(19) Евразийское патентное ведомство

(11) 038063 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2021.06.30

(21) Номер заявки
201991278

(22) Дата подачи заявки
2019.06.24

(51) Int. Cl. ***G06F 21/50*** (2006.01)
G06F 16/22 (2006.01)
G06F 7/24 (2006.01)

(54) СИСТЕМА ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ КИБЕРУГРОЗАМИ

(31) **2019117226**
(32) **2019.06.04**
(33) **RU**
(43) **2020.12.30**

(71)(73) Заявитель и патентовладелец:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(72) Изобретатель:
Рюпичев Дмитрий Юрьевич, Новиков Евгений Александрович, Ничипорчук Максим Михайлович (RU)

(74) Представитель:
Герасин Б.В. (RU)

(56) US-A1-20110039237
US-A1-20170230391
EP-A1-2882159
US-B2-9118702
KR-B1-101039717
RU-C1-2675900

(57) Настоящее изобретение относится к области информационной защиты, в частности к системам интеллектуального управления киберугрозами. Основным техническим результатом является повышение информационной безопасности за счет осуществления автоматизированной обработки данных о поступающих киберугрозах, обеспечивающей постоянную актуализацию данных о типах киберугроз и индикаторов компрометации, соответствующих им. Заявленная система интеллектуального управления киберугрозами содержит по меньшей мере один процессор, обеспечивающий обработку информационных потоков между модулями системы; по меньшей мере одно средство хранения данных, содержащее машиночитаемые инструкции, исполняемые процессором; модуль получения данных, обеспечивающий сбор информации из внешних и внутренних источников данных, содержащих информацию о киберугрозах; фильтрацию полученных данных и преобразование полученной информации в единый формат представления; модуль обогащения данных, обеспечивающий дополнение данных об индикаторах компрометации киберугроз из внешних источников данных; выполнение поиска и сбора информации о вредоносном коде, связанном с известными киберугрозами; обновление информации о кибербезопасности, включающей, по меньшей мере, сведения об уязвимости используемого программного обеспечения, о наличии вредоносного кода, связанного по меньшей мере с одной уязвимостью, и информацию об обновлении по меньшей мере одного программного обеспечения, обеспечивающего защиту по меньшей мере от одного типа уязвимости; выявление учетных записей пользователей, которые были задействованы при взаимодействии с ресурсами, связанными с индикаторами компрометации, информация по которым хранится в базе данных; базу данных, обеспечивающую хранение актуальной информации о киберугрозах, передаваемую от модулей получения данных и модуля обогащения данных; модуль интеграции, обеспечивающий передачу в унифицированном формате данных о киберугрозах системам кибербезопасности; модуль аналитики, обеспечивающий выполнение анализа уязвимостей ИТ-инфраструктуры в подключенных к модулю интеграции системах; выявление и отображение неявных связей между информационными сущностями, относящимися по меньшей мере к одному типу киберугрозы, с помощью анализа цепочек связей между упомянутыми сущностями и поиском общих узлов упомянутых сущностей.

038063 B1

038063 B1

Область техники

Настоящее изобретение в общем относится к области информационной защиты, а в частности к системе интеллектуального управления киберугрозами.

Уровень техники

В настоящее время с учетом массового применения ИТ (информационные технологии) в различных промышленных и экономических сферах, развитие систем и подходов в области кибербезопасности является одним из приоритетных направлений и требует постоянного усовершенствования с учетом постоянного появления новых типов киберугроз. В связи с этим важным аспектом создаваемых решений является актуализация информации о существующих типах киберугроз, а также сведений об их устранении и поддержание актуальной степени киберзащиты внутренней инфраструктуры.

В сфере банковского обслуживания проблема кибербезопасности играет ключевую роль, поскольку внутренняя информационная инфраструктура осуществляет обработку огромного количества структурированных и неструктурированных данных, что требует в свою очередь огромных ресурсов для своевременного выявления потенциально вредоносных объектов, которые могут привести к риску наступления киберугрозы. В качестве аналога заявленного изобретения можно рассмотреть способ выявления киберугроз на основании анализа пользовательских действий, раскрытый в заявке US 20170134415 A1 (патентообладатель: Splunk Inc, дата публикации: 11.05.2017). Известный способ использует алгоритмы машинного обучения для обновления моделей выявления отклонений от поведения сетевой активности пользователя, что может являться индикатором компрометации и свидетельствовать о попытке несанкционированного доступа к информационным ресурсам, порождая тем самым риск наступления угрозы кибербезопасности.

Недостатком известного подхода является отсутствие механизма постоянного обновления и обогащения данных о различных типах киберугроз с помощью мониторинга, выявления данных во внешних источниках информации и их последующую связь на основании данных об индикаторах компрометации для формирования информационных сущностей, содержащих актуальный срез информации о соответствующем типе киберугроз и средствах по их выявлению и устранению.

Раскрытие изобретения

Решаемой технической проблемой или технической задачей является создание новой системы, обеспечивающей интеллектуальное управление киберугрозами, которая обеспечивает комплексный подход в области организации и управления кибербезопасностью инфраструктуры.

Основным техническим результатом, который достигается при решении вышеуказанной технический проблемы, является повышение информационной безопасности за счет осуществления автоматизированной обработки данных о поступающих киберугрозах, обеспечивающей постоянную актуализацию данных о типах киберугроз и индикаторов компрометации, соответствующих им.

Дополнительным эффектом от реализации заявленного изобретения является увеличение скорости выявления индикаторов компрометации киберугроз за счет автоматизированного обогащения данных и построения сущностей, связывающих информацию о типах киберугроз и соответствующих им индикаторах компрометации в единое информационное пространство.

Заявленное изобретение представляет собой систему интеллектуального управления киберугрозами, которая содержит:

по меньшей мере один процессор, обеспечивающий обработку информационных потоков между модулями системы;

по меньшей мере одно средство хранения данных, содержащее машиночитаемые инструкции, исполняемые процессором;

модуль получения данных, обеспечивающий сбор информации из внешних и внутренних источников данных, содержащих информацию о киберугрозах;

фильтрацию полученных данных и преобразование полученной информации в единый формат представления;

модуль обогащения данных, обеспечивающий дополнение данных об индикаторах компрометации киберугроз из внешних источников данных;

выполнение поиска и сбора информации о вредоносном коде, связанном с известными киберугрозами;

обновление информации о кибербезопасности, включающей, по меньшей мере, следующие сведения:

об уязвимости используемого программного обеспечения, о наличии вредоносного кода, связанного по меньшей мере с одной уязвимостью, и информацию об обновлении по меньшей мере одного программного обеспечения, обеспечивающего защиту по меньшей мере от одного типа уязвимости;

выявление учетных записей пользователей, которые были задействованы при взаимодействии с ресурсами, связанными с индикаторами компрометации, информация по которым хранится в базе данных;

база данных, обеспечивающая хранение актуальной информации о киберугрозах, передаваемая от модулей получения данных и модуля обогащения данных;

модуль интеграции, обеспечивающий передачу в унифицированном формате данных о киберугрозах внутренним источникам;

модуль аналитики, обеспечивающий выполнение анализа уязвимостей ИТ-инфраструктуры в подключенных к модулю интеграции системах;

выявление и отображение неявных связей между информационными сущностями, относящимися по меньшей мере к одному типу киберугрозы, с помощью анализа цепочек связей между упомянутыми сущностями и поиска общих узлов упомянутых сущностей.

В одном из частных примеров реализации модуль получения данных дополнительно осуществляет дедупликацию данных, получаемых из внешних источников.

В другом частном примере реализации внешние источники передают данные в структурированном и неструктурированном виде.

В другом частном примере реализации данные получаются из вычислительной сети Интернет.

В другом частном примере реализации система дополнительно содержит модуль администрирования, обеспечивающий контроль прав доступа пользователей и журналирование процесса работы системы.

В другом частном примере реализации запрос данных из внешних источников осуществляется автоматически по расписанию или на основании внешнего запроса пользователя.

В другом частном примере реализации индикатор компрометации киберугроз выбирается из группы: IP-адрес, доменное имя, контрольная сумма, идентификатор ресурса или их сочетания.

В другом частном примере реализации модуль аналитики дополнительно осуществляет приоритезацию информации по киберугрозам.

В другом частном примере реализации приоритезация выполняется на основании ключевых слов или скоринга идентификатора угроз (CVE).

Краткое описание чертежей

Признаки и преимущества настоящего изобретения станут очевидными из приводимого ниже подробного описания изобретения и прилагаемых чертежей.

На фиг. 1 представлен общий вид заявленной системы.

На фиг. 2 представлен общий вид вычислительного устройства.

Осуществление изобретения

Ниже будут описаны понятия и термины, необходимые для понимания данного изобретения.

В данном изобретении под системой подразумевается в том числе компьютерная система, ЭВМ (электронно-вычислительная машина), ЧПУ (числовое программное управление), ПЛК (программируемый логический контроллер), компьютеризированные системы управления и любые другие устройства, способные выполнять заданную, четко определенную последовательность операций (действий, инструкций).

Под устройством обработки команд подразумевается электронный блок либо интегральная схема (микропроцессор), исполняющая машинные инструкции (программы).

Устройство обработки команд считывает и выполняет машинные инструкции (программы) с одного или более устройств хранения данных. В роли устройства хранения данных могут выступать, но не ограничиваясь, жесткие диски (HDD), флеш-память, ПЗУ (постоянное запоминающее устройство), твердотельные накопители (SSD), оптические приводы.

Программа - последовательность инструкций, предназначенных для исполнения устройством управления вычислительной машины или устройством обработки команд.

Киберугрозы - потенциально возможные события, действие (воздействие) которых может нарушить бизнес-процесс или состояние защищенности внутренней информационной инфраструктуры.

Аналитика киберугроз - регулярный и системный сбор, обогащение и обработка информации о киберугрозах в целях ее применения для защиты информационной безопасности.

Система аналитики киберугроз - система, предназначенная для частичной автоматизации процесса аналитики киберугроз.

Внешние источники данных о киберугрозах - ресурсы и сервисы, предоставляющие данные об уязвимостях и угрозах, такие как поставщики фидов (kaspersky security intelligence, IBM X-Force, Group-IB и т.п.), новостные сервисы, аналитические отчеты, посты в социальных сетях, информационные рассылки.

Внутренние источники данных - ресурсы и сервисы, предоставляющие данные от внутренних систем инфраструктуры, в частности от систем кибербезопасности, ИТ-систем.

Фид - коллекция индикаторов компрометации. В контексте текущего документа фид представляет собой поток данных о киберугрозах.

Идентификатор компрометации/Маркер компрометации (англ. Indicator of Compromise, далее - ИК) - перечень данных об угрозах, который дает возможность выявить наличие угрозы в инфраструктуре. В качестве ИК могут выступать список подозрительных или вредоносных IP-адресов, электронных почтовых адресов, доменных имен, идентификаторов сетевых ресурсов, контрольных сумм, имен объектов реестра (куст реестра, ключ и его значение) или файловой системы (путь до объекта, наименование объекта), образцы вредоносного поведения и др.

Эксплоит - компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.

CVE (англ. Common Vulnerabilities and Exposures) - база данных общеизвестных уязвимостей ин-

формационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер.

Как показано на фиг. 1, заявленное изобретение представляет собой распределенную вычислительную систему (100), обеспечивающую автоматизированную комплексную обработку информации о киберугрозах. Система (100) содержит систему интеллектуальной обработки киберугроз (130), которая обеспечивает взаимодействие между внутренней инфраструктурой и внешними источниками (110) в сети Интернет.

Система интеллектуальной обработки киберугроз (130) может выполняться на базе сервера или иного вида компьютерного устройства и содержит такие основные компоненты как процессор (131), средство хранения данных (132), модуль получения данных (133), модуль обогащения данных (134), модуль интеграции (135), модуль аналитики (136), модуль администрирования (137). Компоненты системы (130), как правило, соединяются посредством информационной шины, но также для специалиста должно быть очевидно, что принцип соединения компонентов может быть и иного типа, обеспечивая требуемую программно-аппаратную функциональность.

Процессор (131) осуществляет требуемую обработку информационных потоков между модулями системы (130) на основании машиночитаемых инструкций, хранимых в средстве (132). Под средством хранения данных (132) понимается одно или несколько запоминающих устройств, например ОЗУ, ПЗУ или их сочетания. Машиночитаемые команды, как правило, хранятся в ОЗУ при их непосредственном исполнении процессором (131). Дополнительные программные команды могут содержаться в ПЗУ и использоваться при выполнении соответствующей вычислительной операции. Система интеллектуальной обработки киберугроз (130) обеспечивает сбор и обработку данных, которые получаются из источников данных о киберугрозах. В качестве таких источников используются внешние источники данных (110) и внутренние источники (150). Внешние источники данных о киберугрозах (110) размещаются на различных ресурсах в сети Интернет и передаются по сети передачи данных (120) в модуль получения данных (133).

Модуль получения данных (133) предназначен для сбора информации из внешних (110) и внутренних (150) источников данных. Модуль (133) также осуществляет фильтрацию данных, получаемых из внешних источников (110), и выполняет преобразование полученной информации в единый формат представления. Модуль (133) обеспечивает работу с разнородной информацией, получаемой из внешних источников данных (110), в частности структурированной и неструктурированной информацией. Данные о киберугрозах, могут представлять собой

индикаторы компрометации (репутационные источники);

новостные источники;

тематические источники по уязвимостям;

эксплоиты;

источники обогащения (контекстные источники);

данные из сегмента теневого Интернета (англ. Darknet).

Модуль (133) обеспечивает также автоматизацию обработки получаемых данных, их последующую интеграцию и их преобразование в единый формат для последующего формирования информационных сущностей, идентифицирующих заданный тип киберугрозы. Модуль (133) осуществляет также формализацию получаемых данных, дедупликацию получаемых данных, обеспечивает поддержку таких форматов, как JSON, STIX, XML, HTML и др.

Фильтрация поступающей информации может осуществляться на основании даты размещения/публикации данных в сети Интернет, по ключевым словам, тегам и т.п. Дедупликация должна выполняться автоматически, путем формирования списков маркеров компрометации путем выделения их из контекста, полученного в процессе обработки данных фидов. Обработка неструктурированных данных с помощью модуля (133) может выполняться с помощью парсера. Модуль (133) позволяет осуществлять обработку данных в указанных форматах, получаемых не только из сети Интернет, но и поддерживает загрузку и последующую обработку в режиме "Upload" (Подгрузка), преобразуя данные в сущность CASE.

Алгоритм работы модуля получения данных (133) обеспечивает универсальный конструктор, который позволяет настроить алгоритмы сбора данных с различных внешних источников данных (110) через пользовательский интерфейс, в том числе

задание расписания сбора данных;

создание правил обработки собираемых данных;

возможность настройки HTTP(S) авторизации.

Поиск данных с помощью модуля обогащения (134) может включать в себя, например, сканирование страниц по списку определенных наборов URL, сканирование по тексту (может быть реализована поддержка многоязычных запросов и ответов). Сканирование может выполняться на основе ключевых слов или фраз, которые задаются пользователем, при этом создание ключевых фраз поддерживает использование логических операторов "И", "ИЛИ". Может быть также реализована возможность устанавливать произвольное значение процента наличия ключевых слов/фраз при сканировании. Сканирование может обеспечивать переход по ссылкам, указанным на странице, и сканирование страницы по ссылке.

Запуск сканирования может осуществляться по расписанию или по запросу пользователя.

Результат поиска может представляться в виде списка найденных ссылок с превью текста (несколько строк до и после ключевого слова/фразы). Может быть также осуществлена полнотекстовая индексация собираемых данных для быстрого извлечения данных по задаваемым пользователем параметрам. При выдаче результата поиска может выполняться группировка связанных друг с другом страниц по конкретной теме (ключевому слову, фразе) и тегам. Сохраняемые страницы имеют атрибуты, проставляемые пользователем (например, новая, в работе, обработана-используется, обработана-не используется). Для извлечения конкретной информации с просканированных страниц реализована возможность экспорта результата в форматы XML, JSON и т.п. Поисковый механизм может обеспечивать обход потенциального спама (спам-фильтр).

Данные, полученные и обработанные с помощью модуля (133), подлежат дальнейшей обработке с помощью модуля обогащения данных (134). Модуль обогащения данных (134) осуществляет дополнение данных об ИК киберугроз, полученных из внешних источников данных (110). Основным функциональным назначением модуля (134) является обогащение имеющихся (ранее полученных/хранимых) данных о киберугрозах, которые хранятся в базе данных (140). Обогащение может выполняться как в автоматизированном режиме, так и по пользовательскому запросу. Обогащение происходит за счет множественных интеграций с внешними (110) и внутренними (150) источниками, а также за счет обнаружения связных компонентов в базе данных (140). Модуль (134) также осуществляет выполнение поиска и сбора информации о вредоносном коде, связанном с известными киберугрозами, осуществляет обновление информации о кибербезопасности, в частности информацию об уязвимости используемого программного обеспечения внутренней инфраструктуры, о наличии вредоносного кода, связанного по меньшей мере с одной уязвимостью и информацию об обновлении по меньшей мере одного программного обеспечения, обеспечивающего защиту по меньшей мереот одного типа уязвимости.

Модуль обогащения данных (134) осуществляет выявление учетных записей пользователей, которые были задействованы при взаимодействии с ресурсами, связанными с индикаторами компрометации, информация по которым хранится в базе данных. Основной информацией для обогащения сведений об ИК, как правило, является дополнительная контекстная информация. Данная информация получается при обработке соответствующего запроса, генерируемого модулем (134). Контекст по ИК запрашивается на специализированном внешнем ресурсе (110), на который с помощью модуля (134) отправляются на анализ образцы, а в ответе получаются подробные отчеты с поведенческими индикаторами и баллами серьезности угрозы.

В момент импорта новых данных из внешних источников (110) с помощью модуля обогащения (134) осуществляется сравнение поступающей информации с уже хранимой в базе данных (140). В случае обнаружения изменений каких-либо атрибутов киберугроз осуществляется автоматическая актуализация данных. На этапе импорта происходит поиск существующих контекстов в базе данных (140) на основании значений ключевых полей и ИК. Если контекст с необходимыми значениями в ключевых полях существует в базе данных (140), то он дополняется отсутствующими атрибутами, в противном случае создается новый контекст, который поступает на автоматическую процедуру выявления ИК. Индикаторы могут быть найдены как в базовых полях, которые предназначены для хранения именно ИК, так и в прочих атрибутах контекста. Также в системе имеется возможность указания правил для извлечения ИК (или неизвлечения/исключения/пропуска).

В качестве образцов могут выступать типы файлов или файлоподобные объекты, например процесс, выполняемый в памяти, представленный и анализируемый с помощью упомянутого ресурса. Входными данными для ресурса могут выступать, например, доменное имя, IP-адрес, URL, Hash и т.п. В ответ на обработку запроса с образцом в модуль (134) поступает информация, связанная с определенным ИК, например доменное имя, IP-адрес или URL-адрес. Ресурс принимает входные данные в виде, например, доменного имени, IP или URL и возвращает все образцы, связанные с доменом. Данные возвращаются в систему (130) в виде вложенных массивов JSON. Данная функциональность позволяет извлекать новые ИК при получении новых компонентов киберугроз, которые ранее не присутствовали в базе данных (140). Также модуль (134) осуществляет обогащение информации о киберугрозах на основании ИК из таких внешних источников (110) как Threat Grid, VirusTotal, Kaspersky Threat Lookup, Domain Tools и др. Обогащение информации о киберугрозах с помощью модуля (134) осуществляется также с помощью поиска и сбора эксплоитов для обогащения уязвимостей из неструктурированных внешних источников (110), например exploit-db.com/, Oday.today и др. Поиск и сбор обновлений безопасности из неструктурированных источников (110), может, например, браться из каталога центра обновления Microsoft, ресурсов *NIX, систем - RedHat, FreeBsd и др. Система (130) содержит также базу данных (140), которая представляет собой централизованный банк угроз кибербезопасности. База данных (140) предназначена для хранения в формализованном виде любых данных, которые были получены из структурированных и неструктурированных источников данных. База данных (140) также хранит аналитические результаты, полученные по итогам экспертных оценок и автоматической обработки полученной информации.

База данных позволяет осуществлять ведение и учет следующих информационных сущностей:

Case - сущность, предназначенная для фиксации/ведения/анализа/разбора поступившей информа-

ции и данных о событиях кибербезопасности;

Actor;

Campaign;

Malware;

TTP;

News;

Vulnerability;

ИК;

Brand Monitoring - позволяет вести учет мошеннических ресурсов, платежных реквизитов с целью получения единой базы данных фишинговых/мошеннических кампаний;

Data Leakage.

Система (130) обеспечивает функциональность по выполнению различных операций над сущностями, в частности

создание, редактирование, удаление;

связывание сущностей между собой, построение графов связей;

просмотр списка, фильтрация списка по различным полям сущности;

тегирование сущностей;

прикрепление файлов;

управление черновиками;

управление статусами и состояниями,

например для новости применимо/неприменимо, новая/обработана;

управление версиями:

просмотр всех версий для каждой сущности с возможностью отображения всех изменений, которые были сделаны пользователем или автоматически;

возможность откатиться/вернуться к любой из сохраненных версий. В базе данных (140) также может храниться "белый список" для ИК, целью которого является предотвращение использования невалидных ИК во внутренней инфраструктуре. Могут также применяться и другие известные подходы для предотвращения использования невалидных ИК, например, анализ количества доменных имен на сетевом адресе (англ. "reverse whois") и др. В таблице представлен пример хранения записей о киберугрозах.

Данные о киберугрозах

Сущность	**Описание / Дополнительная информация**
IOC_dns	Информация о доменных именах, которые используются вредоносным программным обеспечением, либо задействованы в инфраструктуре злоумышленника.
IOC_email	Перечень e-mail адресов, задействованных в целях распространения фишинга, либо вредоносного программного обеспечения.
IOC_files	Экземпляры файлов вредоносного кода.
IOC_hash	Хэши вредоносных компонентов, которые присутствуют в системе после ее заражения.
IOC_ip	Список вредоносных IP-адресов, которые используются вредоносным программным обеспечением, либо задействованы в инфраструктуре злоумышленника.
IOC_process	Список имен процессов с вариациями местонахождения на файловой системе, которые вызывают или в которые внедряется вредоносный код.
IOC_registry	Ключи реестра, создаваемые или манипулируемые вредоносным программным обеспечением, либо его компонентами.
IOC_url	Адреса скомпрометированных и зараженных ресурсов, которые участвуют в распространение вредоносного программного обеспечения, либо задействованы в инфраструктуре злоумышленника.
IOC_Pipe	Список наименований именованных каналов, которые создаются вредоносным программным обеспечением при инфицировании вычислительного узла.
IOC_wmi	Список наименований подписок, которые создаются вредоносным программным обеспечением при инфицировании вычислительного узла.

Модуль интеграции (135) обеспечивает передачу в унифицированном формате данных о киберугрозах во внутреннюю инфраструктуру, в частности внутренние источники данных (150). Модуль (135) обеспечивает взаимодействие с системами мониторинга событий информационной безопасности, в частности передает наборы ИК для дальнейшего поиска в списках событий информационной безопасности. Для систем данного типа предоставляется контекстная информация о найденных ИК. Модуль интеграции (135) также получает от средств защиты информации (далее - СЗИ) и/или запрашивает статус индикаторов компрометации на конкретном СЗИ, а также информацию добавлении ИК в исключительные группы/списки, и позволяет осуществлять поиск информации по заданным ИК в журналах событий информационной безопасности за выбранный промежуток времени.

Модуль аналитики (136) обеспечивает взаимодействие с обрабатываемыми данными киберугроз, в частности с помощью модуля (136) осуществляется анализ уязвимостей ИТ-инфраструктуры в подключенных к модулю интеграции (135) внутренних источниках данных (150), выявление и отображение неявных связей между информационными сущностями, относящимися к тому или иному типу киберугроз, с помощью анализа цепочек связей между сущностями и поиска их общих узлов. Модуль аналитики (136) позволяет выявлять взаимосвязи между накопленными ИК, в частности по данным, которые уже присутствуют в базе данных (140), происходит построение связей.

Сущности в системе могут быть связаны между собой как в ручном режиме, так и автоматически. На одну и ту же сущность может быть несколько ссылок/связей из разных мест системы, которые могут быть созданы в разные временные промежутки в рамках различных ситуаций/инцидентов/аналитических отчетов, при этом каждая связь имеет направление (от конкретной сущности к другой конкретной сущности). Таким образом на основании хранящейся в базе данных (140) информации можно визуализировать первый уровень связей для конкретной сущности (т.е. отобразить сущности, на которые ссылается выбранная сущность или сущности, которые ссылаются на выбранную сущность), далее с помощью

функциональности модуля аналитики (136) можно для любой из визуализированных сущностей получить список связанных с ней сущностей и так далее, раскрывая любой из узлов до тех пор, пока в БД (140) существуют связанные сущности.

После раскрытия N уровней связей система (130) может сделать вывод о том, что сущности могут быть связаны между собой не напрямую одной связью, а через другие сущности, находящиеся на расстоянии по меньшей мере одного ребра от каждой. Таким образом, два и более базовых узла после раскрытия связанных с ними сущностей на N уровней могут иметь общие узлы, и такая связь между базовыми узлами называется неявной. Поиск подобных неявных связей и раскрытия связей для каждой сущности выполняется автоматически с помощью модуля аналитики (136).

Модуль (136) также обеспечивает интерактивное взаимодействие между пользователем и системой (130) с целью проведения киберразведки. Взаимодействие может осуществляться с помощью графического интерфейса пользователя (GUI), реализуемого на соответствующем компьютерном устройстве. Модуль аналитики (136) обладает конструктором информационных панелей (дашборды) и обеспечивает следующую функциональность:

создание пользовательских виджетов (Управление критериями отбора данных; Управление вариантами отображения данных);

настройка расположения виджетов;

настройка расписания обновления виджетов;

управление сортировкой;

управление группировкой (в том числе поддерживается многоуровневая группировка, количество уровней ограничено количеством полей, которые существуют для конкретной сущности.

Модуль (136) также содержит конструктор для работы с графом, в частности позволяет визуализировать объекты системы и связи между ними, позволяет найти неочевидные связи на разной глубине между исследуемыми объектами. Модуль аналитики (136) позволяет в автоматизированном режиме осуществлять анализ динамики запросов по тематике кибербезопасности (например, использование Google Trends). Модуль аналитики (136) обеспечивает также построение статистических срезов по заданному временному периоду, задаваемому по запросу пользователя, например неделя, месяц, год и т.п.

Система (130) может содержать также модуль администрирования (137), который обеспечивает контроль прав доступа пользователей и журналирование процесса работы системы (130). Разграничение прав доступа может быть реализовано с помощью известных подходов, в частности, таких как учетные записи, аппаратные средства идентификации (смарт-карта, USB-токен и др.), электронная подпись и т.п. Каждому пользователю может быть присвоен доступ к соответствующей части системы (130) для работы с заданной функциональностью.

Далее рассмотрим на примере процесс работы системы (130) с данными при обогащении информации о киберугрозах с помощью анализа внешних источников (110), в частности новостных источников в сети Интернет.

Данные из внешних источников (110) собираются с помощью их опроса модулем получения данных (133), например, согласно заданному расписанию сбора информации. Далее поступившая информация от источников (110) преобразуется в единый формат представления и выполняется их дедуплекация, что в совокупности формирует входной поток данных для модуля аналитики (136).

Модуль аналитики (136) на основании поступившего потока данных от модуля (133) осуществляет базовую приоритезацию полученных данных на основании заданных ключевых слов, что обеспечивает маркирование релевантной группы данных из большого потока поступающих данных, которые необходимо проанализировать в первую очередь. После анализа актуальности полученного потока задействуется функция ведения и учета сущностей. Первоначально формируется "аналитический отчет" в сущности CASE. Отчет содержит описательную часть полученного потока данных с возможностью задействовать иные сущности в рамках анализа, например добавить к CASE извлеченные ИК. После добавления ИК задействуются возможности модуля обогащения данных (134), который получает информацию от средств защиты информации инфраструктуры, например банка. В частности, такими параметрами могут выступать данные о статусе блокировок данного ИК во внутренней инфраструктуре. Модуль обогащения данных (134) выполняет также обращение к контекстным подпискам для получения возможных взаимосвязанных индикаторов. При этом сущность CASE линкуется (связывается) с новостью (и иными сущностями, в зависимости от содержимого новости), которая была обработана модулем аналитики (136) в системе (130) по сформированному потоку данных от внешних источников (110).

После того как сущность CASE из состояния "Draft" (проект) будет переведена в состояние "Published" (публикация), модуль интеграции (135) выполняет отправку внесенных ИК (в текущем контексте информация о киберугрозах, для определенных систем, представляется сущностью - индикатор компрометации) в систему мониторинга событий информационной безопасности. Модуль интеграции (135) также позволяет аналитику отправить запрос в систему мониторинга событий информационной безопасности с целью получения исторических сведений о наличии добавленных ИК в инфраструктуре за N-период. При получении данных о наличии ИК в инфраструктуре за прошедший N-период модуль обогащения данных (134) производит сбор информации об источнике. Например, определяется сетевая зона

источника инцидента, принадлежность к учетной записи пользователя, а также полная информация о пользователе из иных систем ведения учета пользователей.

По результатам публикации сущности CASE, если требуется блокировка ИК либо заведение какой-либо иной заявки в системе учета заявок (тикетинг), модуль интеграции (135) заполняет определенный набор полей заявки данными из сущности CASE и осуществляет ее регистрацию в системе учета заявок (тикетинг). Далее рассмотрим процесс обработки информации, связанной с уязвимостями. При работе с данным типом информации модуль получения данных (133), согласно заданному расписанию, осуществляет сбор данных из внешних источников (110), выполняет их преобразование в единый формат представления и осуществляет дедупликацию данных, что в совокупности формирует входной поток данных для модуля аналитики (136), при этом учитываются возможные агрегирования схожих потоков данных. Дедупликация данных выполняется, если информация собирается из разных источников, при отсутствии единого эталонного источника данных.

Модуль аналитики (136) на основании поступившего потока данных от модуля (133) осуществляет базовую приоритезацию полученных данных на основании заданных ключевых слов, что обеспечивает маркирование релевантной группы данных из большого потока поступающих данных, которые необходимо проанализировать в первую очередь. Модуль обогащения данных (134) совместно с модулем получения данных (133) осуществляет сбор дополнительной информации из сети Интернет, с учетом идентификатора уязвимости (CVE) следующего вида: наличие программного кода для эксплуатации обозначенной уязвимости (эксплоит), информация об обновлениях безопасности, в том числе замещающих/перекрестных (Microsoft), информация о пакетах безопасности (согласно менеджеру пакетов Unix/Linux систем), информация о версионности уязвимого объекта, информация об общей оценки уязвимости с учетом ее версионности (CVSS 2.0 или CVSS 3.0) и иные атрибуты, используемые в сущности "Vulnerability" (уязвимость).

При этом модуль обогащения (134), согласно заданному расписанию, для сущностей типа "Vulnerability" осуществляет непрерывный процесс поиска дополнительной информации в сети Интернет на определенных ресурсах. В процессе обработки информации по той или иной уязвимости системой (130) задействуется функция ведения и учета сущностей. Первоначально система (130) в автоматизированном режиме формирует сущность "Vulnerability", которая агрегирует результаты работы вышеописанных модулей. Агрегированная информация с учетом приоритезации передается для дальнейшего анализа в модуль аналитики (136).

Во время обработки сущности "Vulnerability" с помощью модуля аналитики (136) также задействуется модуль интеграции (135) для выполнения оценки применимости найденной уязвимости к инфраструктуре. Модуль интеграции (135) позволяет отправить запрос в централизованные системы ведения ИТ-активов, например для определения наличия обновлений безопасности или иных атрибутов, используемых в сущности "Vulnerability".

Модуль аналитики (136) выполняет анализ полученных данных от модуля интеграции (135) согласно заложенным алгоритмам обработки информации. При этом, если тип уязвимости является сетевым, модуль аналитики (136) может осуществить повторный вызов модуля интеграции (135) для получения информации о сетевой достижимости конечных вычислительных узлов. В последующем эта информация может влиять на оценку применимости обрабатываемой уязвимости.

После выполнения анализа (определение актуальности) полученного потока данных об уязвимости и применения ее в инфраструктуре повторно задействуется функция ведения и учета сущностей. По результатам анализа создается "аналитический отчет" в сущности CASE. По результатам публикации сущности CASE, если требуются шаги по устранению уязвимости, либо заведение какой-либо иной заявки в системе учета заявок (тикетинг), модуль интеграции (135) заполняет определенный набор полей заявки данными из сущности CASE и осуществляет ее регистрацию в системе учета заявок (тикетинг).

На фиг. 2 представлен пример общего вида вычислительного устройства (200), с помощью которого может быть реализована функциональность системы (130).

Устройство (200) может является частью компьютерной системы, например сервером, компьютером, облачной платформой и т.п.

В общем случае вычислительное устройство (200) содержит объединенные общей шиной информационного обмена один или несколько процессоров (201), средства памяти, такие как ОЗУ (202) и ПЗУ (203), интерфейсы ввода/вывода (204), устройства ввода/вывода (205), устройство для сетевого взаимодействия (206).

Процессор (201) (или несколько процессоров, многоядерный процессор) могут выбираться из ассортимента устройств, широко применяемых в текущее время, например, компаний Intel™, AMD™, Apple™, Samsung Exynos™, MediaTEK™, Qualcomm Snapdragon™ и т.п. Под процессором также необходимо учитывать графический процессор, например, GPU NVIDIA или ATI, который также может являться пригодным для выполнения требуемой функциональности по вычислительной обработке. При этом средством памяти также может выступать доступный объем памяти графической карты или графического процессора.

ОЗУ (202) представляет собой оперативную память и предназначено для хранения исполняемых процессором (201) машиночитаемых инструкций для выполнения необходимых операций по логической обработке данных. ОЗУ (202), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.).

ПЗУ (203) представляет собой одно или более устройств постоянного хранения данных, например жесткий диск (HDD), твердотельный накопитель данных (SSD), флэш-память (EEPROM, NAND и т.п.), оптические носители информации (CD-R/RW, DVD-R/RW, BlueRay Disc, MD) и др.

Для организации работы компонентов устройства (200) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (204). Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь: PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т.п. Для обеспечения взаимодействия пользователя с вычислительным устройством (200) применяются различные средства (205) В/В информации, например клавиатура, дисплей (монитор), сенсорный дисплей, тач-пад, джойстик, манипулятор мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т.п.

Средство сетевого взаимодействия (206) обеспечивает передачу данных устройством (200) посредством внутренней или внешней вычислительной сети, например Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (206) может использоваться, но не ограничиваться: Ethernet карта, GSM модем, GPRS модем, LTE модем, 5G модем, модуль спутниковой связи, NFC модуль, Bluetooth и/или BLE модуль, Wi-Fi модуль и др.

Дополнительно могут применяться также средства спутниковой навигации в составе устройства (200), например GPS, ГЛОНАСС, BeiDou, Galileo. Представленные материалы раскрывают предпочтительные примеры реализации изобретения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области техники.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система интеллектуального управления киберугрозами, содержащая

по меньшей мере один процессор, обеспечивающий обработку информационных потоков между модулями системы;

по меньшей мере одно средство хранения данных, содержащее машиночитаемые инструкции, исполняемые процессором;

модуль получения данных, обеспечивающий

сбор информации из внешних и внутренних источников данных, содержащих информацию о киберугрозах;

фильтрацию полученных данных и преобразование полученной информации в единый формат представления;

модуль обогащения данных, обеспечивающий

дополнение данных об индикаторах компрометации киберугроз из внешних источников данных;

выполнение поиска и сбора информации о вредоносном коде, связанном с известными киберугрозами;

обновление информации о кибербезопасности, включающей, по меньшей мере, следующие сведения: об уязвимости используемого программного обеспечения, о наличии вредоносного кода, связанного по меньшей мере с одной уязвимостью, и информация об обновлении по меньшей мере одного программного обеспечения, обеспечивающего защиту по меньшей мере от одного типа уязвимости;

выявление учетных записей пользователей, которые были задействованы при взаимодействии с ресурсами, связанными с индикаторами компрометации, информация по которым хранится в базе данных;

база данных, обеспечивающая хранение актуальной информации о киберугрозах, передаваемой от модулей получения данных и модуля обогащения данных;

модуль интеграции, обеспечивающий передачу в унифицированном формате данных о киберугрозах во внутренние источники;

модуль аналитики, обеспечивающий

выполнение анализа уязвимостей ИТ-инфраструктуры в подключенных к модулю интеграции системах;

выявление и отображение неявных связей между информационными сущностями, относящимися по меньшей мере к одному типу киберугрозы, с помощью анализа цепочек связей между упомянутыми сущностями и поиском общих узлов упомянутых сущностей.

2. Система по п.1, характеризующаяся тем, что модуль получения данных дополнительно осущест-

вляет дедупликацию данных, получаемых из внешних источников.

3. Система по п.1, характеризующаяся тем, что внешние источники передают данные в структурированном и неструктурированном виде.

4. Система по п.3, характеризующаяся тем, что данные получаются из вычислительной сети Интернет.

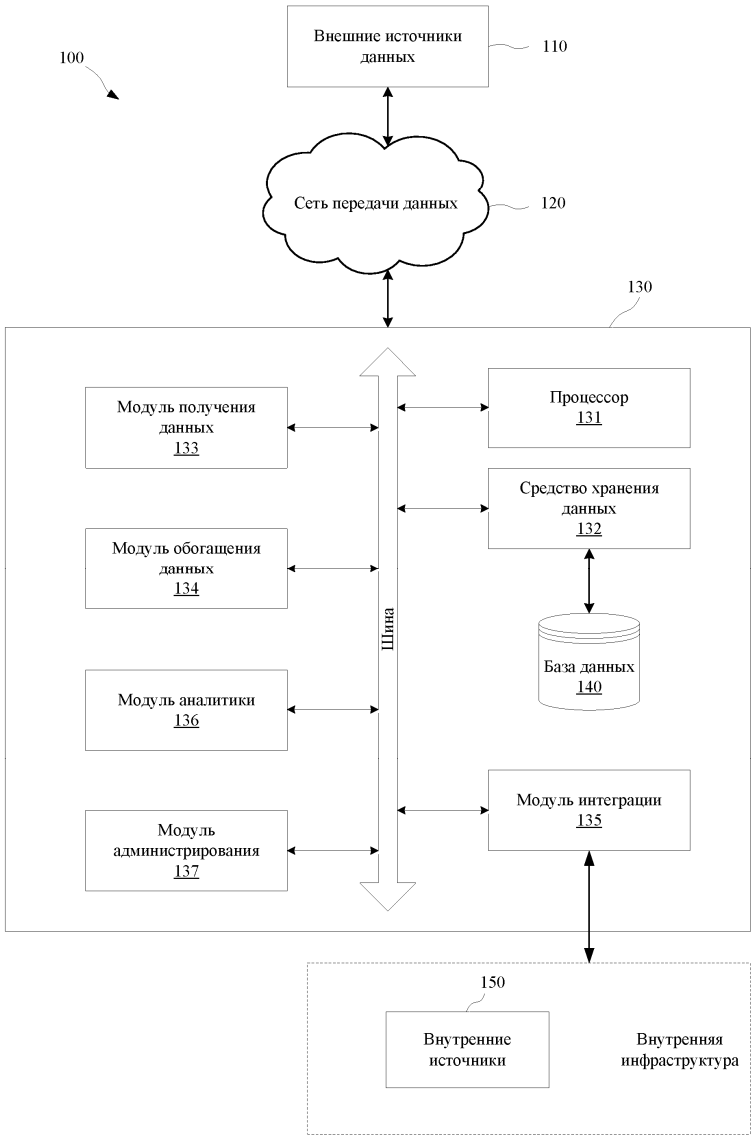
5. Система по п.1, характеризующаяся тем, что дополнительно содержит модуль администрирования, обеспечивающий контроль прав доступа пользователей и журналирование процесса работы системы.

6. Система по п.1, характеризующаяся тем, что запрос данных из внешних источников осуществляется автоматически по расписанию или на основании внешнего запроса пользователя.

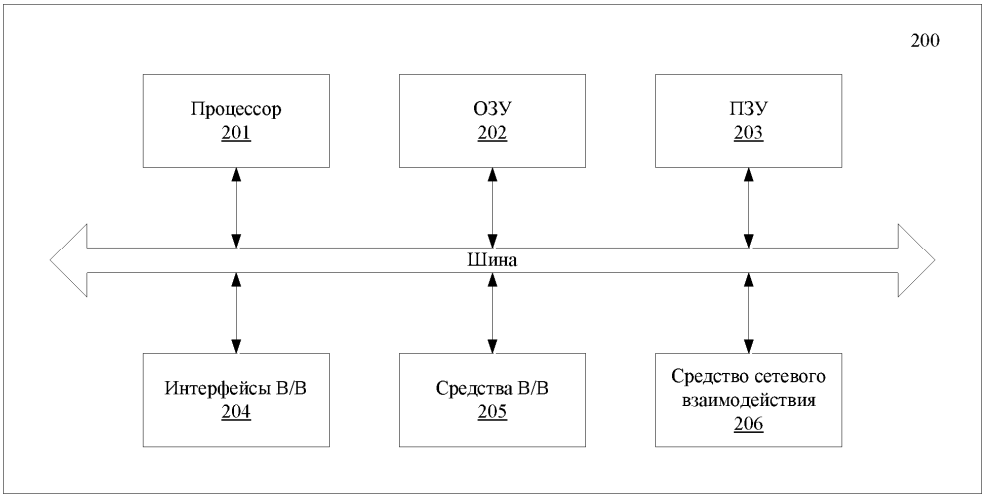
7. Система по п.1, характеризующаяся тем, что индикатор компрометации киберугроз выбирается из группы: IP-адрес, доменное имя, контрольная сумма, идентификатор ресурса или их сочетания.

8. Система по п.1, характеризующаяся тем, что модуль аналитики дополнительно осуществляет приоритезацию информации по киберугрозам.

9. Система по п.8, характеризующаяся тем, что приоритезация выполняется на основании ключевых слов или скоринга идентификатора угроз (CVE).



Фиг. 1



Фиг. 2

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2