(19) Евразийское патентное ведомство

(21) 202092860 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2022.02.28

(22) Дата подачи заявки
2020.12.23

(51) Int. Cl. ***G06F 17/00*** (2019.01)
G06F 21/00 (2013.01)

(54) СИСТЕМА ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ РИСКАМИ И УЯЗВИМОСТЯМИ ЭЛЕМЕНТОВ ИНФРАСТРУКТУРЫ

(31) **2020125916**
(32) **2020.08.04**
(33) **RU**

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

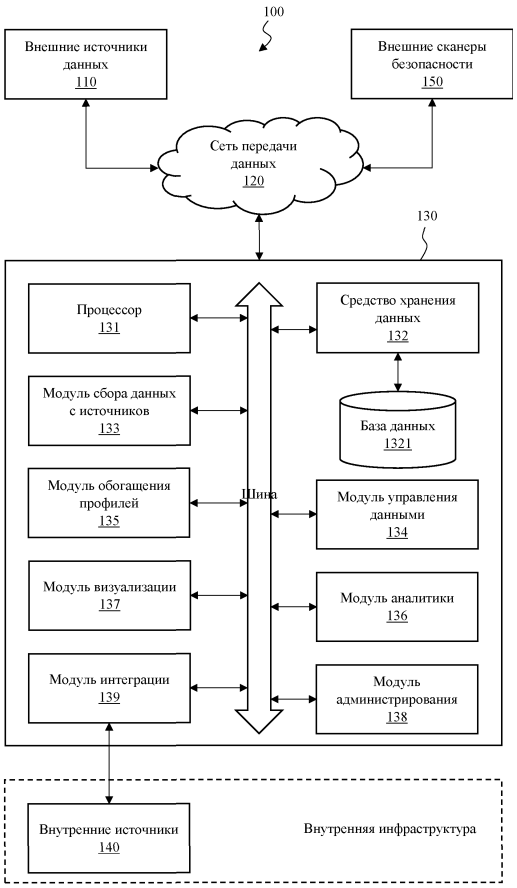
(72) Изобретатель:
Рюпичев Дмитрий Юрьевич, Новиков Евгений Александрович, Ничипорчук Максим Михайлович, Махмутов Рустем Дмитриевич, Эфендян Грант Сергеевич (RU)

(74) Представитель:
Герасин Б.В. (RU)

(57) Изобретение относится к области компьютерных технологий, в частности к информационной защите, для которых предлагается система интеллектуального управления рисками и уязвимостями элементов инфраструктуры. Техническим результатом является повышение эффективности управления безопасностью инфраструктуры, за счет обеспечения полного цикла управления уязвимостями и связанными с ними рисками, с возможностью их своевременного выявления и устранения. Заявленная система интеллектуального управления рисками и уязвимостями элементов инфраструктуры включает в себя по меньшей мере один процессор; по меньшей мере одно запоминающее устройство; модуль сбора данных с источников, выполненный с возможностью получения информации из источников данных, содержащих информацию об уязвимостях элементов инфраструктуры (ЭИ), включающие в себя функциональные и логические ЭИ, при этом функциональные ЭИ представляют собой активы инфраструктуры (АИ), содержащие оконечное физическое или виртуальное оборудование, предоставляющее услугу и/или сервис, и сетевые ЭИ, представляющие устройства, обеспечивающие сетевое взаимодействие между всеми функциональными ЭИ; логические ЭИ представляют собой объединения функциональных ЭИ и логических ЭИ, включающих сущности, взаимодействующие с сетевой инфраструктурой и выбираемые из группы: автоматизированные системы, функциональные подсистемы, или сервисы; модуль управления данными, выполненный с возможностью нормализации данных, собираемых модулем сбора данных, обеспечивая формирование унифицированного вида данных и формирование атрибутного состава в зависимости от типа ЭИ; формирование профиля ЭИ, содержащего атрибутный состав ЭИ; модуль обогащения профилей ЭИ, выполненный с возможностью дополнения атрибутного состава профиля ЭИ информацией, включающей в себя информацию о возможности сетевого взаимодействия между АИ, на основании данных правил безопасности (ACL), а также правил трансляции (NAT) и маршрутизации, определенных на сетевых ЭИ; найденные уязвимости на АИ; данные о критичности функционирования логических ЭИ; сведения о выявленных рисках, а также мероприятиях по их устранению; модуль аналитики, выполненный с возможностью учета, анализа и мониторинга внешнего периметра сетевой инфраструктуры; поиска по атрибутному составу профилей активов; анализа необработанных данных, поступающих из источников данных; управления рисками по найденным уязвимостям; поиска и анализа сетевых маршрутов между АИ для определения возможных путей распространения угрозы; расчёта критичности уязвимого АИ за счет определения влияния уязвимостей на сетевую инфраструктуру и ее функционирование.

202092860 A1

202092860 A1



202092860 A1

202092860 A1

МПК: G06F 17/00; G06F 21/00

СИСТЕМА ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ РИСКАМИ И УЯЗВИМОСТЯМИ ЭЛЕМЕНТОВ ИНФРАСТРУКТУРЫ

ОБЛАСТЬ ТЕХНИКИ

[0001] Настоящее техническое решение относится к области компьютерных технологий, в частности к информационной защите, для которых предлагается система интеллектуального управления рисками и уязвимостями элементов инфраструктуры.

УРОВЕНЬ ТЕХНИКИ

[0002] 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.

[0003] 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.

[0004] В качестве одного из примеров применяемых технологий для управления рисками и потенциальными уязвимостями инфраструктуры можно рассмотреть решение компании Skybox – Vulnerability Control (https://www.skyboxsecurity.com/products/vulnerability-control/). Данное решение позволяет комплексно оценивать потенциальные риски нарушения кибербезопасности инфраструктуры и осуществлять контроль за уязвимостями.

[0005] Другим известным решением является система интеллектуального управления киберугрозами (патент РФ № 2702269, 07.10.2019), которая содержит модульную архитектуру, позволяющую анализировать и обогащать сведения о киберугрозах инфраструктуры для последующего оперативного отслеживания и распознавания киберугроз.

[0006] Заявленное решение направлено на усовершенствование существующих разработок в данной области техники, обеспечивая новую, расширенную

функциональность в части комплексного управления кибербезопасностью инфраструктуры, обеспечивая своевременное выявление уязвимостей, и анализ всех элементов инфраструктуры для обеспечения сетевой безопасности.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

[0007] Настоящее техническое решение направлено на решение технической проблемы, заключающейся в создании нового и эффективного средства управления рисками и уязвимостями инфраструктуры.

[0008] Техническим результатом является повышение эффективности управления безопасностью инфраструктуры, за счет обеспечения полного цикла управления уязвимостями и связанными с ними рисками, с возможностью их своевременного выявления и устранения.

[0009] Дополнительным результатом является расширение функциональных возможностей анализа возникновения рисков киберугроз, за счет отслеживания возможных путей распространения угроз между элементами инфраструктуры.

[0010] Другим дополнительным результатом является формирование исходных данных, необходимых для устранения уязвимостей, таких как:

- идентификационная информация об элементах инфраструктуры (ЭИ);
- информация об обнаруженной уязвимости;
- информация о мероприятиях, необходимых для устранения обнаруженной уязвимости.

[0011] Заявленный технический результат достигается за счет осуществления настоящего изобретения, представляющего собой систему интеллектуального управления рисками и уязвимостями элементов инфраструктуры, которая включает в себя:

- по меньшей мере один процессор;
- по меньшей мере одно запоминающее устройство;
- модуль сбора данных с источников, выполненный с возможностью получения информации из источников данных, содержащих информацию об уязвимостях элементов инфраструктуры (ЭИ), включающие в себя функциональные и логические ЭИ, при этом

  функциональные ЭИ представляют собой активы инфраструктуры (АИ), содержащие оконечное физическое или виртуальное оборудование, предоставляющее услугу и/или сервис, и сетевые ЭИ, представляющие устройства, обеспечивающие сетевое взаимодействие между всеми функциональными ЭИ;

логические ЭИ представляют собой объединения функциональных ЭИ и логических ЭИ, включающих сущности, взаимодействующие с сетевой инфраструктурой и выбираемые из группы: автоматизированные системы, функциональные подсистемы, или сервисы;

- модуль управления данными, выполненный с возможностью

  нормализации данных, собираемых модулем сбора данных, обеспечивая формирование унифицированного вида данных и формирование атрибутного состава в зависимости от типа ЭИ;

  формирование профиля ЭИ, содержащего атрибутный состав ЭИ;

- модуль обогащения профилей ЭИ, выполненный с возможностью дополнения атрибутного состава профиля ЭИ информацией, включающей в себя:

  информацию о возможности сетевого взаимодействия между АИ, на основании данных правил безопасности (ACL), а также правил трансляции (NAT) и маршрутизации, определенных на сетевых ЭИ;

  найденные уязвимости на АИ;

  данные о критичности функционирования логических ЭИ;

  сведения о выявленных рисках, а также мероприятиях по их устранению;

- модуль аналитики, выполненный с возможностью

  учета, анализа и мониторинга внешнего периметра сетевой инфраструктуры;

  поиска по атрибутному составу профилей активов;

  анализа необработанных данных, поступающих из источников данных;

  управления рисками по найденным уязвимостям;

  поиска и анализа сетевых маршрутов между АИ для определения возможных путей распространения угрозы;

  расчёта критичности уязвимого АИ за счет определения влияния уязвимостей на сетевую инфраструктуру и ее функционирование.

[0012] В одном из частных примеров осуществления системы атрибутный состав актива инфраструктуры включает в себя категорию и тип устройств инфраструктуры.

[0013] В другом частном примере осуществления системы информация по обогащению профиля актива инфраструктуры по взаимодействию сетевых потоков получается на основании полученных атрибутов по устройствам инфраструктуры.

[0014] В другом частном примере осуществления системы информация по обогащению профиля актива по найденным уязвимостям на активах формируется на основании полученных результатов работы сканера безопасности.

[0015] В другом частном примере осуществления системы данные для расчета критичности актива или уязвимости получаются из внешних систем.

[0016] В другом частном примере осуществления системы модуль аналитики дополнительно обеспечивает формирование графовых моделей на основании полученных данных по сетевым потокам и информации о связях функциональных ЭИ и логических ЭИ между собой.

[0017] В другом частном примере осуществления системы осуществляется моделирование распространения угрозы за счет определения области уязвимых активов инфраструктуры.

[0018] В другом частном примере осуществления системы дополнительно учитывается информация по взаимодействию сетевых потоков.

[0019] В другом частном примере осуществления системы обеспечивается определение узлов отказа при сетевом взаимодействии и последствий наступления такого рода отказа.

[0020] В другом частном примере осуществления системы модуль аналитики дополнительно обеспечивает управление сканированием, при котором формируется список сетевых адресов для передачи их сканеру безопасности.

[0021] В другом частном примере осуществления системы модуль аналитики дополнительно обеспечивает управление режимом устранения уязвимостей, при котором выявляются активы инфраструктуры для устранения найденных на них уязвимостей.

[0022] В другом частном примере осуществления система дополнительно содержит модуль визуализации, обеспечивающий графическое представление обрабатываемых данных.

[0023] В другом частном примере осуществления системы модуль визуализации обеспечивает формирование виджетов и/или отчетов и/или информационных панелей.

[0024] В другом частном примере осуществления система дополнительно содержит модуль администрирования, обеспечивающий управление политиками доступа, справочниками, настройками существующих модулей системы.

[0025] В другом частном примере осуществления системы при выявлении модулем обогащения АИ, для которых имеется информация об уязвимостях, осуществляется передача упомянутой информации во внешнюю систему для получения пакетов обновлений для устранения уязвимостей на упомянутых АИ.

[0026] В другом частном примере осуществления системы процесс выполняется итеративно для всех АИ, для которых происходит обнаружение уязвимостей.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0027] Фиг. 1 иллюстрирует общий вид заявленного решения.

[0028] Фиг. 2 иллюстрирует пример профиля актива инфраструктуры.

[0029] Фиг. 3 иллюстрирует общий вид вычислительного устройства.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

[0030] В настоящем описании далее будут использоваться следующие термины и определения.

[0031] **Киберугрозы** — потенциально возможные события, действие (воздействие) которых может нарушить бизнес-процесс или состояние защищенности внутренней информационной инфраструктуры.

[0032] **Внешние источники данных о Киберугрозах** — ресурсы и сервисы, предоставляющие данные об уязвимостях, эксплоитах, обновлениях безопасности, результатах сканирования внешнего периметра инфраструктуры.

[0033] **Внутренние источники данных** — ресурсы и сервисы, предоставляющие данные от внутренних систем инфраструктуры, в частности, от систем кибербезопасности, ИТ-систем.

[0034] **Эксплоит** — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.

[0035] **CVE** (англ. Common Vulnerabilities and Exposures) — база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер.

[0036] **Элементы инфраструктуры (ЭИ) —** функциональные и логические ЭИ.

[0037] **Функциональные ЭИ** — ЭИ включающие в себя **Активы инфраструктуры (АИ)**, представляющие собой оконечное физическое или виртуальное оборудование предоставляющее услугу/сервис, выполняющие заданные функции внутри инфраструктуры, например: виртуальные машины, серверное оборудование, АРМ, устройства самообслуживания (банкоматы, терминалы), и т.д.; а также **Сетевые элементы инфраструктуры** — промежуточные устройства (фаерволы, балансировщики, маршрутизаторы и пр.), обеспечивающие сетевое взаимодействие между всеми функциональными элементами инфраструктуры.

[0038] **Логические ЭИ** — группа функциональных элементов и их логическое объединение, например: автоматизированные системы, функциональные подсистемы, или сервисы.

[0039] На Фиг. 1 представлен общий вид заявленного решения (100), которое включает в себя объединенные сетью передачи данных (120), внешние (110) и внутренние источники информации (140), систему (130) интеллектуального управления рисками и уязвимостями элементов инфраструктуры и внешние сканеры безопасности.

[0040] В качестве сети передачи данных (120) может применяться любой известный принцип сетевого обмена, например, Интернет, Интранет, LAN, WAN, PAN, WLAN и т.п.

[0041] Система (130) может выполняться на базе одного или нескольких вычислительных устройств, с программной или программно-аппаратной реализацией модулей (131)-(139) системы (130). Каждый модуль системы (130) при этом может выполняться в виде ПЛИС, SoC (система на чипе), микроконтроллера, логических вентилей, программной логики и т.п. В общем случае необходимые процессы вычислительной логики в системе (130) осуществляются с помощью одного или нескольких процессоров (131), которые обрабатывают команды, передаваемые по общей шине данных между модулями системы (130).

[0042] Модуль сбора данных с источников (133) отвечает за получение информации о найденных уязвимостях, а также получение информации по атрибутному составу ЭИ. Модуль (133) получает данные от внешних (110) и внутренних (140) источников данных, при этом собираемая информация содержит информацию об уязвимостях, активах инфраструктуры и взаимодействиях их сетевых потоков.

[0043] Для сбора данных модулем (133) поддерживаются различные форматы: CPE (Common platform enumeration), XML, JSON, и др. Функциональность модуля (133) также обеспечивает фильтрацию полученных данных и преобразование полученной информации в единый формат представления.

[0044] В качестве внешних источников (110) получения данных об элементах инфраструктуры (внешний периметр) и уязвимостях могут выступать:

- Системы для анализа защищенности (сканеры безопасности – 150), такие как:
  MaxPatrol, Tenable, Qualys, Rapid7 Nexpose, Nmap, Acunetix и др.
- Сервисы по TI/Vulnerability, такие как:
  TIP Sberbank, Shodan, Censys, CPT.Bizone, Anomaly, RiskIQ, Kaspersky Threat Lookup, Group-IB и др.

[0045] Внутренние источники (140) получения данных об активах инфраструктуры и уязвимостях могут представлять собой:

- Системы управления и учета ИТ-инфраструктуры, такие как:
  SCCM, uCMDB, HPSM, EMM (Enterprise Mobility Management – AirWatch), AD (Active Directory), локальные сенсоры и др.

- Системы защиты и анализа инфраструктуры (сканеры безопасности), а также мониторинга событий информационной безопасности, такие как:

  Сканеры безопасности MaxPatrol, Qualys, Nessus, Rapid7 Nexpose, Nmap, Acunetix и др.
- Антивирусные средства защиты: Kaspersky, ESET, SEP и др.
- Системы хранения и мониторинга событий информационной безопасности: Qradar, ArcSight, ClickHouse, Splunk и др.
- Системы управления и учета (менеджмент/оркестратор) сетевым оборудованием:

  Tufin, Cisco Security Management (управлением системами класса FW, NGFW);

  APSolute VISION (управление системами класса балансировки нагрузки);

  BIG-IQ (управление системами класса Web Application Firewall – WAF);

  IPAM/NOC (учет сетевой конфигурации)

  Arbor (управление системами класса Anti-DDos) и др.

[0046] По собранной информации модулем сбора (133) формируется сырой (RAW) набор данных об ЭИ. Далее эта информация передается в средство хранения данных (132), например, ПЗУ, содержащее базу данных (1321). Сохраненная информация, переданная от модуля (133), обрабатывается модулем (134) управления данными.

[0047] Модуль (134) Управление данными отвечает за работу с данными, которые были собраны в базе данных (1321). Модуль (134) выполняет нормализацию собранных модулем (133) данных, обеспечивая формирование унифицированного вида данных и формирования атрибутного состава в зависимости от типа ЭИ. Также, модуль (134) осуществляет формирование базового профиля ЭИ, содержащего атрибутный состав ЭИ.

[0048] Алгоритмы работы, выполняемые модулем (134), отвечают за приведение к единому виду по меньшей мере следующих атрибутов: наименование операционной системы, наименование программного обеспечения и ее версионность, наименование сервисов/служб и т.д.

[0049] Формирование базового профиля ЭИ включает в себя формирование атрибутного состава в зависимости от типа ЭИ. Один и тот же атрибут ЭИ может собираться с разных систем – мастер система и вспомогательная система. Это необходимо для поиска и контроля ошибок в системах учета. В основу модели ЭИ (АРМ, сервер, мобильный телефон, принтер, сетевое устройство, КЭ, сканирование и т.д.), заложена двухуровневая модель, состоящая из «Категория:Тип». Например, «Категория» – сетевое устройство, «Тип» – коммутатор, маршрутизатор, фаервол, балансировщик и т.д.

[0050] Каждая пара «Категория:Тип» обладает своим атрибутным составом (это означает, что атрибуты у АРМ, будут отличаться от атрибутов сетевого оборудования). На Фиг. 2 приведен пример базового атрибутного состава профиля АРМ.

[0051] Модуль (135) обогащение профилей позволяет обогатить базовые профили разных активов информацией из атрибутного состава других активов. Например: «Категория» – сетевое устройство, «Тип» – фаервол. У данного профиля есть свой атрибутный состав, в котором, есть такие атрибуты, как ACL (правила безопасности для сетевого пакета), NAT (правила трансляции) и т.д. Есть ЭИ, которые представляют собой уже конечные точки – АРМ, сервер и т.д. Таким образом, возможно определить сетевую достижимость ЭИ А (АРМ) до ЭИ Б (АРМ) на основании данных фаерволов, что позволяет сформировать механизм, позволяющий определить достижимость ЭИ.

[0052] Модуль обогащения профилей (135) обеспечивает дополнение атрибутного состава базового профиля ЭИ следующей информацией:

- взаимодействие сетевых потоков, на основании полученных атрибутов по сетевым устройствам;
- найденные уязвимости на ЭИ, на основании полученных результатов работы сканера безопасности, либо собственного алгоритма сопоставления CVE для АЭ;
- критичность ЭИ или уязвимости из сторонних систем;
- выявленные и/или установленные риски и мероприятия по их устранению.

[0053] Модуль (135) также выполнен с возможностью обогащения ЭИ, для которых имеется информация об уязвимостях, для чего осуществляется передача упомянутой информации во внешнюю систему для получения пакетов обновлений для устранения уязвимостей на упомянутых ЭИ. Данный процесс выполняется итеративно для всех ЭИ, для которых происходит обнаружение уязвимостей.

[0054] Аналитический модуль (136) реализует аналитические алгоритмы, обеспечивающие анализ накопленной информации по уязвимостям и активам инфраструктуры, а также выполняет приоритезацию их обработки и устранения.

[0055] В частности, модуль (136) осуществляет анализ и мониторинг внешнего периметра инфраструктуры. Периметр инфраструктуры может сканироваться в режиме «инвентаризации», а также в режиме «поиска уязвимостей». Режим «инвентаризации» оперирует данным типа «адрес:порт», чтобы найти соответствующий ЭИ, например, сервер, внутри инфраструктуры, а только потом взаимодействует с информацией об обнаруженных уязвимостях. Это обусловлено тем, что найденную уязвимость на периметре (большую их часть), невозможно проанализировать/верифицировать, не зная, на каком конечном/промежуточном узле она найдена.

[0056] Модуль (136) обеспечивает также работу с ненормализованными данными, что позволяет проводить более глубокую аналитику, за счет возможности поиска по «сырым» и «ненормализованным» данным. Поиск может выполняться по атрибутному составу профилей ЭИ, с помощью механизма фильтрации требуемых атрибутов ЭИ. Эта функция применяется для оперативного определения набора ЭИ по заданному фильтру.

[0057] Управление рисками с помощью модуля аналитики (136) выполняется по найденным уязвимостям ЭИ, для чего реализуется функция заведения и контроля рисков, при которой могут осуществляться следующие шаги:

- предоставление возможности управления полным циклом работы с рисками как на стороне платформы, так и в сторонней системе управления инцидентами информационной безопасности;
- выполнение привязки: ЭИ – CVE – риск, что в последствии используется, как данные для учета информации по рискам. Также данная информация позволяет избежать дублирования рисков и активов, за счет отслеживания уже используемых CVE и активов в ранее заведенных рисках;
- обеспечение контроля за выполнением SLA риска, а также нотификация о его нарушении в сторону ответственных/координирующих лиц, указанных в риске;
- связывание рисков с автоматизированными системами, за счет обогащения информацией из конфигурационных элементов;
- обеспечение вычисления уровня критичности риска за счет наличия определенных условий: наличие эксплоитов в публичном или ограниченном доступе, уровень критичности актива, возможность эксплуатации уязвимости в зависимости от сетевых потоков данных (сегменты и т.д.), количество подверженных активов и т.д.

[0058] Функциональность модуля (136) обеспечивает поиск возможных сетевых маршрутов между ЭИ. Упомянутый поиск маршрутов может выполняться по информации из систем, которые являются пограничными узлами сети, отделяющие разные подсети, а именно по информации из правил доступа (ACL), правил трансляции (NAT) и роутинга, определяются возможные взаимодействия сетевых потоков: актив-актив, подсеть-подсеть, актив-подсеть, и т.д.

[0059] Приоритезация обработки и устранения уязвимости осуществляется с помощью модуля (136).

[0060] Приоритезация обработки позволяет для аналитика отсортировать по важности поступающий поток информации о CVE за счет сопоставления атрибутов ЭИ (используемое программное обеспечение, ОС и т.д.) с атрибутами уязвимости.

[0061] Приоритезация устранения уязвимости оценивается с точки зрения критичности ЭИ, критичности уязвимости и рейтинга риска.

[0062] Выполняется также определение применимости уязвимости, что позволяет определить применимость обнаруженной уязвимости на активы ЭИ, по меньшей мере по следующим атрибутам: версия ОС, разрядность ОС, наименование обновления безопасности, наименование программного обеспечения и его версионности, наименование службы и ее версионности, наименование драйвера и его версионности.

[0063] Анализ уязвимостей ЭИ может выполняться с помощью графовых моделей на основании полученных данных по сетевым потокам, вследствие чего появляется возможность моделирования распространения угрозы за счет определения набора уязвимых ЭИ, а также информации по взаимодействию сетевых потоков.

[0064] Работа аналитического модуля (136) позволяет также определить узлы отказа при сетевом взаимодействии и последствие этого отказа (влияние на АС, которые обеспечивают бизнес-процессы внутренней инфраструктуры). В частности, при определении угрозы отказа выявляются ЭИ, в случае выхода из строя которых, связанные с ними узлы инфраструктуры и/или устройства, также будут выведены из строя или потеряют должную функциональность.

[0065] Модуль визуализации (137) обеспечивает графическое представление обрабатываемых данных, в частности, оперативное представление большого массива данных за счет создания «виджетов», механизма фильтрации и группировок, и т.п. Графическое представление может формироваться в виде различного рода информационных панелей, графиков, диаграмм, карт и др. Модуль (137) также обеспечивает формирование отчетов.

[0066] Модуль администрирования (138) обеспечивает управление доступом к системе (130), в частности, обеспечивает:

- Управление информацией о пользователях;
- Управление политиками доступа;
- Выдачу токенов для доступа по API;
- Управление словарями (учет подсетей периметра и принадлежность их к территориальному блоку и FW; Словарь программного обеспечения, который формируется по результатам сбора профилей активов и последующим наложением на поступающую трубу CVE).

[0067] Модуль интеграции (139) обеспечивает передачу в унифицированном формате данных о киберугрозах во внутреннюю инфраструктуру, и обеспечивает связь с внутренними источниками данных (140).

[0068] Далее рассмотрим один из частных примеров работы заявленного решения. На первом шаге осуществляется сбор ЭИ для выполнения процедуры сканирования (инфраструктура периметра, внутренняя инфраструктура). Данные из внутренних источников (140) собираются с помощью их опроса модулем сбора данных (133), например, согласно заданному расписанию сбора информации. Поступившая информация от источников (140) представляет собой входной поток данных для модуля управления данными (134), задачей которого является нормализация данных и формирование профиля атрибутного состава ЭИ в зависимости от его типа.

[0069] Модуль аналитики (136) на основании поступившего потока данных от модуля управления данными (134) задействует модуль интеграции (139) для передачи списка ЭИ, в частности атрибутов ЭИ, например, внутренних сетевых адресов и/или внешних сетевых адресов/подсетей, на сканер безопасности для выполнения задач сканирования.

[0070] После завершения задач сканирования, а также получения данных из внешних (110) и внутренних (140) источников с помощью модуля сбора данных (133), полученный поток данных передается в модуль обогащения профилей (135), который в свою очередь обогащает ранее созданный профиль модулем (134), обнаруженными уязвимостями.

[0071] Механизмы, используемые для обогащения профилей ЭИ, которые имеют отношение к внешнему периметру инфраструктуры, являются частными случаем. А именно, в отличии от обогащения профиля внутреннего ЭИ, дополнительно задействуется модуль аналитики (136), который в свою очередь использует алгоритмы по анализу внешнего периметра инфраструктуры, позволяющие проецировать внешний адрес и порт ЭИ периметра, на адрес и порт внутреннего ЭИ. После получения внутренних ЭИ модуль обогащения (135) дополняет ранее собранный профиль найденными уязвимостями. Результаты, полученные со сканеров безопасности ведутся в учетной части системы и хранятся в объекте учета «Результат сканирования».

[0072] После обогащения профилей ЭИ найденными уязвимостями, модулем аналитики (136) осуществляется расчёт критичности уязвимого АИ за счет определения влияния уязвимостей на сетевую инфраструктуру и ее функционирование.

[0073] Список уязвимых ЭИ прикрепляется к карточке уязвимости, которая содержит описательную часть найденной уязвимости. Дополнительно карточка уязвимости содержит обновления безопасности, которые ее устраняют, если такие имеются, а также обнаруженные эксплоиты в сети Интернет. Далее из карточки уязвимости вручную или автоматически может быть создана сущность типа «Case», которая содержит информацию о найденной уязвимости, масштабах влияния на инфраструктуру (список уязвимых ЭИ). Большинство полей система заполняет автоматически из других сущностей платформы.

[0074] После заполнений всех полей в объекте типа «Case», модулем аналитики (136) осуществляется расчет рейтинга риска. После расчета рейтинга риска, производится его регистрация с учетом автоматического заполнения полей из сущности Case и Vulnerability. Зарегистрированный риск содержит описательную часть, а также мероприятия, которые необходимо выполнить для устранения уязвимостей. Регистрировать риск можно, как внутри платформы, так и в сторонней системе за счет использования модуля интеграций (139).

[0075] После заведения риска модуль аналитики (136) с помощью модуля интеграций (139) обеспечивает управление режимом устранения уязвимостей, при котором выявляются ЭИ для устранения найденных на них уязвимостей, в частности, с помощью списка уязвимых ЭИ, которые передаются во внешнюю систему управления обновлениями.

[0076] После выполнения циклов обновлений, система управления обновлениями возвращает результат, который повторно отправляется в сканер безопасности. По итогу проведенного сканирования формируется результат, свидетельствующий об устранении или наличии риска на том или ином ЭИ.

[0077] На Фиг. 3 представлен пример общего вида вычислительного устройства (200), с помощью которого может быть реализована функциональность системы (130). Устройство (200) может являться частью компьютерной системы, например, сервером, компьютером, облачной платформой и т.п.

[0078] 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), и устройство для сетевого взаимодействия (206).

[0079] 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.

[0080] ОЗУ (202) представляет собой оперативную память и предназначено для хранения исполняемых процессором (201) машиночитаемых инструкций для выполнение 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.).

[0081] 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.

[0082] Для организации работы компонентов устройства (200) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов B/B (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.

[0083] Для обеспечения взаимодействия пользователя с вычислительным устройством (200) применяются различные средства (205) B/B 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.

[0084] 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.

[0085] Дополнительно могут применяться также средства спутниковой навигации в составе устройства (200), например, GPS, ГЛОНАСС, BeiDou, Galileo.

[0086] Представленные материалы заявки раскрывают предпочтительные примеры реализации технического решения 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

1. Система интеллектуального управления рисками и уязвимостями элементов инфраструктуры, содержащая:

- по меньшей мере один процессор;
- по меньшей мере одно запоминающее устройство;
- модуль сбора данных с источников, выполненный с возможностью получения информации из источников данных, содержащих информацию об уязвимостях элементов инфраструктуры (ЭИ), включающие в себя функциональные и логические ЭИ, при этом

  функциональные ЭИ представляют собой активы инфраструктуры (АИ), содержащие оконечное физическое или виртуальное оборудование, предоставляющее услугу и/или сервис, и сетевые ЭИ, представляющие устройства, обеспечивающие сетевое взаимодействие между всеми функциональными ЭИ;

  логические ЭИ представляют собой объединения функциональных ЭИ и логических ЭИ, включающих сущности, взаимодействующие с сетевой инфраструктурой и выбираемые из группы: автоматизированные системы, функциональные подсистемы, или сервисы;
- модуль управления данными, выполненный с возможностью

  нормализации данных, собираемых модулем сбора данных, обеспечивая формирование унифицированного вида данных и формирование атрибутного состава в зависимости от типа ЭИ;

  формирование профиля ЭИ, содержащего атрибутный состав ЭИ;
- модуль обогащения профилей ЭИ, выполненный с возможностью дополнения атрибутного состава профиля ЭИ информацией, включающей в себя:

  информацию о возможности сетевого взаимодействия между АИ, на основании данных правил безопасности (ACL), а также правил трансляции (NAT) и маршрутизации, определенных на сетевых ЭИ;

  найденные уязвимости на АИ;

  данные о критичности функционирования логических ЭИ;

  сведения о выявленных рисках, а также мероприятиях по их устранению;
- модуль аналитики, выполненный с возможностью

  учета, анализа и мониторинга внешнего периметра сетевой инфраструктуры;

  поиска по атрибутному составу профилей ЭИ;

анализа необработанных данных, поступающих из источников данных;

управления рисками по найденным уязвимостям;

поиска и анализа сетевых маршрутов между АИ для определения возможных путей распространения угрозы;

расчёта критичности уязвимого АИ за счет определения влияния уязвимостей на сетевую инфраструктуру и ее функционирование.

2. Система по п.1, характеризующаяся тем, что атрибутный состав ЭИ включает в себя категорию и тип устройств инфраструктуры.

3. Система по п.1, характеризующаяся тем, что информация по обогащению профиля ЭИ инфраструктуры по взаимодействию сетевых потоков получается на основании полученных атрибутов по устройствам инфраструктуры.

4. Система по п.1, характеризующаяся тем, что информация по обогащению профиля актива по найденным уязвимостям на ЭИ формируется на основании полученных результатов работы сканера безопасности.

5. Система по п.1, характеризующаяся тем, что данные для расчета критичности ЭИ или уязвимости получаются из внешних систем.

6. Система по п.1, характеризующаяся тем, что модуль аналитики дополнительно обеспечивает формирование графовых моделей на основании полученных данных по сетевым потокам и информации о связях функциональных ЭИ и логических ЭИ между собой.

7. Система по п.6, характеризующаяся тем, что осуществляется моделирование распространения угрозы за счет определения области уязвимых ЭИ.

8. Система по п.7, характеризующаяся тем, что дополнительно учитывается информация по взаимодействию сетевых потоков.

9. Система по п.6, характеризующаяся тем, что обеспечивается определение узлов отказа при сетевом взаимодействии и последствий наступления такого рода отказа.

10. Система по п.1, характеризующаяся тем, что модуль аналитики дополнительно обеспечивает управление сканированием, при котором формируется список сетевых адресов для передачи их сканеру безопасности.

11. Система по п.1, характеризующаяся тем, что модуль аналитики дополнительно обеспечивает управление режимом устранения уязвимостей, при котором выявляются активы инфраструктуры для устранения найденных на них уязвимостей.

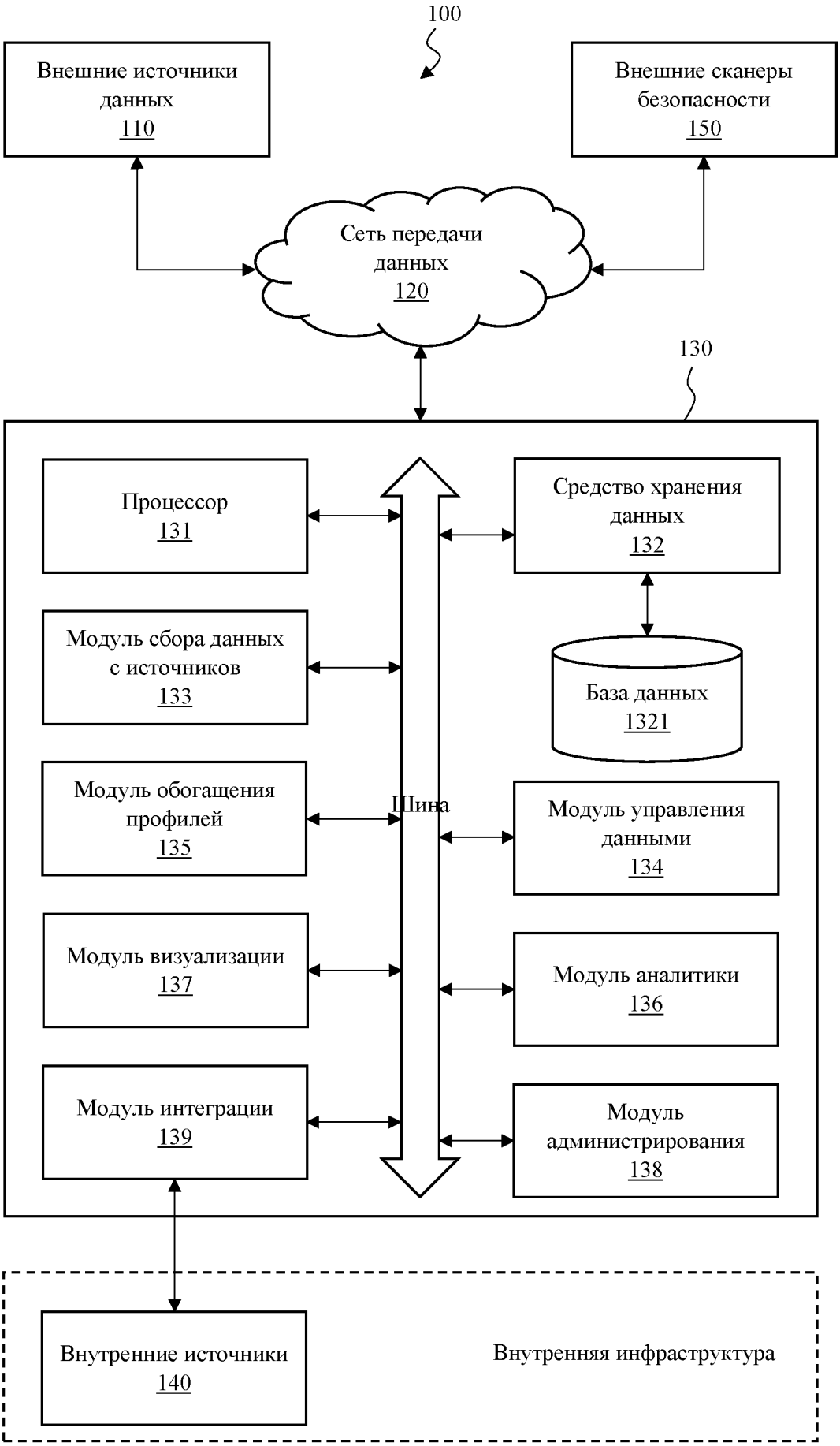
12. Система по п.1, характеризующаяся тем, что дополнительно содержит модуль визуализации, обеспечивающий графическое представление обрабатываемых данных.

13. Система по п.12, характеризующаяся тем, что модуль визуализации обеспечивает формирование виджетов и/или отчетов и/или информационных панелей.

14. Система по п.1, характеризующаяся тем, что дополнительно содержит модуль администрирования, обеспечивающий управление политиками доступа, справочниками, настройками существующих модулей системы.

15. Система по п.1, характеризующаяся тем, что при выявлении модулем обогащения АИ, для которых имеется информация об уязвимостях, осуществляется передача упомянутой информации во внешнюю систему для получения пакетов обновлений для устранения уязвимостей на упомянутых АИ.

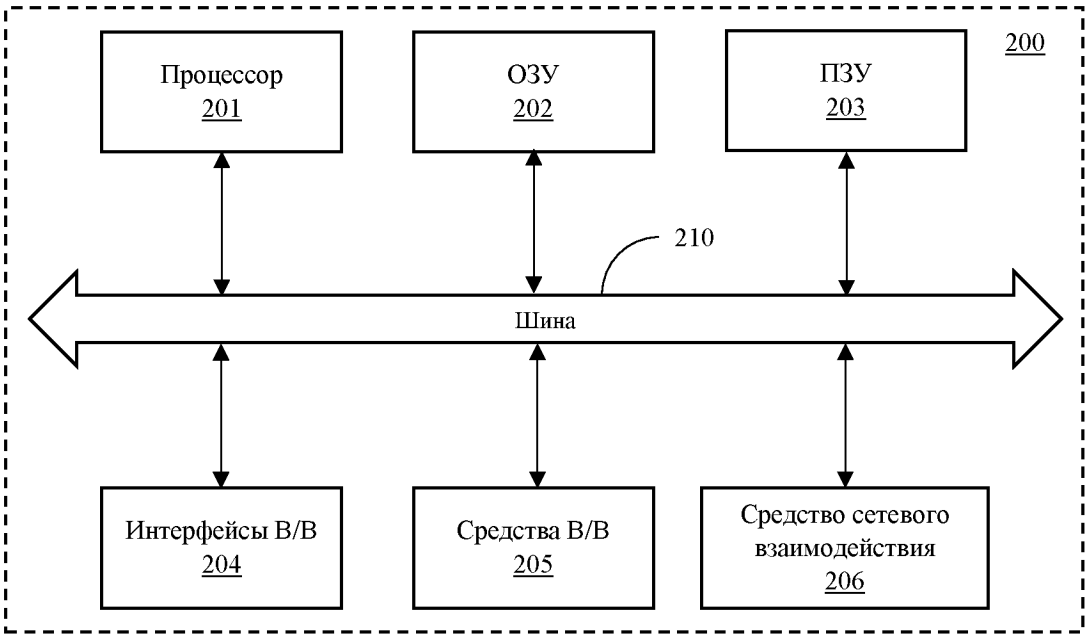
16. Система по п.15, характеризующаяся тем, что процесс выполняется итеративно для всех АИ, для которых происходит обнаружение уязвимостей.


100
Внешние источники данных
110
Внешние сканеры безопасности
150
Сеть передачи данных
120
130
Процессор
131
Средство хранения данных
132
Модуль сбора данных с источников
133
База данных
1321
Модуль обогащения профилей
135
Шина
Модуль управления данными
134
Модуль визуализации
137
Модуль аналитики
136
Модуль интеграции
139
Модуль администрирования
138
Внутренние источники
140
Внутренняя инфраструктура

Фиг. 1

Наименование атрибутов
Внутренний идентификатор ЭИ
Сетевой адрес
Маска подсети
MAC-адрес
Наименование сетевой карты
Описание подсети
Наименование ОС
Архитектура ОС (разрядность)
Сборка/Версия ОС
Наименование BIOS
Версия BIOS
Наименование CPU
Установленные сервисы
Установленные приложения
Установленные обновления безопасности
Список локальных пользователей
Список локальных групп пользователей
Обнаруженные уязвимости

Фиг. 2


200
Процессор
201
ОЗУ
202
ПЗУ
203
210
Шина
Интерфейсы В/В
204
Средства В/В
205
Средство сетевого
взаимодействия
206

Фиг. 3

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ

(статья 15(3) ЕАПК и правило 42 Патентной инструкции к ЕАПК)

Номер евразийской заявки:

202092860

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

G06F 17/00 *(2019.01)*
G06F 21/00 *(2013.01)*

Согласно Международной патентной классификации (МПК)

Б. ОБЛАСТЬ ПОИСКА:

Просмотренная документация (система классификации и индексы МПК)
G06F 15/00-15/173, 17/00-17/30, 21/00, H04L 29/00-29/06, G06N 20/00-20/20

Электронная база данных, использовавшаяся при поиске (название базы и, если, возможно, используемые поисковые термины)
ESP@CENET, K-PION, PAJ, RUPTO, USPTO, WIPO, GOOGLE, ЕАПАТИС

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
A	US2017/0346846 A1, (FINDLAY V.A.), 30.11.2017	1 – 16
A	US2016/0014147 A1, (FAIR ISAAC CORPORATION), 14.01.2016	1 – 16
A	US2019/0342311 A1, (SPLUNK INC.), 07.11.2019	1 – 16
A	WO2016/003756 A1, (NEO PRIME, LLC), 07.01.2016	1 – 16
A	WO2017/100534 A1, (SERVICENOW, INC),15.06.2017	1 – 16
A	US2020/0076839 A1, (FORCEPOINT , LLC),05.03.2020	1 – 16

☐ последующие документы указаны в продолжении

* Особые категории ссылочных документов:
«A» - документ, определяющий общий уровень техники
«D» - документ, приведенный в евразийской заявке
«E» - более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее
«O» - документ, относящийся к устному раскрытию, экспонированию и т.д.
"P" - документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета"

«T» - более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения
«X» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности
«Y» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории
«&» - документ, являющийся патентом-аналогом
«L» - документ, приведенный в других целях

Дата проведения патентного поиска: **05/07/2021**

Уполномоченное лицо:
Начальник отдела механики,
физики и электротехники

_____ В.Ю. Панько