигналов безопасности вредоносным или безвредным, дополнительно содержит:

выделение признаков из упомянутого конкретного сигнала безопасности;

определение того, удовлетворяют ли эти признаки, выделенные из конкретного сигнала безопасности, набору признаков, обозначенному административным пользователем как определяющий тип атаки;

в ответ на определение того, что выделенные признаки удовлетворяют набору признаков, обозначение упомянутого конкретного сигнала безопасности как вредоносного; и

в ответ на определение того, что выделенные признаки не удовлетворяют набору признаков, обозначение упомянутого конкретного сигнала безопасности как безвредного.

5. Способ по п.4, в котором обеспечение баланса вредоносных сигналов из набора сигналов безопасности на основе типа атаки, идентифицированного для каждого вредоносного сигнала, дополнительно содержит обеспечение баланса относительного числа типов атаки для набора типов атак, наблюдаемых для вредоносных сигналов, посредством по меньшей мере одного из:

увеличения относительного количества недостаточно представленных типов атаки в наборе типов атак и

уменьшения относительного количества чрезмерно представленных типов атак в наборе типов атак.

6. Способ по п.4, в котором набор признаков идентифицируется в структурированном документе, подаваемом административным пользователем, причем структурированный документ предписывает типы признаков и поля данных для наблюдения в сигналах безопасности, и признаки из набора признаков динамически выделяются из набора сигналов безопасности на основе структурированного документа без необходимости модифицировать код.

7. Способ по п.1, в котором сигналы данных предыстории включаются в набор сигналов безопасности.

8. Способ по п.1, в котором обеспечение баланса вредоносных сигналов безвредных сигналов из набора сигналов безопасности, чтобы создать сбалансированный обучающий набор данных на основе типа устройства, от которого принят каждый безвредный сигнал, дополнительно содержит:

идентификацию устройства в онлайновой услуге, от которого был собран по меньшей мере один вредоносный сигнал в пределах скользящего окна; и

удаление безвредных сигналов, связанных с этим устройством, из набора сигналов безопасности.

9. Способ по п.8, в котором обеспечение баланса вредоносных сигналов с безвредными сигналами посредством перекрестного соединения вредоносных сигналов с безвредными сигналами дополнительно содержит перекрестное соединение вредоносных сигналов с безвредными сигналами, чтобы создать множество сценариев атак для сбалансированного обучающего набора данных, каковое множество сценариев атак включают в себя вредоносные сигналы и безвредные сигналы.

10. Способ по п.1, в котором сбор набора сигналов безопасности в скользящем окне времени дополнительно содержит:

идентификацию временного интервала, в котором должно быть определено скользящее окно времени, от текущего момента времени;

прием, в текущий момент времени, новых сигналов безопасности от онлайновой услуги;

добавление новых сигналов безопасности, принятых в текущий момент времени, в набор сигналов безопасности;

идентификацию имеющихся сигналов безопасности, которые были добавлены в набор сигналов безопасности вне упомянутого временного интервала от текущего момента времени; и

удаление из набора сигналов безопасности имеющихся сигналов безопасности, которые были идентифицированы как добавленные в набор сигналов безопасности вне упомянутого временного интервала от текущего момента времени.

11. Система для обеспечения безопасности онлайновой услуги, предоставляемой через сеть, посредством модели с постоянным обучением, содержащая:

процессор; и

запоминающее устройство, включающее в себя команды, которые при их исполнении процессором приспособлены, чтобы:

принимать сигналы безопасности от устройств в рамках онлайновой услуги, причем сигналы безопасности связаны с одним или более сетевыми сеансами;

выделять векторы признаков из каждого из сигналов безопасности, причем конкретный вектор признаков обеспечивает числовые значения, представляющие состояние конкретного устройства, от которого принимается конкретный сигнал безопасности;

получать результаты обнаружения для каждого из векторов признаков посредством соответствующих предсказательных моделей, причем конкретный результат обнаружения идентифицирует, является ли упомянутый конкретный сигнал безопасности, который связан с конкретным сетевым сеансом, указывающим вредоносную или безвредную активность на упомянутом конкретном устройстве;

задавать скользящее окно, причем скользящее окно включает в себя множество сигналов безопасности и соответствующие результаты обнаружения, которые были приняты во временном интервале от текущего момента времени;

создавать сбалансированный обучающий набор данных для скользящего окна, причем для создания сбалансированного обучающего набора данных система дополнительно выполнена с возможностью:

идентифицировать тип атаки для каждого сигнала из сигналов безопасности в скользящем окне, идентифицированного указывающим вредоносную активность;

увеличивать количество сигналов безопасности, идентифицированных с недостаточно представленными типами атаки, в скользящем окне относительно сигналов безопасности, идентифицированных с чрезмерно представленными типами атаки; и

выполнять перекрестное соединение сигналов безопасности, идентифицированных указывающими вредоносную активность, с сигналами безопасности, идентифицированными указывающими безвредную активность, чтобы создать сценарии атаки для скользящего окна; и

обновлять, согласно алгоритму машинного обучения, упомянутые соответствующие предсказательные модели на основе сбалансированного обучающего набора данных.

12. Система по п.11, в которой обновление соответствующих предсказательных моделей включает в себя замену рабочих моделей, используемых для получения результатов обнаружения, моделями стадии разработки, разработанными на основе сбалансированного обучающего набора данных согласно алгоритму машинного обучения, в ответ на указание алгоритмом машинного обучения того, что модели стадии разработки более точно идентифицируют то, являются ли сигналы безопасности указывающими вредоносную или безвредную активность на устройствах, согласно сбалансированному обучающему набору данных.

13. Система по п.11, в которой сигналы предыстории включаются в скользящее окно, причем сигналы предыстории включают в себя сигналы безопасности, собранные вне временного интервала.

14. Система по п.11, в которой сигналы безопасности, принятые от устройств в

рамках онлайновой услуги, включают в себя сигналы безопасности, сгенерированные в ответ на выполнение автоматизированным источником атаки известных вредоносных активностей в онлайновой услуге, при этом результаты обнаружения, создаваемые для сигналов безопасности, сгенерированных в ответ на выполнение автоматизированным источником атаки известных вредоносных активностей, устанавливаются, чтобы указывать, что упомянутый конкретный сигнал безопасности является указывающим вредоносную активность, на основе уведомления от автоматизированного источника атаки.

15. Система по п.11, при этом для создания сбалансированного обучающего набора данных система дополнительно выполнена с возможностью удалять сигналы безопасности, идентифицированные указывающими безвредную активность, из скользящего окна в ответ на идентификацию того, что конкретное устройство, от которого были приняты сигналы безопасности, идентифицированные указывающими безвредную активность, связано с одним или более сигналами безопасности, идентифицированными указывающими вредоносную активность, в скользящем окне.

16. Система по п.11, при этом для создания сбалансированного обучающего набора данных система дополнительно выполнена с возможностью:

идентифицировать тип устройства, от которого был принят каждый сигнал из сигналов безопасности в скользящем окне, идентифицированный указывающим безвредную активность; и

увеличивать количество сигналов безопасности, идентифицированных с недостаточно представленными типами устройств в скользящем окне относительно сигналов безопасности, идентифицированных с чрезмерно представленными типами устройств.

17. Машиночитаемое запоминающее устройство, включающее в себя исполняемые процессором команды для обеспечения безопасности онлайновой услуги, предоставляемой через сеть, посредством модели с постоянным обучением, содержащие:

сбор набора сигналов безопасности от онлайновой услуги, причем набор сигналов безопасности собирается в скользящем окне времени;

исследование каждого сигнала безопасности из набора сигналов безопасности посредством предсказательных моделей, чтобы идентифицировать, является ли каждый сигнал безопасности, связанный с конкретным сетевым сеансом, вредоносным или безвредным, причем предсказательные модели сконфигурированы, чтобы давать результаты обнаружения того, является ли конкретный сигнал безопасности вредоносным или безвредным, на основе вектора признаков, определяемого административным пользователем;

связывание набора сигналов безопасности с результатами обнаружения, чтобы идентифицировать набор сигналов безопасности как вредоносные сигналы или безвредные сигналы;

обеспечение баланса вредоносных сигналов с безвредными сигналами, чтобы создать сбалансированный обучающий набор данных, включающее в себя:

идентификацию типа атаки для каждого из вредоносных сигналов,

идентификацию типа устройства, от которого был собран каждый из безвредных сигналов,

выравнивание относительных чисел вредоносных сигналов в скользящем окне на основе идентифицированных типов атак, чтобы создать набор примеров атак,

выравнивание относительных чисел безвредных сигналов в скользящем окне на основе идентифицированных типов устройств, чтобы создать набор идентифицированных безвредных примеров, и

перекрестное соединение набора примеров атаки с, по меньшей мере, частью набора безвредных примеров, чтобы обеспечить баланс числа примеров атаки в наборе примеров атаки относительно числа безвредных примеров в наборе безвредных примеров; и

уточнение предсказательных моделей на основе сбалансированного обучающего набора данных и алгоритма машинного обучения.

18. Машиночитаемое запоминающее устройство по п.17, при этом обеспечение баланса вредоносных сигналов с безвредными сигналами дополнительно содержит:

идентификацию устройства в онлайновой услуге, с которого был собран по меньшей мере один вредоносный сигнал в пределах скользящего окна; и

удаление безвредных сигналов, связанных с этим устройством, из набора сигналов безопасности.

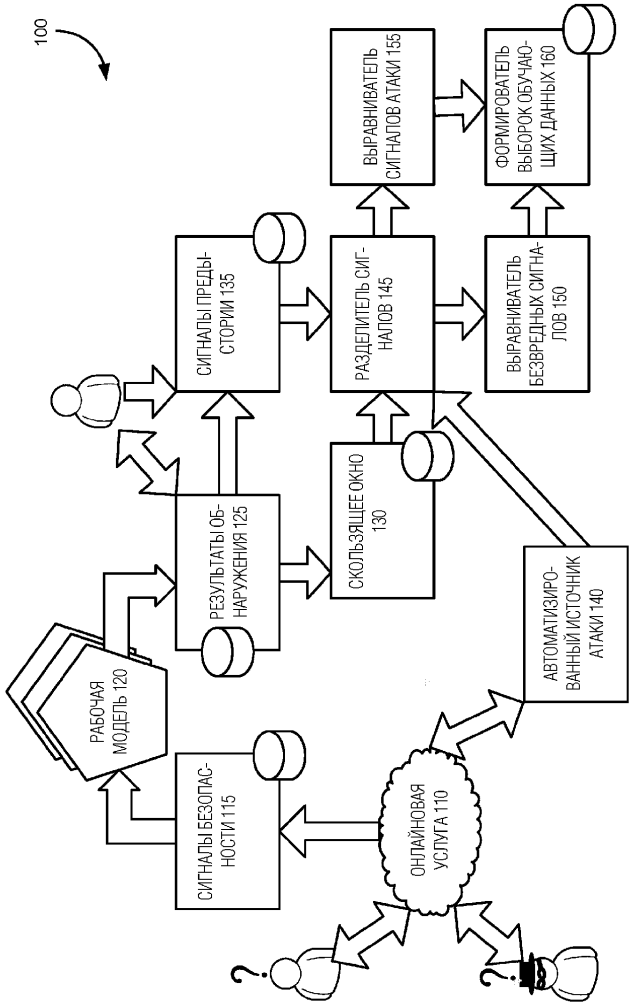
19. Машиночитаемое запоминающее устройство по п.17, при этом исследование каждого сигнала безопасности посредством предсказательных моделей дополнительно содержит:

передачу результатов обнаружения пользователю-аналитику; и

в ответ на прием от пользователя-аналитика действия в отношении результатов обнаружения, обновление результатов обнаружения, чтобы указать, является ли конкретный сигнал безопасности вредоносным или безвредным, в свете упомянутого действия от пользователя-аналитика.

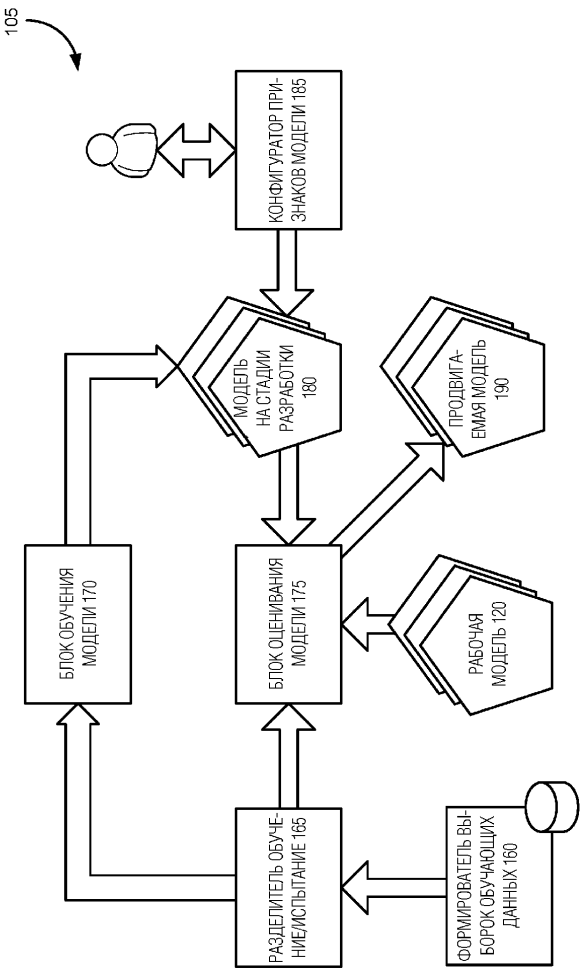
20. Машиночитаемое запоминающее устройство по п.17, при этом вектор признаков включает в себя набор признаков состояния устройства, которые идентифицированы в структурированном документе, подаваемом административным пользователем, для определения предсказательной модели, сконфигурированной для идентификации одного или более типов атак, причем структурированный документ задает типы признаков и поля данных для наблюдения в наборе сигналов безопасности, и признаки из этого набора признаков динамически выделяются из набора сигналов безопасности на основе структурированного документа без необходимости модифицировать код.

1


100
ВЫРАВНИВАТЕЛЬ СИГНАЛОВ АТАКИ 155
ФОРМИРОВАТЕЛЬ ВЫБОРОК (ОБУЧАЮЩИХ ДАННЫХ 160
СИГНАЛЫ ПРЕДЫСТОРИИ 135
РАЗДЕЛИТЕЛЬ СИГНАЛОВ 145
ВЫРАВНИВАТЕЛЬ БЕЗВРЕДНЫХ СИГНАЛОВ 150
СКОЛЬЗЯЩЕЕ ОКНО 130
РЕЗУЛЬТАТЫ ОБНАРУЖЕНИЯ 125
АВТОМАТИЗИРОВАННЫЙ ИСТОЧНИК АТАКИ 140
РАБОЧАЯ МОДЕЛЬ 120
СИГНАЛЫ БЕЗОПАСНОСТИ 115
ОНЛАЙНОВАЯ УСЛУГА 110

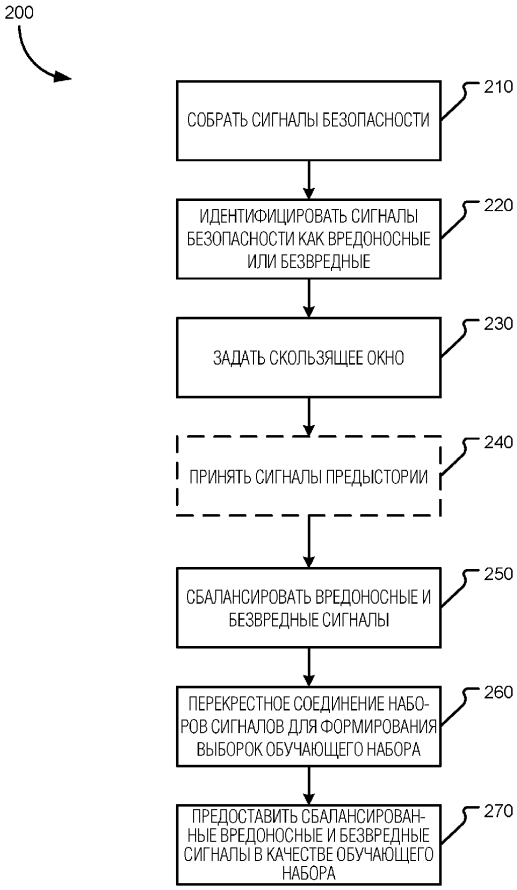
ФИГ. 1А

2


105
КОНФИГУРАТОР ПРИЗНАКОВ МОДЕЛИ 185
МОДЕЛЬ НА СТАДИИ РАЗРАБОТКИ 180
ПРОДВИГАЕМАЯ МОДЕЛЬ 190
БЛОК ОБУЧЕНИЯ МОДЕЛИ 170
БЛОК ОЦЕНИВАНИЯ МОДЕЛИ 175
РАБОЧАЯ МОДЕЛЬ 120
РАЗДЕЛИТЕЛЬ ОБУЧЕНИЕ/ИСПЫТАНИЕ 165
ФОРМИРОВАТЕЛЬ ВЫБОРОК ОБУЧАЮЩИХ ДАННЫХ 160

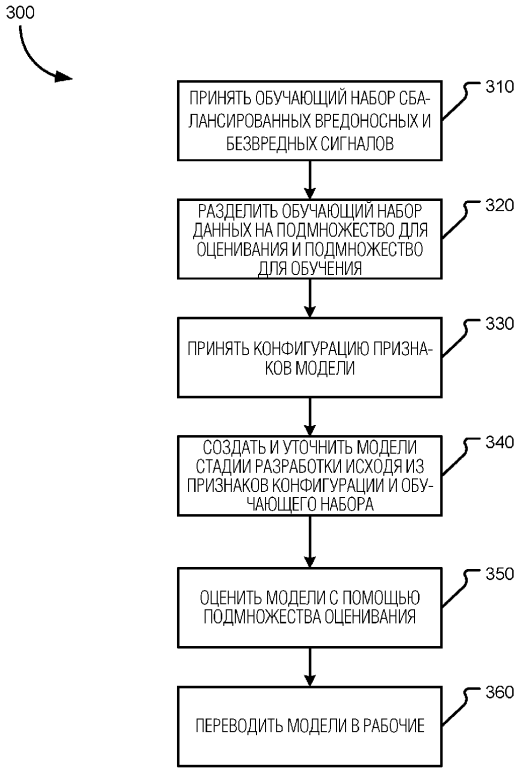
ФИГ. 1В

3


200
СОБРАТЬ СИГНАЛЫ БЕЗОПАСНОСТИ
210
ИДЕНТИФИЦИРОВАТЬ СИГНАЛЫ БЕЗОПАСНОСТИ КАК ВРЕДОНОСНЫЕ ИЛИ БЕЗВРЕДНЫЕ
220
ЗАДАТЬ СКОЛЬЗЯЩЕЕ ОКНО
230
ПРИНЯТЬ СИГНАЛЫ ПРЕДЫСТОРИИ
240
СБАЛАНСИРОВАТЬ ВРЕДОНОСНЫЕ И БЕЗВРЕДНЫЕ СИГНАЛЫ
250
ПЕРЕКРЕСТНОЕ СОЕДИНЕНИЕ НАБОРОВ СИГНАЛОВ ДЛЯ ФОРМИРОВАНИЯ ВЫБОРОК ОБУЧАЮЩЕГО НАБОРА
260
ПРЕДОСТАВИТЬ СБАЛАНСИРОВАННЫЕ ВРЕДОНОСНЫЕ И БЕЗВРЕДНЫЕ СИГНАЛЫ В КАЧЕСТВЕ ОБУЧАЮЩЕГО НАБОРА
270

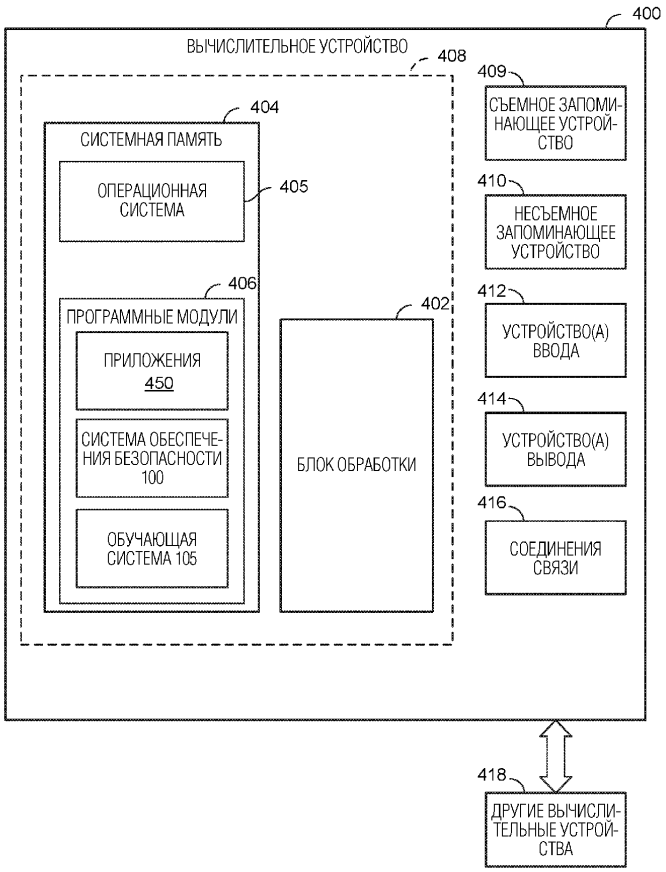
ФИГ. 2

4


300
ПРИНЯТЬ ОБУЧАЮЩИЙ НАБОР СБАЛАНСИРОВАННЫХ ВРЕДОНОСНЫХ И БЕЗВРЕДНЫХ СИГНАЛОВ
310
РАЗДЕЛИТЬ ОБУЧАЮЩИЙ НАБОР ДАННЫХ НА ПОДМНОЖЕСТВО ДЛЯ ОЦЕНИВАНИЯ И ПОДМНОЖЕСТВО ДЛЯ ОБУЧЕНИЯ
320
ПРИНЯТЬ КОНФИГУРАЦИЮ ПРИЗНАКОВ МОДЕЛИ
330
СОЗДАТЬ И УТОЧНИТЬ МОДЕЛИ СТАДИИ РАЗРАБОТКИ ИСХОДЯ ИЗ ПРИЗНАКОВ КОНФИГУРАЦИИ И ОБУЧАЮЩЕГО НАБОРА
340
ОЦЕНИТЬ МОДЕЛИ С ПОМОЩЬЮ ПОДМНОЖЕСТВА ОЦЕНИВАНИЯ
350
ПЕРЕВОДИТЬ МОДЕЛИ В РАБОЧИЕ
360

ФИГ. 3

5


400
ВЫЧИСЛИТЕЛЬНОЕ УСТРОЙСТВО
408
409
СЪЕМНОЕ ЗАПОМИНАЮЩЕЕ УСТРОЙСТВО
404
СИСТЕМНАЯ ПАМЯТЬ
ОПЕРАЦИОННАЯ СИСТЕМА
405
410
НЕСЪЕМНОЕ ЗАПОМИНАЮЩЕЕ УСТРОЙСТВО
406
ПРОГРАММНЫЕ МОДУЛИ
402
412
УСТРОЙСТВО(А) ВВОДА
ПРИЛОЖЕНИЯ 450
СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ 100
БЛОК ОБРАБОТКИ
414
УСТРОЙСТВО(А) ВЫВОДА
ОБУЧАЮЩАЯ СИСТЕМА 105
416
СОЕДИНЕНИЯ СВЯЗИ
418
ДРУГИЕ ВЫЧИСЛИТЕЛЬНЫЕ УСТРОЙСТВА

ФИГ. 4