Компания ИнфоТеКС является одним из лидеров высокотехнологичной отрасли информационной безопасности в России. Компания обладает высоким интеллектуальным и творческим потенциалом, что обеспечивает ей многолетний устойчивый рост и ведущее положение на рынке.

Продукты и сервисы ИнфоТеКС являются результатом инвестиций и большого объема проводимых научно-исследовательских и опытно-конструкторских работ. Неотъемлемая часть наших исследований и разработок является своевременное выявление и защита охраноспособных технических решений. Подавая заявки и получая патенты, ИнфоТеКС фиксирует за собой научно-технический приоритет. Патент как подтверждение прав на интеллектуальную собственность, данное уполномоченными государственными и международными органами, позволяет как лицензировать результаты разработок партнерам компании, так и ограничить их использование конкурентами.

Часть изобретений и патентов появляются задолго до создания продукта или сервиса, подтверждая результат перспективных разработок, приоритет и экспертизу ИнфоТеКС в развитии информационных технологий. В иных случаях патенты создаются в процессе разработки конкретного продукта, обеспечивают защиту реализуемых решений к моменту выхода этого продукта на рынок.

Разрабатывая большой объем высокотехнологичной и наукоемкой продукции, мы на регулярной основе реализуем собственную двухфазную процедуру защиты результатов интеллектуальной деятельности путем их патентования. На первой фазе идет оценка и отбор потенциально охраноспособных решений, получаемых в процессе разработки конкретного продукта или инновационных исследований. Для этого организованы отдельные процессы как на этапе планирования работ, так и по их окончании, когда результаты оцениваются с точки зрения их новизны, изобретательского уровня и технической реализуемости.

На второй фазе реализуется защита изобретения. Авторами готовится предварительная патентная заявка. При поддержке специалистов по интеллектуальной собственности проводится патентный анализ и выполнимость формальных критериев, необходимых для успешного получения патента. Сформированная заявка поступает в Экспертный совет по интеллектуальной собственности, функционирующий в ИнфоТеКС на постоянной основе. В случае одобрения заявка подается в национальный орган по патентованию.

Для дополнительной стимуляции процессов изобретательства и патентования в нашей компании регулярно проводятся занятия по основам патентования и консультации с начинающими авторами, а также практикуется поощрение изобретателей. Объективным и независимым свидетельством большого научно-технического потенциала ИнфоТеКС является выбор наиболее интересных и значимых изобретений Роспатентом.

Так, изобретение по патенту РФ № 2577200 «Способ синхронизации доступа к разделяемым ресурсам вычислительной системы под управлением POSIX-совместимой ОС и обнаружения и устранения повисших блокировок с использованием блокировочных файлов» (автор – Мардугаллямов Р.Т.) вошло в базу данных «100 лучших изобретений России» за 2016 год.

Изобретение по патенту РФ № 2630415 «Способ обнаружения аномальной работы сетевого сервера (варианты)» (авторы – Елисеев В.Л., Шабалин Ю.Д.) вошло в базу данных «100 лучших изобретений России» за 2017 год. Это же изобретение по патенту РФ № 2630415, а также изобретение по патенту РФ № 2636403 «Способ выбора маршрутов, получаемых по протоколу DHCP, в сети с коммутацией пакетов» (авторы – Вороков Е.Л., Щеглов А.В.) вошли в базу данных «Перспективные изобретения» за 2017 год.

Изобретение по патенту РФ № 2667805 «Способ работы межсетевого экрана» (автор – Оладько А.Ю.) вошло в базу данных «Перспективные изобретения» за 2018 год.

Технологический бизнес, особенно в области информационной безопасности, глобален по своей сути. Поэтому ИнфоТеКС не ограничивается патентной защитой только на территории России. Для обеспечения своих интересов на внешних рынках мы активно проводим патентование изобретений в странах Европы, Азии, Северной и Южной Америки.

Реализуемые меры отбора и стимуляции изобретений обеспечивают устойчивый рост патентной базы ИнфоТеКС. Общее количество полученных компанией патентов неуклонно увеличивается. На сегодняшний день компания обладает весьма обширным портфолио патентов, представляющим самостоятельную бизнес-ценность. Патентами защищены все ключевые продукты и инновационные разработки ИнфоТеКС.

Данным знаком далее в каталоге помечены вышеперечисленные патенты

ИЗОБРЕТЕНИЯ

Защита в цифровых сетях передачи данных

Информационная безопасность в цифровых сетях передачи данных

Криптография и шифрование

Параллельная обработка данных

Технологии блокчейн

Квантовые технологии

Генераторы случайных чисел

Прикладные технологии

Повышение надежности и производительности компьютерных систем

Интернет вещей (Internet of Things, IoT)

ПРОМЫШЛЕННЫЕ ОБРАЗЦЫ

ПОЛЕЗНЫЕ МОДЕЛИ

ИЗОБРЕТЕНИЯ

Защита в цифровых сетях передачи данных

Зарубежные патенты

Патент США № 9055108

Method for increasing performance in encapsulation of TCP/IP packets into HTTP in network communication system

Автор:
Тычина Л.А.

Заявка США
№ 13/938809
от 10.07.2013 г.

The disclosure relates to methods of transmitting data over TCP/IP through HTTP. The method includes establishing a connection between a client and a server through at least two proxies; generating a tunnel message in the client; sending the tunnel message to the server; choosing a delay value T based on a maximum transmission rate of the tunnel message; and determining a size Q of a dummy data packet by .times..times. ##EQU00001## where MSS.sub.i is a maximum segment size in TCP connections between the i-th proxy and the (i+1)-th proxy, and N is the number of proxies. The method also includes sending, from the client, a dummy data packet of size Q in T seconds after the last transmission of non-dummy data via the HTTP tunnel; receiving the tunnel message by the server; and disabling usage of Nagle's algorithm and TCP delayed acknowledgement algorithm for the TCP connection in the client and server.


The United States of America

The Director of the United States Patent and Trademark Office

Has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.

Therefore, this

United States Patent

Grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America, and if the invention is a process, of the right to exclude others from using, offering for sale or selling throughout the United States of America, or importing into the United States of America, products made by that process, for the term set forth in 35 U.S.C. 154(a)(2) or (c)(1), subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b). See the Maintenance Fee Notice on the inside of the cover.

Michelle K. Lee

Deputy Director of the United States Patent and Trademark Office

Патент США № 8910267

Method for managing connections in firewalls

Автор:
Иванов А.В.

Заявка США
№ 13/938578
от 10.07.2013 г.

The disclosure relates to a method for managing connections in a firewall. The method includes receiving packets from an external network; generating a connection table; determining the total number of currently established connections; determining a level of firewall load by comparing the number of established connections with a threshold; identifying new and established connections based on two-way exchange of packets between a client and server; identifying closed connections based on processing ICMP error messages or flags in a TCP header; and dynamically determining current timeout values for connections from the network protocol type, the connection state, and the firewall load level. The method also includes modifying the last packet processing timestamp if any packet is passed within a given connection or a group of connections; and removing the connection if the last packet processing timestamp differs from the current time by a value greater than the timeout of said connection.

The United States of America

The Director of the United States Patent and Trademark Office

Has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.

Therefore, this

United States Patent

Grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America, and if the invention is a process, of the right to exclude others from using, offering for sale or selling throughout the United States of America, or importing into the United States of America, products made by that process, for the term set forth in 35 U.S.C. 154(a)(2) or (c)(1), subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b). See the Maintenance Fee Notice on the inside of the cover.

Michelle K. Lee

Deputy Director of the United States Patent and Trademark Office

Патент Мексики № 346629

Metodo para evitar la reutilization de paquetes da datos digitales en un sistema de transmision de datos en red

Автор:
Тычина Л.А.

Заявка Мексики
№ MX/A/2015/
011047
от 25.08.2015 г.

A method for preventing repeated use of digital packet data in a network system of data transmission, which method can be realized with the aid of a system comprising computers which are connected via a data transmission network and which send and receive messages in the form of a sequence of digital packet data, in which method useful data and meta data are formed for each packet which can be sent, and also data for checking the integrity of the meta data are formed, wherein the meta data comprise a serial number of the packet, and the time of sending the packet data; the packet is sent via the data transmission network; a permissible value of an error time interval is established; in a memory, fields for storing the time of sending the latest received packet, the serial number of the latest received packet, and a list of the serial numbers of packets received earlier are formed; a packet comprising useful data and meta data is received, a check is carried out for repetition of a received packet, checking whether the time of sending the received packet goes beyond the limits of the error time interval and whether the number of the received packet corresponds to the number of the latest received packet or with numbers in the list of serial numbers of packets received earlier; and packets are accepted or declined on the basis of the results of the check.

Instituto Mexicano de la Propiedad Industrial

TÍTULO DE PATENTE NO. 346629

P15/1201F

Titular(es): JOINT STOCK COMPANY "INFOTECS"

Domicilio: Building 1, 1/23 Stariy Petrovsko-Razumovskiy Proezd, 127287, Moscow, FEDERACIÓN DE RUSIA

Denominación: MÉTODO PARA EVITAR LA REUTILIZACIÓN DE PAQUETES DE DATOS DIGITALES EN UN SISTEMA DE TRANSMISIÓN DE DATOS EN RED.

Clasificación: Int.Cl.®: H04L12/64; H04L12/823; H04L29/06; H04L29/08; H04L9/32

Inventor(es): LEONID ANATOLIEVICH TYCHINA

SOLICITUD

Número: MX/a/2015/011047

Fecha de presentación internacional: 14 de Noviembre de 2013

PRIORIDAD

País:	Fecha:	Número:
RU	26 de febrero de 2013	2013108211

Vigencia: Veinte años

Fecha de Vencimiento: 14 de noviembre de 2033

Fecha de expedición: 24 de marzo de 2017

LA DIRECTORA DIVISIONAL DE PATENTES

NAHANNY CANAL REYES

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2694336

Способ аутентифицированного шифрования

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

Авторы: *Бабуева Александра Алексеевна (RU), Ефимов Дмитрий Владимирович (RU), Науменко Антон Павлович (RU), Калистру Илья Иванович (RU)*

Заявка № 2018117029
Приоритет изобретения 08 мая 2018 г.
Дата государственной регистрации в Государственном реестре изобретений Российской Федерации 11 июля 2019 г.
Срок действия исключительного права на изобретение истекает 08 мая 2038 г.

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Общий пример Патента РФ

Патент РФ № 2517411

Способ управления соединениями в межсетевом экране

Автор:
Иванов А.В.

Заявка РФ
№ 2012145170
от 24.10.2012 г.

Изобретение относится к вычислительной технике. Технический результат заключается в повышении надежности работы установленных соединений и обеспечении максимальной пропускной способности при повышении нагрузки. Такой результат достигается тем, что получают пакеты из внешней сети, формируют таблицу соединений, определяют общее количество установленных соединений на данный момент времени, определяют уровень загрузки межсетевого экрана, сравнивая количество установленных соединений с пороговой величиной, определяют новые и установленные соединения на основе двустороннего обмена пакетами между клиентом и сервером, определяют закрытые соединения на основании обработки ICMP-сообщений об ошибках или флагов в TCP-заголовке, динамически определяют текущие значения таймаутов для соединений на основании типа сетевого протокола, состояния соединения, уровня загрузки межсетевого экрана, изменяют отметку времени обработки последнего пакета в случае прохождения любого пакета в рамках данного соединения или в рамках группы соединений, удаляют соединение, если отметка времени обработки последнего пакета отличается от текущего времени больше, чем таймаут данного соединения.

Патент РФ № 2530663

Способ передачи данных в цифровых сетях передачи данных по протоколу TCP/IP через HTTP

Автор:
Тычина Л.А.

Заявка РФ
№ 2012148627
от 16.11.2012 г.

Изобретение относится к области передачи данных в цифровых сетях передачи данных по протоколу TCP/IP через HTTP. Техническим результатом является повышение скорости передачи данных между клиентом и сервером. Способ передачи данных в цифровых сетях передачи данных по протоколу TCP/IP через HTTP реализуется с помощью системы, включающей сетевые модули, встроенные в компьютер-клиент и компьютер-сервер и обеспечивающие формирование соединения между компьютером-клиентом и компьютером-сервером; прием и передачу сетевых пакетов в соединении между клиентом и сервером; шифрование сетевых пакетов для установленного соединения: туннелирование сетевых пакетов; причем между клиентом и сервером имеется, по крайней мере, два прокси-сервера, связанных с клиентом и сервером, способ заключается в том, что формируют с помощью сетевых модулей соединение между клиентом и сервером, причем соединение устанавливается, по крайней мере, через два прокси-сервера; создают туннельное сообщение в сетевом модуле клиента; передают туннельное сообщение серверу; подбирают величину задержки T по признаку максимальной скорости передачи туннельного сообщения между клиентом и сервером, выполняя следующие действия: устанавливают интервал изменения времени T и шаг по времени; выполняют измерение скорости передачи туннельного сообщения для каждого значения T в интервале; выбирают значение T, соответствующее максимальной скорости передачи; определяют объем пакета с фиктивными данными Q; отправляют из клиента пакет с фиктивными данными объемом Q через T секунд с момента последней передачи нефиктивных данных через HTTP-туннель, принимают на сервере туннельное сообщение; отключают алгоритм Нэйгла для TCP-соединения в сетевых модулях клиента и сервера; отключают алгоритм TCP delayed acknowledgment в сетевых модулях клиента и сервера.

Патент РФ № 2535172

Способ предотвращения повторного использования пакетов цифровых данных в сетевой системе передачи данных

Автор:
Тычина Л.А.

Заявка РФ
№ 2013108211
от 26.02.2013 г.

Изобретение относится к вычислительной технике. Технический результат заключается в предотвращении повторного приема пакетов в установленном промежутке времени рассогласования. Способ предотвращения повторного использования пакетов цифровых данных в сетевой системе передачи данных, в котором формируют полезные данные и метаданные для каждого отправляемого пакета; формируют пакет, включающий полезные данные, метаданные и данные для проверки целостности метаданных; отправляют пакет через сеть передачи данных; устанавливают допустимую величину промежутка времени рассогласования; принимают пакет; проверяют целостность метаданных принятого пакета, используя данные для проверки целостности метаданных; проводят проверку на повтор принятого пакета, выполняя следующие действия: если время отправки принятого пакета выходит за пределы промежутка времени рассогласования, то отклоняют пакет; если время отправки пакета находится в пределах промежутка времени рассогласования, то сравнивают время отправки принятого пакета с временем отправки последнего принятого пакета; если время отправки принятого пакета больше времени отправки последнего принятого пакета, то заменяют время отправки последнего принятого пакета на время отправки принятого пакета; заменяют номер последнего принятого пакета на номер принятого пакета; заносят номер принятого пакета в список порядковых номеров ранее принятых пакетов и принимают пакет.

Патент РФ № 2565488

Способ разрешения конфликта адресации узлов в асинхронных сетях с топологией «общая шина»

Автор:
Рябиков А.Н.

Заявка РФ
№ 2014146703
от 21.11.2014 г.

Изобретение относится к способам разрешения конфликта адресации узлов в асинхронных сетях. Технический результат, заключающийся в повышения надежности обнаружения и разрешения конфликта адресации узлов, достигается за счет выполняемых в сетевой системе операций, включающих этапы на которых ведущее устройство, подключенное к сети, инициирует обмен данными и формирует запросы; передает запросы по сети ведомым устройствам. Ведомые устройства принимают ответы из сети, каждое из которых подключено к сети, имеет собственный сетевой адрес и выполнено с возможностью принимать запросы ведущего устройства через сеть. Посылают из ведущего устройства в адрес выбранного ведомого устройства 1-й запрос, без задержки отправляют ответ из ведомых устройств. Посылают из ведущего устройства в адрес выбранного ведомого устройства 2-й запрос, содержащий команду, обеспечивающую случайную задержку ответа. Посылают из ведущего устройства в адрес выбранного ведомого устройства 3-й запрос выбранному ведомому устройству на изменение сетевого адреса. В случае обнаружения в сети ответа на 3-й запрос от другого ведомого устройства ведомое устройство не изменяет свой сетевой адрес, иначе ведомое устройство изменяет свой сетевой адрес и высылает ответ на 3-й запрос ведущему устройству.

Патент РФ № 2604328

Способ формирования защищенного соединения в сетевой компьютерной системе

Автор:
Тычина Л.А.

Заявка РФ
№ 2015126544
от 03.07.2015 г.

Изобретение относится к способам обеспечения безопасности в сетях передачи данных. Технический результат заключается в повышении защищенности соединения между компьютерами-клиентами. Указанный результат достигается за счет применения способа формирования защищенного соединения в сетевой компьютерной системе. Система включает прикладной сервер, осуществляющий прием и обработку запросов по прикладному протоколу от компьютеров-клиентов по сети через туннелирующий сервер. Компьютеры-клиенты выполнены с возможностью осуществлять взаимодействие между собой и с прикладным сервером по прикладному протоколу. Посылают запрос из первого компьютера-клиента в прикладной сервер для осуществления взаимодействия со вторым компьютером-клиентом; анализируют в туннелирующем сервере ответ из прикладного сервера первому компьютеру-клиенту; если в ответе присутствует сетевой адрес второго компьютера-клиента, то передают из туннелирующего сервера первому компьютеру-клиенту вместе с сообщением прикладного протокола информацию, необходимую для установки защищенного соединения со вторым компьютером-клиентом; формируют защищенное соединение между первым компьютером-клиентом и вторым компьютером-клиентом.

Патент РФ № 2636403

Способ выбора маршрутов, получаемых по протоколу DHCP, в сети с коммутацией пакетов

Авторы:
Вороков Е.Л.,
Щеглов А.В.

Заявка РФ
№ 2016124471
от 21.06.2016 г.

Изобретение относится к технологиям сетевой связи. Технический результат заключается в повышении скорости передачи данных в сети. В способе запрашивают и получают сетевые адреса и сетевые маршруты от удаленных DHCP-серверов по протоколу DHCP; обрабатывают полученные таблицы маршрутов в средстве первичной обработки протокола DHCP, назначают каждому маршруту первичную метрику; записывают маршруты в первичную таблицу маршрутов; выявляют маршруты с одинаковым адресом клиентской сети; для каждого существующего в первичной таблице маршрутов адреса клиентской сети выбирают наилучший маршрут в данную клиентскую сеть с учетом первичных метрик; передают наилучшие маршруты для каждой клиентской сети в средство выбора наилучших маршрутов; обрабатывают наилучшие маршруты, полученные от средств первичной обработки протоколов динамической маршрутизации, включая DHCP, в средстве выбора наилучших маршрутов, сопоставляют вторичную метрику для каждого из используемых протоколов динамической маршрутизации, включая DHCP; сопоставляют вторичные метрики маршрутов, исходя из протокола, с помощью которого маршрут был передан в средство выбора наилучших маршрутов.

Патент РФ № 2635216

Способ маршрутизации IP-пакетов при использовании VPLS совместно с DHCP в сети с коммутацией пакетов

Авторы:
Вороков Е.Л.,
Щеглов А.В.

Заявка РФ
№ 2016142692
от 31.10.2016 г.

Изобретение относится к области цифровых сетей передачи данных с коммутацией пакетов (IP). Техническим результатом является упрощение настройки маршрутизации, снижение нагрузки на сервис DPLS и в целом на сеть, устранение ограничений на расположение и реализацию DHCP-сервера. Способ маршрутизации IP-пакетов при использовании VPLS совместно с DHCP в сети с коммутацией пакетов, причем в состав сети входят клиентские компьютеры, расположенные в клиентских сетях; пограничные маршрутизаторы, причем каждая клиентская сеть подключена к своему пограничному маршрутизатору через заданный интерфейс, образующий шлюз по умолчанию; DHCP-сервер, находящийся в одной из клиентских сетей; при этом каждый пограничный маршрутизатор содержит средство обработки, выполненное с возможностью: сравнения IP-адресов, содержащихся в кадрах запроса; модификации кадра запроса путем добавления или удаления данных; замены IP-адресов, содержащихся в кадрах запроса; способ заключается в том, что передают запрос из клиентского компьютера на получение IP-адреса интерфейса и IP-адреса шлюза по умолчанию в пограничный маршрутизатор своей клиентской сети, причем запрос содержит набор кадров; опции протокола DHCP; передают запрос из пограничного маршрутизатора клиентской сети, содержащей клиентский компьютер, в пограничный маршрутизатор, находящийся в клиентской сети DHCP-сервера; передают запрос из пограничного маршрутизатора, находящегося в клиентской сети DHCP-сервера, в DHCP-сервер; формируют ответ в DHCP-сервере в виде совокупности кадров; передают ответ DHCP-сервера в пограничный маршрутизатор, находящийся в клиентской сети DHCP-сервера; обрабатывают полученный ответ DHCP-сервера в средстве обработки пограничного маршрутизатора, выполняя следующие действия: проверяют, содержат ли сведения, имеющиеся в кадрах, какой-либо маршрут, имеющий в качестве IP-адреса шлюза по умолчанию IP-адрес шлюза по умолчанию данного пограничного маршрутизатора; если был обнаружен факт совпадения, то модифицируют ответ путем добавления отметки в кадр; передают ответ DHCP-сервера из пограничного маршрутизатора, находящегося в клиентской сети

DHCP-сервера, в пограничный маршрутизатор клиентской сети, в которой находится клиентский компьютер, пославший запрос; обрабатывают ответ DHCP-сервера в средстве обработки пограничного маршрутизатора клиентской сети, из которой поступил запрос, выполняя следующие действия: проверяют, содержат ли сведения, имеющиеся в кадрах, отметку; если отметка присутствует, то выполняют следующие действия: в каждом случае, когда в сведениях, имеющихся в кадрах, указан маршрут, заменяют IP-адрес шлюза по умолчанию пограничного маршрутизатора клиентской сети, в которой находится DHCP-сервер, на IP-адрес шлюза по умолчанию пограничного маршрутизатора клиентской сети, из которой поступил запрос; удаляют из ответа DHCP-сервера отметку; передают ответ DHCP-сервера из пограничного маршрутизатора клиентской сети, из которой поступил запрос, в клиентский компьютер, пославший запрос; принимают ответ DHCP-сервера.

Патент РФ № 2635215

Способ подключения компьютера пользователя к виртуальной частной сети через локальную сеть провайдера

Автор:
Милич Н.В.

Заявка РФ
№ 2016151332
от 27.12.2016 г.

Изобретение относится к способам обеспечения безопасности в сетях передачи данных и, в частности, к способам организации защищенного канала взаимодействия с сервером. Техническим результатом является повышение безопасности компьютера пользователя. Раскрыт способ подключения компьютера пользователя к виртуальной частной сети через локальную сеть провайдера, причем локальная сеть провайдера имеет соединение с локальной сетью организации, в которой развернуты узлы VPN, через глобальную сеть; причем локальная сеть провайдера включает портал, обеспечивающий соединение между локальной сетью провайдера и глобальной сетью и выполненный с возможностью обеспечивать авторизацию компьютера пользователя; по крайней мере, одно сетевое устройство, подключенное к локальной сети провайдера; по крайней мере, один компьютер пользователя, подключенный к сетевому устройству; причем сетевое устройство имеет процессор и выполнено с возможностью безопасного подключения к компьютеру пользователя; принимать запрос на подключение к VPN-сети организации от компьютера пользователя; передавать в портал запрос на авторизацию от компьютера пользователя; принимать из портала данные для страницы авторизации; формировать изображение страницы авторизации для компьютера пользователя; передавать в компьютер пользователя изображение страницы авторизации; принимать из компьютера пользователя данные для авторизации; передавать данные для авторизации в портал; способ заключается в том, что передают запрос на подключение к VPN-сети организации из компьютера пользователя в сетевое устройство; принимают запрос на подключение к VPN-сети организации в сетевом устройстве; передают запрос на авторизацию компьютера пользователя из сетевого устройства в портал; принимают в сетевом устройстве данные для страницы авторизации из портала; передают из сетевого устройства в компьютер пользователя изображение страницы авторизации; принимают на компьютере пользователя управляющее воздействие от пользователя; передают из компьютера пользователя данные об управляющем воздействии пользователя в сетевое устройство; при помощи полученных данных об управляющем воздействии формируют данные для авторизации в сетевом устройстве; передают из сетевого устройства данные для авторизации в портал; авторизуют компьютер пользователя с помощью портала в локальной сети провайдера; передают сведения об успешной авторизации из портала через сетевое устройство в компьютер пользователя; устанавливают подключение через сетевое устройство и портал между компьютером пользователя и узлом VPN-сети организации.

Патент РФ № 2648949

Способ защиты вычислительной сети от несанкционированного сканирования и блокирования сетевых служб

Автор:
Оладько А.Ю.

Заявка РФ
№ 2017107811
от 10.03.2017 г.

Изобретение относится к способу защиты вычислительной сети от несанкционированной передачи информации, сканирования и блокирования сетевых служб. Техническим результатом является повышение защищенности вычислительной сети. Способ защиты вычислительной сети от несанкционированной передачи информации, сканирования и блокирования сетевых служб, причем на входе защищаемой сети установлен шлюз-компьютер с межсетевым экраном, в котором определено множество A разрешенных для использования протоколов прикладного уровня и который содержит средство контроля, выполненное с возможностью проводить определение используемого в сетевом соединении протокола прикладного уровня, содержит этапы: принимают от отправителя с адресом S1 для получателя с адресом R1 сетевой пакет P1, имеющий номер инкапсулированного протокола транспортного уровня, соответствующего номеру протокола TCP, и установленный флаг SYN; блокируют передачу сетевого пакета P1 получателю с адресом R1; посылают с помощью межсетевого экрана отправителю с адресом S1 сетевой пакет P2, сформированный в соответствии с протоколом TCP, с установленными флагами SYN и ACK и имеющий адрес отправителя R1; получают от отправителя с адресом S1 сетевой пакет P3 с номером инкапсулированного протокола транспортного уровня, соответствующим номеру протокола TCP и установленным флагом ACK, обозначающего завершение процедуры установления TCP-сессии; получают от отправителя с адресом S1 сетевой пакет P4, в котором содержатся данные D; определяют с помощью средства контроля факт использования в составе данных D протокола прикладного уровня из множества A; если факт использования установлен, то посылают из межсетевого экрана получателю с адресом R1 сетевой пакет P5, сформированный в соответствии протоколом TCP, с установленным флагом SYN и имеющий адрес отправителя S1; получают от отправителя с адресом R1 сетевой пакет P6 с номером инкапсулированного протокола транспортного уровня, соответствующего номеру протокола TCP, и установленными флагами SYN и ACK; посылают из межсетевого экрана получателю с адресом R1 сетевой пакет P7, сформированный в соответствии с протоколом TCP, с установленным флагом ACK, обозначающего завершение процедуры установления TCP-сессии, и имеющий адрес отправителя S1; посылают из межсетевого экрана получателю с адресом R1 сетевой пакет P8, сформированный в соответствии с протоколом TCP, имеющий адрес отправителя S1 и содержащий данные D в неизменном виде; осуществляют с помощью межсетевого экрана прозрачную ретрансляцию пакетов между отправителем с адресом S1 и получателем с адресом R1; иначе сбрасывают соединение между отправителем с адресом S1 и получателем с адресом R1.

Патент РФ № 2665247

Способ доставки сертификатов в защищенной сетевой вычислительной системе

Автор:
Ерыгин А.В.

Заявк РФ
№ 2017137602
от 27.10.2017 г.

Изобретение относится к технологиям сетевой связи. Технический результат заключается в повышении безопасности передачи данных. Способ доставки сертификатов в защищенной сетевой вычислительной системе, которая содержит сервер распространения, причем сервер включает установленное на нем средство распространения, выполненное с возможностью: хранить сертификаты; принимать запросы от компьютеров пользователей на загрузку сертификатов; передавать сертификаты в ответ на запросы от компьютеров пользователей; а также компьютеры пользователей, причем каждый компьютер включает средство установки сертификатов, выполненное с возможностью перехватывать запросы на загрузку сертификатов от компьютера пользователей к внешним по отношению к вычислительной системе удостоверяющим центрам; перенаправлять запросы на загрузку сертификатов от компьютера пользователя к средству распространения; принимать сертификаты; устанавливать сертификаты на компьютер пользователя.

Патент РФ № 2667805

Способ работы межсетевого экрана

Автор:
Оладько А.Ю.

Заявка РФ
№ 2017143804
от 14.12.2017 г.

Изобретение относится к способу работы межсетевого экрана. Техническим результатом является повышение защищенности вычислительной сети. Принимают от отправителя с адресом для получателя с адресом сетевой пакет. Если сетевой пакет имеет номер инкапсулированного протокола транспортного уровня, соответствующий номеру протокола UDP, и содержит данные, то выполняют следующие действия: выполняют пакетную фильтрацию для сетевого пакета; определяют с помощью модуля контроля факт использования в составе данных протокола прикладного уровня из множества. Если факт использования установлен, то выполняют следующие действия: заменяют в сетевом пакете адрес получателя на адрес прокси-модуля в модуле сетевой трансляции адресов; выполняют фильтрацию сетевого потока в прокси-модуле; обрабатывают данные в прокси-модуле.

Патент РФ № 2679227

Способ работы межсетевого экрана

Автор:
Оладько А.Ю.

Заявка РФ
№ 2018112218
от 05.04.2018 г.

Изобретение относится к области вычислительной техники. Технический результат заключается в повышении защищенности сети в защищаемом сегменте. Способ содержит этапы, на которых: принимают от отправителя с адресом S1 для получателя с адресом R1 сетевой пакет P1; осуществляют поиск с помощью модуля обработки таблицы сетевых соединений дескриптора сетевого соединения, к которому относится сетевой пакет P1, на основе адреса отправителя S1, адреса получателя R1, номера инкапсулированного протокола транспортного уровня, информации о протоколе транспортного уровня; если дескриптор сетевого соединения не найден, то создают и сохраняют в таблице сетевых соединений дескриптор сетевого соединения с помощью модуля обработки таблицы сетевых соединений; производят анализ сетевого пакета в модуле классификации сетевых пакетов; сохраняют в дескрипторе сетевого соединения информацию, полученную в результате анализа сетевого пакета из модуля классификации сетевых пакетов; выполняют фильтрацию сетевого пакета.

Патент РФ № 2684495

Способ предотвращения повторного использования пакетов цифровых данных в сетевой системе передачи данных

Авторы:
Паршин И.А.,
Тычина Л.А.

Заявка РФ
№ 2018113078
от 11.04.2018 г.

Изобретение относится к обеспечению безопасности в сетях передачи данных. Технический результат – предотвращение повторного приема пакетов цифровых данных в сетевой системе передачи данных. Способ предотвращения повторного использования пакетов цифровых данных в сетевой системе передачи данных, в котором получают в выбранном шлюзе полезные данные для каждого отправляемого пакета, формируют метаданные для каждого отправляемого пакета, причем метаданные включают номер пакета, время отправки пакета данных, данные для проверки целостности метаданных, отправляют пакет из выбранного шлюза через сеть передачи данных, устанавливают на компьютере, принимающем сообщения, допустимую величину промежутка времени рассогласования, формируют в памяти компьютера, принимающего сообщения, области для хранения времени отправки и номера последнего принятого пакета, списка номеров ранее принятых пакетов данных от каждого отправителя, принимают пакет, включающий полезные данные и метаданные, проверяют целостность метаданных принятого пакета, используя данные для проверки целостности метаданных, проводят проверку на повтор принятого пакета, принимают пакет, включающий полезные данные и метаданные, проверяют целостность метаданных принятого пакета, используя данные для проверки целостности метаданных, проводят проверку на повтор принятого пакета, при этом если время отправки принятого пакета выходит за пределы промежутка времени рассогласования, то отклоняют пакет, если время отправки пакета находится в пределах промежутка времени рассогласования, то принимают пакет.

Патент РФ № 2687217

Способ предотвращения фрагментации TCP/IP-пакетов при использовании VPLS в сети с коммутацией пакетов

Авторы:
Вороков Е.Л.,
Щеглов А.В.

Заявка РФ
№ 2018122435
от 20.06.2018 г.

Изобретение относится к цифровым сетям передачи данных с коммутацией пакетов (IP). Технический результат – повышение пропускной способности в сети с коммутацией пакетов. В состав сети входят клиентские сети (КС), каждая из которых содержит клиентские компьютеры (КК) и пограничный маршрутизатор (ПМ); внешнюю сеть, соединяющую все ПМ по технологии VPLS, причем каждый ПМ имеет внешний интерфейс, связанный с внешней сетью и имеющий установленное значение максимального размера полезного блока данных одного пакета, который может быть передан протоколом без фрагментации (MTU); имеет внутренний интерфейс, связанный со своей КС и имеющий установленное значение MTU; содержит средство обработки, выполненное с возможностью: сравнения IP-адресов, содержащихся в кадрах запроса; модификации кадра запроса путем изменения данных. В результате использования данного способа устанавливается TCP-соединение со значением максимального размера MSS, позволяющим осуществлять передачу пакетов без фрагментации, при этом минимизируются задержки при обработке пакетов и уменьшается нагрузка на сервис VPLS, полностью используется доступный канал передачи, а при автоматическом расчете значения максимального размера MSS не требуется дополнительных настроек.

Патент РФ № 2695983

Способ фильтрации защищенных сетевых соединений в цифровой сети передачи данных

Автор:
Минко В.С.

Заявка РФ
№ 2018126029
от 16.07.2018 г.

Изобретение относится к технике фильтрации защищенных сетевых соединений. Технический результат – расширение контроля сетевых соединений и повышение защищенности контролируемой сети передачи данных. Данный способ определяет запрещенный для использования сетевой протокол прикладного уровня (F), а также обеспечивает взаимодействие по протоколу (F); установление соединений по протоколам E; по протоколу (T) транспортного уровня; определение факта использования протокола (E) в сетевом соединении; установление соединения транспортного уровня T1 с компьютером с адресом R; прием от клиента C для получателя с адресом R пакета P, который пересылается через установленное соединение T1 и содержит данные D; определение факта наличия в составе данных D запроса на установку защищенного соединения E1; если факт наличия запроса не установлен, то пропускают пакет P; если факт наличия запроса установлен, то устанавливают транспортное соединение T2 с адресом назначения R; запрашивают через T2 установку защищенного соединения E2; если соединение E2 установить не удалось, то пропускают пакет P; если соединение E2 установлено, то осуществляют взаимодействие по протоколу (F) с компьютером по адресу R; если взаимодействие по протоколу (F) оказывается успешным, то блокируют пакет P.

Патент РФ № 2694585

Способ создания защищенного L2-соединения между сетями с коммутацией пакетов

Авторы:
Гузев О.Ю.,
Чижов И.В.

Заявка РФ
№ 2018135893
от 11.10.2018 г.

Изобретение относится к области вычислительной техники. Технический результат заключается в обеспечении возможности создания кластера криптомаршрутизаторов без ограничений на их количество. Способ содержит этапы, на которых: формируют ключевую информацию для всех криптомаршрутизаторов; выделяют в каждой сети диапазоны IP-адресов для установленных устройств, а также диапазоны туннелируемых криптомаршрутизаторами IP-адресов; загружают на криптомаршрутизаторы ключевую информацию; настраивают на крипто-маршрутизаторах IP-адреса; настраивают на криптомаршрутизаторах выделенные диапазоны туннелируемых IP-адресов; создают на каждом коммутаторе два виртуальных порта: порт для инкапсуляции/декапсуляции сетевых пакетов в заголовки протокола туннелирования; порт уровня L3, служащий конечным IP-интерфейсом туннеля; настраивают на сетевых интерфейсах всех коммутаторов IP-адреса; настраивают на коммутаторах IP-адрес контроллера; создают на контроллере конфигурационный файл, содержащий значения следующих констант: таймаут неактивности правил в таблицах потоков, интервал запроса статистики, длительность одной итерации сбора статистики.

Патент РФ № 2694584

Способ обработки TCP-протокола в кластере сетевой вычислительной системы

Автор:
Тычина Л.А.

Заявка РФ
№ 2018137584
от 25.10.2018 г.

Изобретение относится к способу обработки пакетов TCP-протокола, проходящих через кластер шлюзов безопасности сетевой вычислительной системы. Техническим результатом является повышение защиты кластера от DoS-атак. Формируют в оперативной памяти каждого шлюза таблицу для хранения трех ключей и относящихся к каждому ключу атрибутов. Формируют в шлюзе безопасности имеющий наименьший номер случайный ключ. Вычисляют для сформированного ключа порядковый номер, начиная с нуля, признаки четности порядкового номера и время создания ключа. Рассылают ключ и связанные с ним атрибуты во все остальные шлюзы безопасности. Сохраняют во всех шлюзах безопасности ключ и связанные с ним атрибуты в таблицу. Устанавливают период смены ключа в кластере. Посылают сетевой пакет, содержащий TCP-сообщение SYN для установки соединения (запрос), из клиента на сервер.

Патент РФ № 2718217

Способ обеспечения передачи зашифрованных данных со сменой ключей шифрования и имитозащиты в цифровой системе передачи данных

Автор:
Калистру И.И.

Заявка РФ
№ 2019110108
от 05.04.2019 г.

Изобретение относится к области вычислительной техники. Техническим результатом является снижение объема служебных данных, которые требуется передавать для обеспечения расшифрования данных и проверки подлинности сообщений. Раскрыт способ обеспечения передачи зашифрованных данных со сменой ключей шифрования и имитозащиты в цифровой системе передачи данных, содержащей по крайней мере один компьютер, отправляющий защищенные сообщения в виде последовательности кадров цифровых данных через сеть передачи данных и выполненный с возможностью формировать кадры данных, содержащие поле данных, служебное поле B размером 1 бит и поле имитовставки кадра, зашифровывать кадры, вычислять имитовставку для кадров; по крайней мере один компьютер, принимающий защищенные сообщения через сеть передачи данных и выполненный с возможностью расшифровывать кадры, проверять имитовставку для кадров; при этом выбирают количество N>0 кадров данных, шифруемых на одном ключе; выбирают количество K>0 ключей для шифрования кадров данных; (А) формируют на компьютере, отправляющем защищенные сообщения, и на компьютере, принимающем защищенные сообщения, идентичные списки ключей шифрования, количество ключей в которых составляет K, причем каждому ключу ставят в соответствие его порядковый номер, начиная с 0; обнуляют значение номера K1 используемого ключа на компьютере, отправляющем защищенные сообщения; обнуляют значение номера K2 используемого ключа на компьютере, принимающем защищенные сообщения; обнуляют на компьютере, отправляющем защищенные сообщения, количество D зашифрованных на данном ключе кадров; (Б) обрабатывают очередной кадр данных на компьютере отправляющем защищенные сообщения, для этого: на компьютере, отправляющем защищенные сообщения, сравнивают N с D, если D=N, то увеличивают значение K1 на 1, обнуляют D; иначе увеличивают значение D на 1; на компьютере, отправляющем защищенные сообщения, формируют очередной кадр данных, записывая в служебное поле B младший бит двоичного представления значения K1; зашифровывают кадр данных на ключе с номером K1 и вычисляют имитовставку на ключе с номером K1; записывают имитовставку в поле имитовставки кадра; отправляют кадр компьютерам, принимающим защищенные сообщения; если K1<K-1 или D не равно N, то переходят к этапу Б; если K1=K-1 и D=N, то, при необходимости, переходят к этапу А; (В) на каждом из компьютеров, принимающих защищенные сообщения, выполняют обработку приходящих кадров данных: принимают очередной кадр; сравнивают значение поля B принятого кадра со значением младшего бита двоичного представления значения K2, если они равны, то расшифровывают кадр данных с помощью ключа с номером K2 и проверяют имитовставку с помощью ключа номер K2, если имитовставка не совпала, то удаляют кадр; если имитовставка совпала, то передают кадр данных по назначению; если значение поля B принятого кадра не равно значению младшего бита двоичного представления значения K2, то вычисляют T=K2+1; если T=K, то удаляют кадр; расшифровывают кадр данных с помощью ключа с номером T и проверяют имитовставку с помощью ключа номер T, если имитовставка не совпала, то удаляют кадр; если имитовставка совпала, то присваивают K2=T, передают кадр данных по назначению; при необходимости, переходят к этапу В.

Патент РФ № 2713759

Способ обнаружения сетевых атак на основе анализа фрактальных характеристик трафика в информационно-вычислительной сети

Авторы:
Репин Д.С.,
Филаретов Г.Ф.
Червова А.А.,

Заявка РФ
№ 2019116376
от 28.05.2019 г.

Изобретение относится к способу обнаружения сетевых атак на основе анализа фрактальных характеристик трафика в информационно-вычислительной сети, причем на входе сети установлено средство контроля, выполненное с возможностью принимать входящий трафик и обрабатывать данные. Технический результат заключается в обеспечении возможности обнаружения компьютерных атак разных видов путем анализа в реальном масштабе времени фрактальных характеристик интенсивности поступающего трафика без предварительного определения его статистических характеристик. Способ заключается в том, что: устанавливают интервал дискретизации по времени, значение масштабирующего множителя, ширину временного скользящего окна, пороговое значение для показателя Херста H; (А) принимают входящий трафик с помощью средства контроля; осуществляют с помощью средства контроля фильтрацию трафика путем исключения из данных прикладного уровня заголовков протоколов низлежащих уровней; вычисляют с помощью средства контроля значения интенсивности трафика на интервале дискретизации по времени; вычисляют для трех последних значений интенсивности трафика масштабированные значения интенсивности трафика путем умножения каждого значения на масштабирующий множитель, показатель кривизны ломаной на основе масштабированных значений интенсивности трафика; вычисляют значения суммарной кривизны ломаной по значениям показателей ее кривизны, зафиксированным в скользящем окне за последний и предыдущие моменты времени; вычисляют значение геометрического индекса фрактальности; вычисляют значение показателя Херста H с помощью приведенного выражения, если рассчитанное значение показателя Херста H ниже порогового значения, то сдвигают временное скользящее окно на один интервал дискретизации по времени; переходят к этапу А; принимают решение о факте наличия компьютерной атаки.

Патент РФ № 2706176

Способ обеспечения криптографической защиты информации в сетевой информационной системе

Автор:
Ерыгин А.В.

Заявка РФ
№ 2019116881
от 31.05.2019 г.

Изобретение относится к области защиты информации. Технический результат заключается в расширении арсенала средств. Способ обеспечения криптографической защиты информации в сетевой информационной системе, которая содержит сервер распространения, защищаемые сетевые устройства (ЗСУ), причем каждое ЗСУ включает средство обработки, зашифровывать данные, расшифровывать данные, при необходимости, в каждом ЗСУ с помощью средства обработки зашифровывают данные в адрес других ЗСУ с использованием прикладных сертификатов этих ЗСУ, если в полученном пакете обновления корневой служебный сертификат средства распространения указан в качестве издателя сертификата ключа электронной подписи и электронная подпись корректна, то расшифровывают данные из пакета обновления с использованием закрытого ключа ключевой пары для служебного сертификата ЗСУ и обновляют данные в каждом ЗСУ иначе отклоняют пакет обновления.

Патент РФ № 2757297

Способ работы кластера шлюзов безопасности

Авторы:
Гузев О.Ю.,
Тычина Л.А.

Заявка РФ
№ 2021110887
от 19.04.2021 г.

Изобретение относится к области сетевых технологий. Технический результат заключается в возможности масштабирования сетевых функций; увеличении скорости обработки сетевых пакетов в коммутаторе; и обеспечении возможности защищенного взаимодействия кластера с внешними шлюзами безопасности и с защищенными клиентами. Способ работы кластера шлюзов безопасности (ШБ) включает следующие операции: формирование ключевой информации для ШБ; выделение двух IP- и MAC - адресов для ШБ, диапазонов туннелируемых ШБ IP-адресов, IP-адреса для устройств кластера, семь физических портов на коммутаторе, уникальный диапазон транспортных портов для каждого ШБ, шесть уровней приоритета для правил таблицы потоков коммутатора; формирование правил фильтрации трафика и правил трансляции IP-адресов для ШБ; выбор ШБ в качестве ведущего ШБ кластера (ВШБ) и контроллера; выбор выделенного ШБ для обработки пакетов, имеющих транспортный протокол, отличный от TCP/UDP; формирование набора статических правил обработки сетевых пакетов для коммутатора; включение всех ШБ и загрузку на каждый ключевой информации, настройку IP-, MAC-адресов, диапазонов туннелируемых IP-адресов, правил фильтрации трафика и трансляции IP-адресов; настройку на всех ШБ, кроме ВШБ, IP-адреса ВШБ из служебной сети; задание в конфигурационном файле ВШБ промежутка времени неактивности динамических правил обработки сетевых пакетов; включение коммутатора и настройку собственного IP-адреса и IP-адреса ВШБ из служебной сети, регистрацию коммутатора в контроллере; загрузку в таблицу потоков коммутатора наборов статических правил обработки сетевых пакетов; включение кластера в рабочий режим для обработки трафика между сетями.

Информационная безопасность в цифровых сетях передачи данных

Патент РФ № 2538292

Способ обнаружения компьютерных атак на сетевую компьютерную систему

Авторы:
Фаткиева Р.Р.,
Атисков А.Ю.,
Левоневский Д.К.

Заявка РФ
№ 2013134440
от 24.07.2013 г.

Изобретение относится к вычислительной технике. Технический результат заключается в обнаружении компьютерных атак разных видов, комбинированных одновременных атак разных видов и определении видов атак. Способ обнаружения компьютерных атак на сетевую компьютерную систему, включающую, по крайней мере, один компьютер, подключенный к сети и имеющий установленную операционную систему и установленное прикладное программное обеспечение, включающее систему анализа трафика, в котором для анализа получаемых из сети пакетов выбираются определенные параметры и вычисляются их значения, которые затем сравниваются с эталонными значениями, а факт наличия одиночной или комбинированной одновременной атаки и определение видов атак определяется по сочетанию установленных условий для параметров. Для обработки получаемых из сети пакетов данных используется система анализа трафика, позволяющая вычислять параметры трафика в реальном масштабе времени.

Патент РФ № 2610395

Способ расследования распределенных событий компьютерной безопасности

Авторы:
Гайнов А.Е.,
Заводцев И.В.

Заявка РФ
№ 2015155443
от 24.12.2015 г.

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

Патент РФ № 2630415

Способ обнаружения аномальной работы сетевого сервера (варианты)

Авторы:
Елисеев В.Л.,
Шабалин Ю.Д.

Заявка РФ
№ 2016105967
от 20.02.2016 г.

Изобретение относится к области мониторинга и защиты информационных систем. Технический результат заключается в повышении безопасности передачи данных. Способ заключается в том, что запускают сервер в режиме контролируемой нормальной работы; формируют нейронную сеть в средстве обнаружения аномальной работы, выполняя следующие действия: запоминают и накапливают в единицу времени значения векторов динамического отклика сервера, вычисляемые на основе следующих параметров: количество, размер и тип входных и выходных пакетов по всем обслуживаемым сервером протоколам; уровень загруженности процессора сервера; уровень использования оперативной памяти сервера; уровень использования виртуальной памяти сервера; количество операций ввода-вывода в дисковых устройствах сервера; формируют обучающее множество нейронной сети; обучают нейронную сеть для минимизации ошибки классификации векторов обучающего множества; устанавливают и запоминают пороговое значение ошибки классификации; запускают сервер в рабочем режиме; обнаруживают аномальную работу сервера.

Патент РФ № 2780166

Способ обнаружения фишинговых доменных имен

Автор:
Колпинский С.В.

Заявка РФ
№ 2021137053
от 15.12.2021 г.

Изобретение относится к области информационной безопасности. Техническим результатом является повышение вероятности обнаружения фишинговых доменных имен. Технический результат достигается за счет того, что способ обнаружения содержит этапы, на которых: составляют множество легитимных доменных имен; создают множество псевдофишинговых доменных имен путем внесения изменений в легитимные имена; для каждого псевдофишингового доменного имени определяют расчетное расстояние до множества легитимных имен и формируют из расчетных расстояний одномерный числовой массив; на основании чего определяют пороговое расчетное расстояние; анализируют поступившее доменное имя: определяют расчетное расстояние до множества легитимных имен; если расчетное расстояние равно нулю, то данное имя считают легитимным; если расчетное расстояние не равно нулю, то: сравнивают расчетное расстояние с пороговым расчетным расстоянием; если расчетное расстояние больше порогового, то данное доменное имя не считают фишинговым; если расчетное расстояние меньше порогового или равно ему, то данное имя считают фишинговым и выполняют следующие действия: определяют для данного доменного имени легитимное доменное имя, до которого нормированное расстояние минимально; формируют отчет об обнаруженном фишинговом доменном имени; завершают обработку данного доменного имени.

Криптография и шифрование

Зарубежные патенты

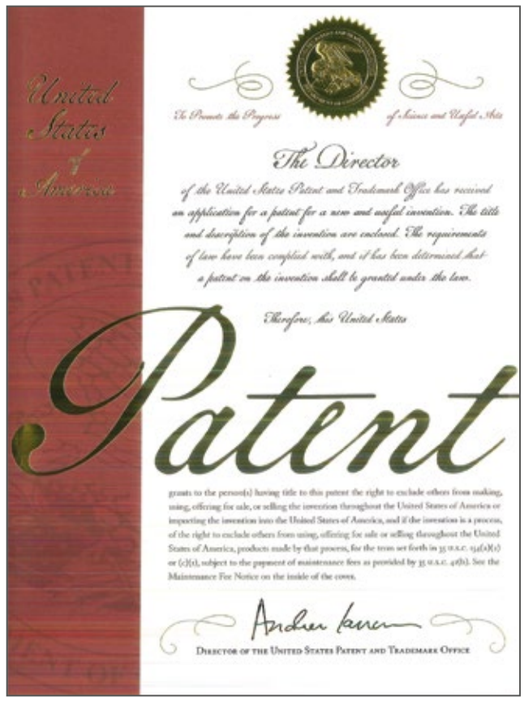
Патент США № 10601582

Metodo de transformacion lineal (variantes)

Авторы:
Борисенко Н.П.,
Уривский А.В

Заявка США
№ 15/513823
от 23.03.2017 г.

The invention relates to the field of computer engineering and cryptography and, in particular, to methods for implementing linear transformation that operate with a specified speed and require minimum amount of memory, for further usage in devices for cryptographic protection of data. The technical results enables the selection of interrelated parameters (performance and required amount of memory) for a particular computing system when implementing a high-dimensional linear transformation. The use of the present method allows for a reeducation of the amount of consumed memory at a given word size of processors employed. To this end, based on a specified linear transformation, a modified linear shift register of Galois-type of Fibonacci-type is generated according to the rules provided in the disclosed method, and the usage thereof enables to obtain the indicated technical results.


United States of America

To Promote the Progress of Science and Useful Arts

The Director

of the United States Patent and Trademark Office has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.

Therefore, this United States

Patent

grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America, and if the invention is a process, of the right to exclude others from using, offering for sale or selling throughout the United States of America, products made by that process, for the term set forth in 35 U.S.C. 154(a)(1) or (c)(1), subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b). See the Maintenance Fee Notice on the inside of the cover.

Director of the United States Patent and Trademark Office

Патент Мексики № 381513

Metodo de transformacion lineal (variantes)

Авторы:
Борисенко Н.П.,
Уривский А.В

Заявка Мексики
№ MX/A/2017/
006999
от 29.05.2017 г.

La invención se refiere al campo de la ingeniería en computación y la criptografía y, en particular, a métodos para implementar transformaciones lineales que operan con una velocidad especificada y requieren una cantidad mínima de memoria, para su uso adicional en dispositivos para la protección criptográfica de datos; el resultado técnico se refiere a permitir seleccionar parámetros interrelacionados (rendimiento y cantidad requerida de memoria) para un sistema de cómputo en particular cuando se implementa una transformación lineal de alta dimensionalidad; el uso del presente método permite reducir la cantidad de memoria consumida en un tamaño de palabra determinado de los procesadores empleados; para este fin, con base en una transformación lineal especificada, un registro de desplazamiento lineal modificado de tipo Galois o de tipo Fibonacci se genera de conformidad con las reglas proporcionadas en el método descrito, y el uso del mismo permite obtener el resultado técnico indicado.


ECONOMÍA IMPI

"2021: Año de la Independencia"

COPIA CERTIFICADA

Por la presente certifico que los documentos adjuntos son copia exacta de TÍTULO, de la Patente número 381513, expedido por este Organismo con fecha 14 de abril de 2021.

Ciudad de México, 29 de octubre de 2021.

COORDINADOR DEPARTAMENTAL DE ARCHIVO DE PATENTES

Ing. Cesar Enrique Rodriguez Hernández

Патент ЕПВ № 3185462

Linear transformation method

Авторы:
Борисенко Н.П.,
Уривский А.В.

Заявка ЕПВ
№ 16833401.9
от 21.03.2017 г.

The invention relates to the field of computer engineering and cryptography and, in particular, to methods for implementing linear transformations which operate with a specified speed and require minimum amount of memory, for further usage in devices for cryptographic protection of data. The technical result relates to enabling to select inter-related parameters (performance and required amount of memory) for a particular computing system when implementing a high-dimensional linear transformation. The use of the present method allows to reduce the amount of consumed memory at a given word size of processors employed. To this end, based on a specified linear transformation, a modified linear shift register of Galois-type or Fibonacci-type is generated according to the rules provided in the disclosed method, and the usage thereof enables to obtain the indicated technical result.

URKUNDE

Europäisches Patent

CERTIFICATE

European patent

CERTIFICAT

Brevet européen

3185462

Joint Stock Company "Infotecs"
Building 1, 1/23
Dlaty Petrovsko-Razumovsky proezd
Moscow 127287 RU

03.07.19

Antonio Campinos

Евразийский патент № 021803

Способ шифрования данных для вычислительных платформ с SIMD-архитектурой

Автор:
Тычина Л.А.

Евразийская заявка на изобретение
№ 201200672
от 25.04.2012 г.

Изобретение относится к шифрованию данных. Предложена методика реализации цикла шифрования данных для вычислительных платформ с SIMD-архитектурой, позволяющая избежать вынужденного смешивания инструкций стандартной архитектуры и SIMD-инструкций за счет специализированной адаптации узлов замены, обеспечивающей возможность выполнения операции замены исключительно при помощи SIMD-инструкций. Технический результат заключается в приросте производительности.

Патент РФ № 2564243

Способ криптографического преобразования

Авторы:
Бородин М.А.,
Рыбкин А.С.

Заявка РФ
№ 2014107554
от 28.02.2014 г.

Изобретение относится к криптографии и средствам защиты информации. Технический результат – увеличение скорости обработки информации и снижение количества операций при реализации итерационного криптографического преобразования. Способ криптографического преобразования сообщения c, представленного в двоичном виде, в котором вычисляют на основе имеющегося набора итерационных ключей K0, …, Kn новый набор итерационных ключей KZ0, …, KZn, причем нулевой ключ в новом наборе определяют по формуле KZ0=K0, а остальные по формуле KZj=L-1(Kj); вычисляют двоичные векторы u[i][j] длины w по формуле u[i][j]=π-1(τ (j))·Gi; вычисляют двоичный вектор m длины w, используя новые итерационные ключи KZ0, …, KZn, выполняя следующие действия: вычисляют mn=S(c), причем S:Vw→Vw, a=at-1||…||a0, где ai∈Vb ; S(a)=S(at-1||…||a0)=π(at-1)||…||π(a0); вычисляют mj-1=X[KZj](qj), где mj=mj[t-1]||mj[t-2]||…||mj[0]; j=n, …, 1; X[KZ] - линейное преобразование, зависящее от итерационного ключа KZ, причем X[KZ]:Vw→Vw, , где KZ, a∈Vw; вычисляют m=X[KZ0](S-1(m0)).

Патент РФ № 2607613

Способ формирования S-блока

Автор:
Иванов А.Г.

Заявка РФ
№ 2015121014
от 03.06.2015 г.

Изобретение относится к области обработки информации и криптографии и, в частности, к способам формирования S-блоков замены с минимальным количеством логических элементов. Техническим результатом является уменьшение схемотехнических затрат при реализации S-блока с помощью логических элементов & и ⊕ (XOR), обеспечение возможности учета различных схемотехнических затрат на реализацию элементов & и ⊕ в процессе минимизации результирующей логической схемы S-блока. Заявляемый способ состоит из аналитического этапа, на котором выполняется последовательная декомпозиция исходных многочленов, задающих S-блок, на суммы и произведения более простых многочленов, для реализации которых требуется меньше суммарных схемотехнических затрат, этапа синтеза, на котором создаются схемы реализации этих далее не упрощаемых многочленов и на основе этих схем в порядке обратном декомпозиции строится итоговая логическая схема реализации S-блока, и третьего этапа, в ходе которого итоговая логическая схема реализуется в электронной схеме.

Патент РФ № 2572423

Способ формирования S-блоков с минимальным количеством логических элементов

Авторы:
Борисенко Н.П.,
Хоанг Д.Т.,
Васинев Д.А.

Заявка РФ
№ 2014112547
от 02.04.2014 г.

Изобретение относится к области вычислительной техники и криптографии и, в частности, к способам формирования S-блоков с минимальным количеством логических элементов для последующей реализации в устройствах защиты данных криптографическими методами. Техническим результатом является уменьшение схемотехнических затрат при реализации S-блока за счет минимизации результирующей логической схемы. Способ состоит в следующем: по заданному S-блоку строят систему булевых функций в виде таблиц истинности, умножают двоичную матрицу размером 2n×2n на значение булевой функции, получают систему полиномов Жегалкина, на этапе анализа определяют данные для минимизации, а на этапе синтеза получают результирующую логическую схему для реализации S-блока, после чего реализуют схему аппаратно на основе различных интегральных микросхем, в том числе на ПЛИС.

Патент РФ № 2598781

Способ линейного преобразования (варианты)

Авторы:
Борисенко Н.П.,
Уривский А.В.

Заявка РФ
№ 2015131963
от 31.07.2015 г.

Группа изобретений относится к области вычислительной техники и может быть использована в устройствах защиты данных. Техническим результатом является уменьшение объема памяти при заданной разрядности процессоров. Способ содержит этапы, на которых задают разрядность W процессора вычислительной системы, равную целочисленной степени числа 2, задают доступный объем памяти вычислительной системы M бит, задают размер s сообщения S, причем s кратно W, задают значение разрядности n регистра сдвига с линейной обратной связью (РСЛОС) по схеме Галуа, формируют РСЛОС по схеме Галуа, модифицируют РСЛОС, осуществляют R тактов работы модифицированного РСЛОС, вычисляют выходное состояние ячеек модифицированного РСЛОС, получают после R тактов работы РСЛОС линейное преобразование блоков s сообщения S, считывают из ячеек модифицированного РСЛОС блоки s линейно преобразованного сообщения S, объединяют блоки и получают линейно преобразованное сообщение S.

Патент РФ № 2666303

Способ и устройство для вычисления хэш-функции

Автор:
Калистру И.И.

Заявка РФ
№ 2017143805
от 14.12.2017 г.

Группа изобретений относится к вычислительной технике и может быть использована для вычисления хэш-функции. Техническим результатом является повышение быстродействия вычислений, расширение возможности выбора конфигурации устройства. Устройство содержит блок предварительной подготовки, имеющий M входов размерностью k бит, при этом M>1; M блоков конвейерного вычисления, работающих параллельно, каждый из которых содержит модуль памяти, модуль отключения обратной связи, сумматор, конвейерный перемножитель, имеющий L каскадов, блок обратной связи и блок накопления; блок объединения.

Российские патенты

Патент РФ № 2686005

Способ обеспечения передачи зашифрованных данных в цифровой системе передачи данных (варианты)

Автор:
Калистру И.И.

Заявка РФ
№ 2018106405
от 21.02.2018 г.

Изобретение относится к вычислительной технике. Технический результат – повышение эффективности расшифровки кадров данных. Способ обеспечения передачи зашифрованных данных в цифровой системе передачи данных, в котором если в компьютере, отправляющем защищенные сообщения, инициализация переменных не проведена, то инициализируют переменные, считывают текущее значение времени из таймера компьютера, отправляющего защищенные сообщения, если текущее значение времени из таймера больше или равно сумме времени отправки предыдущего служебного кадра и значения промежутка времени между служебными кадрами, то отправляют служебный кадр, иначе, если присутствует кадр данных требующий отправки, то обрабатывают этот кадр, если в компьютере, принимающем защищенные сообщения, инициализация переменных не проведена, то сбрасывают флаг, принимают очередной кадр от компьютера, отправляющего защищенные сообщения, определяют тип кадра, если кадр на входе компьютера, принимающего защищенные сообщения, является служебным кадром, то извлекают из служебного кадра значение синхропосылки, проверяют имитовставку служебного кадра, иначе, если кадр на входе компьютера, принимающего защищенные сообщения, не является служебным кадром, то удаляют кадр, иначе проверяют имитовставку кадра.

Патент РФ № 2694336

Способ аутентифицированного шифрования

Авторы:
Бабуева А.А.,
Ефимов Д.В.,
Калистру И.И.,
Науменко А.П.

Заявка РФ
№ 2018117029
от 08.05.2018 г.

Изобретение относится к криптографии и средствам защиты информации. Технический результат – повышение криптографической стойкости способа аутентифицированного шифрования. Способ аутентифицированного шифрования сообщения с использованием блочного шифрования, ключа шифрования K, ключа финализации F, вектора инициализации S, причем сообщение включает в себя ассоциированные данные, имеющие в составе хотя бы один ненулевой блок, и, возможно, открытый текст, способ заключается в том, что зашифровывают открытый текст, вычисляя значения счетчиков, вычисляют начальное значение счетчика, получают каждое последующее значение счетчика путем прибавления единицы по модулю к правым битам предыдущего значения счетчика, зашифровывают открытый текст в режиме гаммирования, формируют имитовставку, вычисляют значение имитозащитной группы, вычисляют ключ имитозащиты с использованием блочного шифрования и ключа K, вычисляют значение вектора с помощью операции умножения в конечном поле Галуа, вычисляют значение имитозащитной группы с использованием блочного шифрования и ключа F, расшифровывают шифртекст, полученный из пакета, в режиме гаммирования, проверяют имитовставку, если значения имитовставок совпали, расшифрованный открытый текст и ассоциированные данные признают истинными.

Патент РФ № 2710669

Способ шифрования данных

Автор:
Рыбкин А.С.

Заявка РФ
№ 2018138851
от 06.11.2018 г.

Изобретение относится к вычислительной технике. Технический результат заключается в повышении производительности процесса шифрования. Способ шифрования s сообщений m1 , m2 , ..., ms , представленных в двоичном виде и имеющих длину, равную 128 бит каждый, где s=t·n, причем t, n - натуральные числа, реализуемый посредством вычислительной системы, имеющей процессор с SIMD-архитектурой, заключающийся в том, что вычисляют u=0; (A) вычисляют параллельно с использованием SIMD-инструкций процессора значения c_{ut+1}, c_{ut+2}, c_{ut+3}, ..., $c_{ut+t} \in V_{128}$; вычисляют преобразованияRSHIFT4 вида $V_8 \to V_8$, преобразования CMPR вида $V_8 \times V_8 \to V_8$ и преобразования BLEND вида $V_8 \times V_8 \times V_8 \to V_8$; преобразования T_2 , T_3 , T_4 вида $V_4 \to V_4$ и преобразования α_0 , α_1 , T_1 , T_5 , T_6 вида $V_4 \to V_8$ вычисляют путем загрузки данных из вспомогательных таблиц, содержащих векторы значений этих преобразований; преобразования MULT148,0, MULT148,1, $MULT_{195,0}$, $MULT_{195,1}$ вида $V_4 \to V_8$ вычисляют путем загрузки данных из вспомогательных таблиц, содержащих векторы значений этих преобразований; вычисляют u=u+ 1; если u <n , то переходят к этапу (A); получают зашифрованные сообщения c_i ,i=1, 2, ...,s.

Параллельная обработка данных

Зарубежный патент

Патент США № 9069625

Method of parallel processing of ordered data streams

Авторы:
Морозов В.В.,
Тычина Л.А.

Заявка США
№ 13/938381
от 10.07.2013 г.

The disclosure relates to parallel processing of multiple digital data streams. The method includes transferring portions of incoming streams and attributes thereof to processors and obtaining respective portions of output streams and providing a sequence of the portions. Providing includes searching for a processor which is processing a portion of a particular incoming stream that has been located in a particular first stream before a portion already processed in said processor, and when several such processors are found, selecting a processor which is processing a portion of the particular incoming stream that is closest to the processed portion of the particular incoming stream. The processed portion of the particular incoming stream (and previously processed portions of the incoming stream from other processors) is transferred to the selected processor. If no such processors are found, the processed portions of the incoming stream are transferred to a respective output stream.

The United States of America

The Director of the United States Patent and Trademark Office

Has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.

Therefore, this

United States Patent

Grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America, and if the invention is a process, of the right to exclude others from using, offering for sale or selling throughout the United States of America, or importing into the United States of America, products made by that process, for the term set forth in 35 U.S.C. 154(a)(2) or (c)(1), subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b). See the Maintenance Fee Notice on the inside of the cover.

Michelle K. Lee

Deputy Director of the United States Patent and Trademark Office

Российские патенты

Патент РФ № 2507569

Способ параллельной обработки упорядоченных потоков данных

Авторы:
Морозов В.В.,
Тычина Л.А.

Заявка РФ
№ 2012129031
от 11.07.2012 г.

Изобретение относится к вычислительной технике и может быть использовано для параллельной обработки нескольких цифровых потоков данных, каждый из которых представляет последовательность дискретных наборов данных определенного вида. Техническим результатом является повышение производительности обработки входных потоков за счет устранения ожидания момента окончания обработки очередной части входного потока в случаях, когда предыдущие части уже обработаны. Способ заключается в том, что получают входные потоки данных, передают части входных потоков данных для обработки в процессорные блоки, каждая часть каждого входного потока данных снабжается атрибутами – идентификатором входного потока и идентификатором положения данной части во входном потоке, обрабатывают части входных потоков данных, обеспечивают порядок следования частей выходных потоков данных, который соответствует порядку частей входных потоков данных, для этого проводят поиск процессорного блока, в котором обрабатывается часть определенного входного потока данных, находившаяся в определенном первом потоке перед частью, уже обработанной в рассматриваемом процессорном блоке, причем, если после поиска таких процессорных блоков найдено несколько, то выбирают тот процессорный блок, в котором обрабатывается часть определенного входного потока данных, расположенная наиболее близко к обработанной части определенного входного потока; передают обработанную часть определенного входного потока данных из рассматриваемого процессорного блока в выбранный процессорный блок, а также, при наличии, ранее полученные от других процессорных блоков обработанные части входного потока данных; если после поиска таких процессорных блоков не найдено, то передают обработанные части входного потока данных в соответствующий выходной поток данных, в которых порядок следования частей соответствует порядку следования частей в соответствующем входном потоке, с учетом ранее полученных от других процессорных блоков обработанных частей входного потока данных.

Патент РФ № 2571376

Способ и устройство для параллельной обработки цифровой информации в вычислительной системе

Автор:
Козырев С.А.

Заявка РФ
№ 2014146704
от 21.11.2014 г.

Изобретение относится к вычислительной технике. Технический результат – повышение скорости обработки цифровой информации. Для этого принимают в первом блоке указатель, дескриптор и данные для обработки из общесистемной шины; передают принятые указатель и дескриптор во второй блок по локальной шине; проводят поиск во втором блоке свободного блока обработки; передают выбранному свободному блоку обработки указатель, дескриптор и данные для обработки; выполняют обработку данных в выбранном блоке обработки по алгоритму, заданному в дескрипторе; передают обработанные данные из блока обработки во второй блок по локальной шине; модифицируют указатель во втором блоке; формируют во втором блоке сигнал для формирования запроса на прерывание; передают модифицированный указатель и сигнал для формирования запроса на прерывание из второго блока в первый блок; получают в первом блоке сигнал запроса на прерывание, модифицированный указатель и обработанные данные от второго блока; формируют в первом блоке запрос на прерывание; передают из первого блока в процессор запрос на прерывание, модифицированный указатель и обработанные данные по общесистемной шине.

Патент РФ № 2685018

Способ распараллеливания программ в вычислительной системе

Автор:
Малов А.В.

Заявка РФ
№ 2018115087
от 24.04.2018 г.

Изобретение относится к вычислительной технике. Технический результат заключается в расширении класса решаемых задач, включая задачи, которые не обладают списочным гомоморфизмом. Способ распараллеливания программ в вычислительной системе заключается в том, что получают входные данные и приложение для их обработки; формируют функции отображения; осуществляют декомпозицию приложения в последовательность обособленных функций; формируют функцию разбиения исходных данных на части для работы одного из множества рабочих процессов; формируют функцию объединения результатов работы множества рабочих процессов в единые промежуточные модели знаний; формируют функцию для формирования финальной выходной модели знаний из промежуточной модели знаний; формируют функцию приема данных главного рабочего процесса; формируют функцию главного рабочего процесса; формируют функцию рабочих процессов; запускают выполнение функции главного рабочего процесса; выполняют последовательность обособленных функций, реализующих шаги приложения, начиная с первой, на множестве рабочих процессов; объединяют единые промежуточные модели знаний в финальную выходную модель знаний и получают финальную выходную модель знаний.

Патент РФ № 2691860

Способ распараллеливания программ в среде логического программирования в вычислительной системе

Автор:
Малов А.В.

Заявка РФ
№ 2018122944
от 25.06.2018 г.

Изобретение относится к способу распараллеливания программ в среде логического программирования. Технический результат заключается в обеспечении распараллеливания задач (алгоритмов) логического программирования, которые не обладают списочным гомоморфизмом. Формируют предикаты, при удовлетворении которых в процессе логического вывода исходные данные D из файлов или баз данных преобразуются в факты базы знаний логической программы. Осуществляют декомпозицию алгоритма на отдельные шаги, которые представляют собой предикаты, являющиеся левой частью правила логической программы, реализующей алгоритм. Формируют предикат для разбиения исходных данных на части для работы одного из множества рабочих процессов. Формируют предикат для объединения результатов работы множества рабочих процессов в единую промежуточную модель знаний в виде фактов базы знаний логической программы. Формируют предикат приема данных главного рабочего процесса, выполненный с возможностью принимать данные из множества рабочих процессов. Формируют предикат главного рабочего процесса, являющийся правой частью правила. Формируют предикаты рабочих процессов, при этом данные предикаты являются правой частью правил. Запускают на выполнение множество рабочих процессов и главный рабочий процесс, с помощью чего выполняют следующие действия: в процессе логического вывода последовательно удовлетворяют предикаты, представляющие шаги приложения, начиная с первого на множестве рабочих процессов.

Патент РФ № 2704533

Способ распараллеливания программ в среде агентно-ориентированного программирования в вычислительной системе

Автор:
Малов А.В.

Заявка РФ
№ 2019102187
от 28.01.2019 г.

Изобретение относится к вычислительной технике. Технический результат заключается в расширении класса решаемых задач, включая задачи, которые не обладают списочным гомоморфизмом. В способе распараллеливания программ в среде агентно-ориентированного программирования в вычислительной системе получают входные данные и приложение для их обработки; формируют функции отображения, преобразующие исходные данные D из файлов или баз данных в набор списочных структур данных, содержащих списки атрибутов и списки векторов; осуществляют декомпозицию приложения в последовательность шагов; формируют специализированную приложением функцию разбиения исходных данных на части для работы каждого из множества программных агентов; формируют специализированную приложением функцию объединения результатов работы множества программных агентов, реализующих шаг приложения, в единые промежуточные модели знаний в виде набора списочных структур данных; формируют специализированную приложением функцию для формирования финальной выходной модели знаний из промежуточной модели знаний, полученной на последнем этапе.

Технологии блокчейн

Российский патент

Патент РФ № 2722285

Способ проверки подлинности изделий

Автор:
Шишкин Е.С.

Заявка РФ
№ 2019144325
от 27.12.2019 г.

Изобретение относится к проверке подлинности изделий. Технический результат заключается в расширении арсенала средств. Способ реализуется с использованием системы, содержащей базу данных (БД) типа публичный блокчейн, связанную с сетью Интернет и выполненную с возможностью назначать идентификаторы пользователям БД, осуществлять вызовы запрограммированных пользователями функций по управлению данными (смарт-контракт), которые способны выполнять следующие действия: в случае если изделие с заданным идентификатором отсутствует в БД, добавлять идентификатор изделия и указывать соответствие этого идентификатора изделия идентификатору производителя, менять соответствие между идентификатором изделия и идентификатором владельца при наличии электронной цифровой подписи (ЭЦП) от текущего владельца изделия и ЭЦП нового владельца; менять соответствие между идентификатором изделия и идентификатором владельца при указании цепочки транзакций между владельцами с указанием корректных ЭЦП всех промежуточных владельцев, добавлять смарт-контракты пользователей; причем при очередной передаче изделия текущий владелец посылает подписанную своей подписью транзакцию напрямую следующему владельцу, избегая необходимости производить транзакцию в блокчейн, обеспечивая анонимность покупателю.

Квантовые технологии

Российские патенты

Патент РФ № 2665249

Способ управления интерференционной картиной в однопроходной системе квантовой криптографии

Авторы:
Балыгин К.А.,
Зайцев В.И.,
Климов А.Н.,
Кулик С.П.,
Молотков С.Н.

Заявка РФ
№ 2017144533
от 19.12.2017 г.

Изобретение относится к области квантовой криптографии. Технический результат – исключение прерывания передачи ключей в режиме квазиоднофотонных состояний для управления интерференционной картиной. Способ заключается в том, что генерируют случайную последовательность нулей и единиц с помощью генератора случайных чисел в передающей части, генерируют на основании последовательности нулей и единиц последовательность квазиоднофотонных состояний в передающей части, разделяют каждое квазиоднофотонное состояние с помощью интерферометра передающей части на пару пространственно разнесенных квазиоднофотонных когерентных состояний, передают полученные пространственно разнесенные квазиоднофотонные когерентные состояния из передающей части в принимающую часть с помощью линии связи, принимают пространственно разнесенные квазиоднофотонные когерентные состояния в принимающей части, получают интерференционную картину от пространственно разнесенных квазиоднофотонных когерентных состояний на выходе интерферометра принимающей части, регистрируют последовательность квазиоднофотонных состояний после прохождения интерферометра принимающей части в фотоприемном блоке в виде последовательности нулей и единиц в зависимости от видности полученной интерференционной картины для каждого квазиоднофотонного состояния, определяют сигнал ошибки в блоке обработки принимающей части на основании сравнения принятой и переданной последовательностей нулей и единиц, при этом в качестве сигнала ошибки применяется величина, пропорциональная числу несовпадений в позициях принятой и переданной последовательностей единиц и нулей, и регулируют видность интерференционной картины, полученной на выходе интерферометра принимающей части, посредством компенсации относительной разности хода в интерферометре принимающей части на основании принятого сигнала ошибки.

Патент РФ № 2706175

Способ квантового распределения ключей в однопроходной системе квантового распределения ключей

Авторы:
Втюрина А.Г.,
Балыгин К.А.,
Зайцев В.И.,
Климов А.Н.,
Кулик С.П.,
Молотков С.Н.

Заявка РФ
№ 2018146854
от 27.12.2018 г.

Изобретение относится к области квантовой криптографии. Технический результат заключается в обеспечении возможности получения секретного ключа заданной длины при установленной длине линии связи и неизменной системе КРК. Технический результат достигается за счет способа квантового распределения ключей, обеспечивающего увеличение длины линии связи с секретным распределением ключей по сравнению с известными протоколами за счет выбора равномерно распределенных по углу относительных фаз информационных квазиоднофотонных когерентных состояний, в которые кодируются биты ключа, и их числа, которое выбирается в зависимости от длины линии связи, на которую требуется обеспечить секретность передачи ключей. Переход на новую длину линии связи осуществляется увеличением числа базисов и, соответственно, числа информационных состояний.

Патент РФ № 2697696

Способ передачи сообщения через вычислительную сеть с применением аппаратуры квантового распределения ключей

Автор:
Поздняков А.М.

Заявка РФ
№ 2019101393
от 18.01.2019 г.

Изобретение относится к области защищенных информационных сетей с квантовым распределением криптографических ключей. Техническим результатом является повышение защищенности передаваемого сообщения. Способ заключается в том, что (А) зашифровывают сообщение в блоке обработки выходного узла k-го звена обработки, при этом: получают квантовый ключ длинной Xk бит; зашифровывают сообщение на квантовом ключе k-го звена обработки с применением выбранного алгоритма шифрования; передают зашифрованное сообщение в блок обработки входного узла k-го звена обработки; добавляют к полученному зашифрованному сообщению ключ Xk, полученный во входном узле k-го звена обработки; формируют значение Yk в зависимости от длины ключа Xk; добавляют к полученному сообщению Yk; формируют значение Zk в зависимости от выбранного алгоритма шифрования; добавляют к полученному сообщению Zk, получая входное сообщение для следующего входного узла; если k<M, то передают входное сообщение в блок обработки выходного узла k+1 звена через цифровую сеть передачи данных; вычисляют k=k+1; получают зашифрованное сообщение в блоке обработки входного узла k-го звена обработки через цифровую сеть передачи данных; обрабатывают зашифрованное сообщение в блоке обработке входного узла k-го звена обработки.

Патент РФ № 2708511

Способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей

Автор:
Жиляев А.Е.

Заявка РФ
№ 2019102923
от 04.02.2019 г.

Изобретение относится к области квантовой криптографии. Технический результат заключается в повышении защищенности передаваемого ключа, возможности использования разных алгоритмов шифрования на каждом участке вычислительной сети, снижении возможности проведения атак, основанных на сборе статистики по побочным каналам. Технический результат достигается за счет способа формирования ключа между двумя узлами вычислительной сети с использованием системы квантового распределения ключей, причем в сети установлены последовательно соединенные М узлов, причем каждый узел включает входной и выходной модули аппаратуры квантового распределения ключей, выполненные с возможностью формирования квантовых ключей в результате выполнения установленного протокола квантового распределения ключей, модуль обработки информации; входной модуль одного узла и выходной модуль предыдущего узла связаны квантовым каналом связи, выполненным в виде оптоволоконной линии; модуль обработки информации связан с входным и выходным модулями цифровой сетью передачи данных и выполнен с возможностью принимать данные, генерировать случайные числа, зашифровывать данные, расшифровывать данные и передавать данные.

Патент РФ № 2736870

Комплекс для защищенной передачи данных в цифровой сети передачи данных с использованием однопроходной системы квантового распределения ключей и способ согласования ключей при работе комплекса

Авторы:
Втюрина А.Г.,
Жиляев А.Е.

Заявка РФ
№ 2019144324
от 27.12.2019 г.

Изобретение относится к защите информации. Технический результат заключается в повышении защищенности передаваемых пользовательских данных, в повышении надежности комплекса, в повышении стойкости квантовых ключей, вырабатываемых системой квантового распределения ключей (КРК), за счет аутентификации служебных данных системы КРК на ключах аутентификации, сформированных из квантовых ключей, и аутентификации служебных данных системы КРК целиком, до разбиения на блоки, используемые при передаче по цифровой линии связи, и последующего шифрования служебных данных системы КРК. В комплексе используется транспортная линия связи, соединяющая два шифратора и два узла системы КРК. Канал передачи системы КРК состоит из аутентифицированного с использованием квантовых ключей канала передачи служебной информации и квантовых ключей из приемного узла системы КРК в сопряженный шифратор и обратно, аутентифицированного с использованием квантовых ключей канала передачи пользовательских данных между шифраторами, аутентифицированного с использованием квантовых ключей канала передачи служебной информации и квантовых ключей из передающего узла системы КРК в сопряженный шифратор и обратно.

Патент РФ № 2752844

Система выработки и распределения ключей и способ распределенной выработки ключей с использованием квантового распределения ключей (варианты)

Автор:
Жиляев А.Е.

Заявка РФ
№ 2020140774
от 10.12.2020 г.

Изобретение относится к системам генерации ключей с использованием технологии квантового распределения ключей (КРК) для криптографических средств защиты информации. Техническим результатом является повышение отказоустойчивости системы за счет децентрализованной обработки запросов пользовательских ключей и расчета квантовых маршрутов. Вырабатывают классический пользовательский ключ в первом и последнем узле сети КРК зарезервированного квантового маршрута в модулях выработки пользовательских ключей с использованием предварительных ключей согласно выбранному порядку выработки классического пользовательского ключа. Вырабатывают в модулях выработки пользовательских ключей первого и последнего узлов сети КРК зарезервированного квантового маршрута пользовательский ключ с использованием квантового пользовательского ключа и классического пользовательского ключа согласно выбранному порядку объединения квантового пользовательского ключа и классического пользовательского ключа. Передают выработанный пользовательский ключ из модуля выработки пользовательского ключа первого и последнего узлов сети КРК зарезервированного квантового маршрута в модули управления пользовательскими ключами первого и последнего узлов сети КРК зарезервированного квантового маршрута. Сохраняют в хранилище пользовательских ключей модуля управления пользовательскими ключами узла сети КРК полученный пользовательский ключ. Передают пользовательский ключ из хранилища пользовательских ключей модуля управления пользовательскими ключами узла сети КРК в шифратор пользователя, запросивший пользовательский ключ.

Патент РФ № 2764458

Способ распределения симметричных ключей между узлами вычислительной сети с системой квантового распределения ключей

Авторы:
Бородин М.А.,
Рыбкин А.С.

Заявка РФ
№ 2021113834
от 17.05.2021 г.

Изобретение относится к области квантовой криптографии. Технический результат заключается в повышении защиты передаваемой информации. Технический результат достигается за счет того, что ключевая информация распространяется по открытым каналам внутри двух ключевых контейнеров: внешний контейнер защищен при помощи квантовых ключей, внутренний контейнер защищается при помощи классических ключей, размер зашифрованных сообщений зависит только от длины распределяемого ключа, что позволяет прогнозировать расход ключевого материала, который используется для защиты.

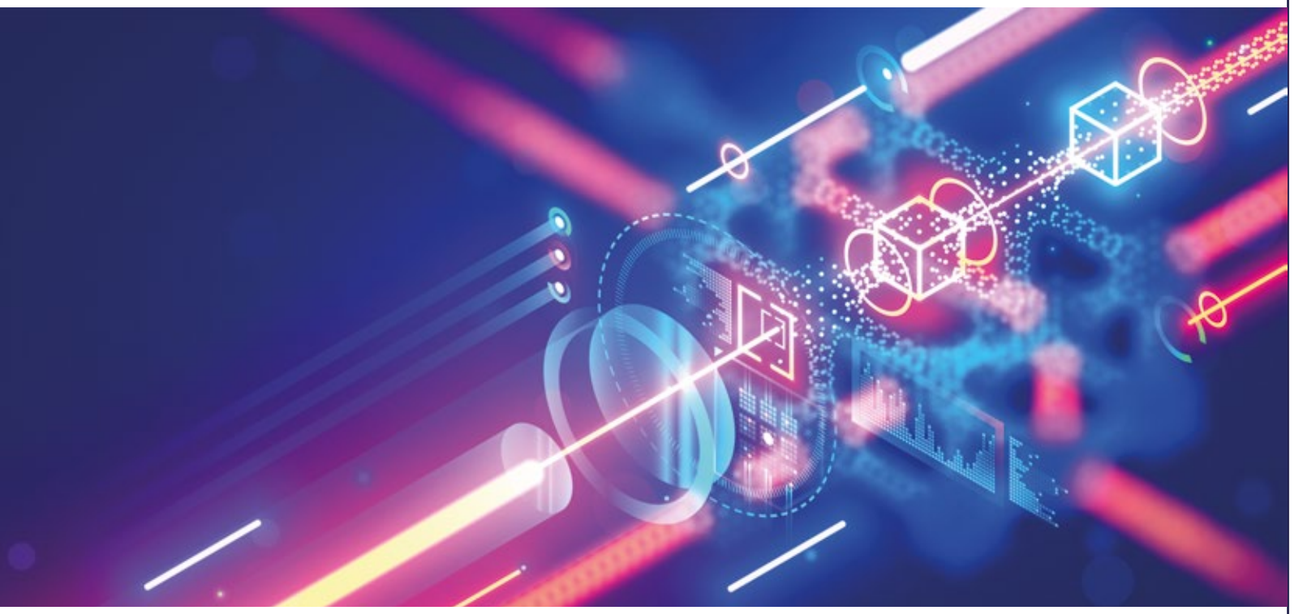
Патент РФ № 2783977

Способ обнаружения атаки с ослеплением детекторов в системе квантовой криптографии с поляризационным кодированием

Автор:
Молотков С.Н.

Заявка РФ
№ 2021134990
от 30.11.2021 г.

Предполагаемое изобретение относится к области квантовой криптографии. Технический результат заключается в обеспечении возможности выявления в системах квантовой криптографии с поляризационным кодированием ложных квантовых состояний в квантовом канале связи, сгенерированных подслушивателем при атаке с ослеплением детекторов. Система включает передающую часть, принимающую часть, включающую фотоприемный блок, линию связи, выполненную в виде одномодового оптического волокна и соединяющую передающую и принимающую части, причем фотоприемный блок содержит два независимых канала - информационный канал и контрольный канал, асимметричный светоделитель, имеющий один вход и два выхода и разделяющий информационный и контрольный каналы, симметричный светоделитель, имеющий один вход и два выхода, управляемый поляризационный преобразователь, имеющий два выхода, два детектора, причем входное излучение принимающей части поступает на вход асимметричного светоделителя, вход поляризационного преобразователя соединен с первым выходом асимметричного светоделителя, вход симметричного светоделителя соединен со вторым выходом асимметричного светоделителя, первый выход поляризационного преобразователя соединен с первым детектором, второй выход поляризационного преобразователя соединен со вторым детектором, первый выход симметричного светоделителя соединен с первым детектором, второй выход симметричного светоделителя соединен со вторым детектором, при этом в информационном канале обеспечиваются поляризационные преобразования входных квантовых состояний перед регистрацией детектором путем подачи управляющих сигналов в поляризационный преобразователь, в контрольном канале не используются поляризационные преобразования входных квантовых состояний перед регистрацией детектором, коэффициент деления асимметричного светоделителя выбирается таким образом, чтобы контрольные состояния и состояния после преобразования поляризации при совпадающих базисах передающей и приемной стороны имели одинаковую интенсивность в первом и втором фотодетекторах.



Патент РФ № 2777422

Способ и устройство генерации квантовых состояний в системе квантового распределения ключей с фазовым кодированием

Авторы:
Алферов С.В.,
Паргачев И.А.

Заявка РФ
№ 2021137055
от 15.12.2021 г.

Изобретение относится к средствам генерации когерентных квантовых состояний для реализации протоколов с фазовым кодированием. Техническим результатом является обеспечение возможности согласования оптических схем в приемнике и передатчике путем электронной регулировки задержки между оптическими импульсами, соответствующей разности оптического хода в плечах интерферометра в приемнике. Получают сообщение с разностью задержки распространения света T в плечах измерительного интерферометра в приемнике. Устанавливают частоту сигнала в электронном генераторе равную 1/2T. Подают сигнал от выхода электронного генератора на вход управления акустооптического модулятора сдвига частоты света. Случайным образом выбирают базис и бит, кодируемые в квантовом состоянии. Генерируют с помощью лазера одиночный оптический импульс. Формируют когерентную пару оптических импульсов, разделенных во времени, выполняя следующие действия. Подают через оптический циркулятор первый пакет из двух когерентных оптических импульсов на вход модулятора фазы. Кодируют в первом пакете из двух когерентных оптических импульсов выбранные бит и базис. Подают на вход аттенюатора первый пакет когерентных импульсов, где он ослабляется до квазиоднофотонного уровня. Получают на выходе аттенюатора квантовое состояние. Направляют сгенерированное квантовое состояние по назначению.

Генераторы случайных чисел

Российские патенты

Патент РФ № 2642351

Способ выбора шумовых диодов с использованием измерительного устройства для генератора случайных чисел

Авторы:
Андрущенко А.С.,
Самоделов А.С.

Заявка РФ
№ 2017101200
от 16.01.2017 г.

Изобретение относится к генераторам случайных чисел (ГСЧ) и может быть использовано для генерации случайных цифровых последовательностей в различной радиоизмерительной аппаратуре и системах тестирования каналов обмена информацией, датчиков случайных чисел, средств криптографической защиты информации. Техническим результатом является упрощение процесса подготовки ГСЧ к последующей работе. Способ содержит этапы, на которых устанавливают перечень статистических характеристик числовой последовательности, включающий, по крайней мере, математическое ожидание и дисперсию частоты появления логической единицы в битовой числовой последовательности; для каждого диода из набора однотипных диодов: отмечают диод из набора однотипных диодов; устанавливают диод в генератор аналогового шума измерительного устройства; получают статистические характеристики числовой последовательности, относящиеся к отмеченному диоду, на выходе измерительного устройства; сохраняют данные о статистических характеристиках отмеченного диода; выбирают пару диодов из набора, осуществляя следующие действия: отмечают пары диодов, имеющих максимальную разницу математического ожидания с идеальным значением и минимальную разницу значений математического ожидания в паре; выбирают из совокупности пар диодов с минимальной разницей значений математического ожидания пару диодов, имеющих минимальную разницу значений дисперсии, определяют положение диодов выбранной пары в генераторах аналогового шума генератора случайных чисел, осуществляя следующие действия: устанавливают на основе случайного выбора диоды из выбранной пары в генераторы аналогового шума, отмечают сведения об установленных диодах для каждого генератора аналогового шума (положение 1), получают математическое ожидание числовой последовательности на выходе генератора случайных чисел, сохраняют его значение, меняют местами диоды в генераторах аналогового шума, отмечают сведения об установленных диодах для каждого генератора аналогового шума (положение 2), получают математическое ожидание числовой последовательности на выходе генератора случайных чисел, сравнивают значения математического ожидания числовой последовательности на выходе генератора случайных чисел для положения 1 и положения 2, выбирают положение диодов с наименьшим отклонением от заданного значения математического ожидания и с наименьшим отклонением от заданного значения дисперсии числовой последовательности на выходе генератора случайных чисел, устанавливают диоды в выбранное положение в генераторы аналогового шума для последующего использования в генераторе случайных чисел.

Патент РФ № 2577201

Способ генерации случайного числа с использованием компьютера (варианты)

Автор:
Курочкин Н.Н.

Заявка РФ
№ 2014115968
от 22.04.2014 г.

Группа изобретений относится к вычислительной технике и может быть использована для генерации случайных чисел с использованием компьютера. Техническим результатом является обеспечение получения случайного числа с энтропией не меньше заданной величины. Способ генерации случайных чисел с использованием компьютера, который содержит таймер для формирования значений текущего времени, не связанный с генератором тактовой частоты компьютера, прикладное программное обеспечение, выполненное с возможностью получать из таймера значения текущего времени, выполнять обработку данных по заранее заданному алгоритму, выполнять операцию хэширования. Способ содержит этапы, на которых задают значение энтропии, определяют для данного компьютера количество M элементов последовательности D, которое необходимо обработать для получения значения энтропии не меньше заданного, формируют последовательность D(M), получают случайное число в результате обработки элементов последовательности D.

Зарубежные патенты

Патент Великобритании № 2417352

Electronic voting method

Автор:
Никишин Н.А.

Заявка РФ
№ 0418505.4
от 18.08.2004 г.

The present invention relates to electronic voting methods and is suitable for collecting and recording data and for processing the results of electronic voting conducted both in a local network or as on-line voting, e,g. over the Internet channels.

INTELLECTUAL PROPERTY OFFICE

Certificate of Grant of Patent

Patent Number: GB2417352
Proprietor(s): Joint Stock Company InfoTeCS
Inventor(s): Nikolai A Nikishin

This is to Certify that, in accordance with the Patents Act 1977,

a Patent has been granted to the proprietor(s) for an invention entitled **"Electronic voting method"** disclosed in an application filed **18 August 2004**.

Dated 4 March 2009

Ian Fletcher
Comptroller General of Patents, Designs and Trade Marks
Intellectual Property Office

The attention of the Proprietor(s) is drawn to the important notes overleaf.

Intellectual Property Office is an operating name of the Patent Office

Евразийский патент № 021508

Способ защищенного обмена данными при электронном аукционе и система для его реализации

Авторы:
Уривский А.В.,
Чмора А.Л.

Евразийская заявка на изобретение
№ 201101235
от 24.08.2011 г.

Изобретение относится к электронным аукционам. Технический результат заключается в обеспечении гарантированной информационной безопасностью потоков данных, возникающих в результате взаимодействия заинтересованных сторон электронного аукциона. Предложены способы защищенного обмена данными при электронном аукционе и компьютерная система для его реализации. Согласно настоящему предложению применяются специализированные протоколы взаимодействия сторон с привлечением широкого спектра криптографических решений. Электронный аукцион состоит из четырех фаз, каковыми фазами являются подготовительная фаза, фаза размещения предложений по заявке, содержащая этапы уведомления о размещении предложений, формирования и подачи предложения участниками и регистрации предложений посредником; фаза рассмотрения предложений, содержащая этапы уведомления о приеме ключей расшифрования участников, обнародования ключей расшифрования и регистрации ключей расшифрования и фаза обнародования результатов по заявке, содержащая этапы определения победителя аукциона, уведомления о результатах и согласительного подтверждения.

Российские патенты

Патент РФ № 2242793

Способ электронного голосования

Автор:
Никишин Н.А.

Заявка РФ
№ 2003103607
от 06.02.2003 г.

Изобретение относится к способам электронного голосования. Технический результат заключается в повышении достоверности результатов выборов. В способе используют компьютерное оборудование, включенное в сеть и установленное у избирателя и у организатора голосования на избирательном участке. При голосовании избиратель заполняет электронный бюллетень для голосования, подписывает его своей электронной цифровой подписью (ЭЦП) и отправляет его на избирательный участок. После проверки ЭЦП на бюллетене с избирательного участка направляют избирателю квитанцию, подписанную ЭЦП организатора голосования. Квитанция содержит полное имя избирателя, результат его голосования и присвоенный ему уникальный персональный идентификатор (УПИ). Избиратель посылает расписку с подтверждением правильности сведений, содержащихся в квитанции, подписанную своей ЭЦП. В процессе голосования создают и публикуют два списка: один список с результатами электронного голосования, в котором приведены УПИ избирателей, а второй список с именами избирателей, принявших участие в электронном голосовании.

Патент РФ № 2624554

Способ обнаружения скрытого программного обеспечения в вычислительной системе, работающей под управлением POSIX-совместимой операционной системы

Автор:
Андрюхин Е.В.

Заявка РФ
№ 2016118865
от 17.05.2016 г.

Изобретение относится к области обнаружения скрытого программного обеспечения в вычислительных системах, работающих под управлением POSIX-совместимых операционных систем, например Solaris, Android и др. Техническим результатом является повышение защищенности вычислительной системы. Раскрыт способ обнаружения скрытого программного обеспечения в вычислительной системе, работающей под управлением POSIX-совместимой операционной системы, причем операционная система, помимо ядра, включает следующие программные средства: 1-е средство, выполненное с возможностью определять количество инсталлированных приложений в вычислительной системе, 2-е средство, выполненное с возможностью определять количество запущенных процессов в вычислительной системе, 3-е средство, выполненное с возможностью определять для процессов статусы pid, name, uid, groups, state, 4-е средство, выполненное с возможностью сравнивать результаты работы 1-го, 2-го и 3-го средств; при этом способ заключается в том, что получают с помощью 1-го средства количество инсталлированных приложений в вычислительной системе; получают с помощью 2-го средства количество запущенных процессов в вычислительной системе; получают с помощью 3-го средства значения статусов pid, name, uid, groups, state каждого процесса; выполняют с помощью 4-го средства для каждого процесса, список которых получен с помощью 3-го средства, следующие действия: сравнивают значение статуса groups, полученное из 3-го средства, с нулем; если значение статуса groups равно нулю – приложение считается скрытым, и сведения о приложении заносятся в отчет о наличии скрытых приложений и процессов; сравнивают значения статусов uid и name, полученные из 3-го средства, с соответствующими значениями uid и name, полученными из 1-го средства; если хотя бы одно из значений одноименных статусов не существует или не совпадает – приложение считается скрытым, и сведения о приложении заносятся в отчет о наличии скрытых приложений и процессов; сравнивают значения статусов pid, name и state, полученные из 3-го средства, с соответствующими значениями pid, name и state, полученными из 2-го средства; если хотя бы одно из значений одноименных статусов не существует или не совпадает – процесс считается скрытым, и сведения о процессе заносятся в отчет о наличии скрытых приложений и процессов; предоставляют отчет о наличии скрытых приложений и процессов; удаляют из вычислительной системы выявленные скрытые приложения.

Патент РФ № 2648621

Способ выявления пользователя-нарушителя в многопользовательской сетевой системе, передающего данные внешнему контрагенту без разрешения

Авторы:
Богатырев М.А.,
Сокуренко А.А.

Заявка РФ
№ 2017112949
от 14.04.2017 г.

Изобретение относится к обеспечению безопасности в сетях передачи данных. Технический результат – возможность определения пользователей, получающих данные из сетевого централизованного хранилища данных легальным способом и предоставляющих эти данные третьим лицам без разрешения владельца данных. Способ заключается в том, что получают сведения о внешнем контрагенте, способном предоставить данные из хранилища данных без использования системы, осуществляют запрос данных из хранилища к внешнему контрагенту без использования системы, получают данные из хранилища от внешнего контрагента без использования системы, определяют расположение полученных данных в хранилище данных, определяют заданный промежуток времени для внесения меток, вносят метки в данные хранилища через заданные промежутки времени, осуществляют запрос данных из хранилища к внешнему контрагенту без использования системы, получают данные хранилища от внешнего контрагента без использования системы, находят метку в составе полученных данных хранилища, осуществляют поиск найденной метки в журнале внесения меток, устанавливают сведения о пользователях, которые соответствуют найденной метке, формируют текущий список пользователей-подозреваемых, которые соответствуют найденной метке, выбирают очередного пользователя-подозреваемого из списка, отключают обслуживание запросов для очередного пользователя-подозреваемого, осуществляют запрос данных из хранилища к внешнему контрагенту без использования системы, если получают данные из хранилища от внешнего контрагента без использования системы, то формируют очередной список пользователей-подозреваемых, которые соответствуют найденной метке, исключают из текущего списка тех пользователей-подозреваемых, которые отсутствуют в текущем или очередном списках, очищают журнал внесения меток, признают очередного пользователя-подозреваемого в качестве пользователя-нарушителя.

Патент РФ № 2688202

Способ скрытой маркировки потока данных цифрового телевизионного сигнала

Автор:
Шишкарев В.Н.

Заявка РФ
№ 2018124210
от 03.07.2018 г.

Изобретение относится к способам скрытой маркировки потока данных цифрового телевизионного сигнала (встраиванию цифровых «водяных знаков» (ЦВЗ)). Техническим результатом является улучшение целостности передаваемого контента, повышение скрытности ЦВЗ, упрощение процесса вставки ЦВЗ. Предложен способ скрытой маркировки потока данных цифрового телевизионного сигнала, заключающийся в том, что формируют совокупность макроблоков для замены; записывают сформированные для замены макроблоки в память; принимают транспортный поток данных цифрового вещательного телевидения; записывают часть транспортного потока в память; находят в записанной части транспортного потока пакетированный элементарный поток (ПЭП); проводят обработку ПЭП, выполняя следующие действия: (A) выполняют поиск заголовка ПЭП; определяют начало ПЭП; определяют по данным структуры уровня сетевой абстракции наличие в составе ПЭП B-псевдокадров; если не найдено ни одного B-псевдокадра, то переходят к этапу (A); (B) декодируют очередной B-псевдокадр на слайсы; определяют пригодность очередного слайса для обработки, выполняя следующие действия: декодируют слайсы на макроблоки; определяют для очередного макроблока выполнение условий: макроблок не является опорным для других макроблоков в других слайсах и/или кадрах; макроблок не содержит векторов движения; если условия выполнены, то помечают найденный макроблок; если очередной B-псевдокадр последний из найденных, то переходят к этапу (A); если не найдено ни одного пригодного макроблока, то переходят к этапу (B); записывают слайс, содержащий найденный макроблок, в память; выбирают из заранее сформированных макроблоков подходящий макроблок для замены найденного макроблока; записывают в памяти подходящий макроблок вместо найденного макроблока; восстанавливают исходный B-псевдокадр, содержащий замененный макроблок; вычисляют контрольную сумму измененного B-псевдокадра; вставляют контрольную сумму в транспортный поток на более высокий уровень, чем тот, где заменялся макроблок; вставляют измененный B-псевдокадр в ПЭП; вставляют ПЭП из памяти в записанную часть транспортного потока; передают часть транспортного потока из памяти в сети распространения ТВ-сигналов.

Патент РФ № 2700185

Способ обнаружения скрытого программного обеспечения в вычислительной системе, работающей под управлением POSIX-совместимой операционной системы

Автор:
Андрюхин Е.В.

Заявка РФ
№ 2018127626
от 27.07.2018 г.

Изобретение относится к области обнаружения скрытого программного обеспечения в вычислительных системах, работающих под управлением POSIX-совместимых операционных систем. Техническим результатом является повышение защищенности вычислительной системы. В способе сравнивают значения статусов name, gid, полученные из 1-го программного средства, с соответствующими значениями name, gid, полученными из 4-го программного средства; сравнивают значения статусов name и uid, полученные из 2-го программного средства, с соответствующими значениями name и uid, полученными из 1-го программного средства; сравнивают значения статусов name и pid, полученные из 2-го программного средства, с соответствующими значениями name и pid, полученными из 3-го программного средства; сравнивают значения статусов pid и uid, полученные из 3-го программного средства, с соответствующими значениями pid и uid, полученными из 2-го программного средства; сравнивают значения статусов name, pid, ppid, state, полученные из 3-го программного средства, с соответствующими значениями name, pid, ppid, state, полученными из 4-го программного средства; если хотя бы одно из значений одноименных статусов не существует или не совпадает – приложение считается скрытым; предоставляют отчет о наличии скрытых приложений и процессов.

Патент РФ № 2726266

Способ работы регистра сдвига с линейной обратной связью

Автор:
Рыбкин А.С.

Заявка РФ
№ 2020107680
от 20.02.2020 г

Изобретение относится к области вычислительной техники. Технический результат заключается в повышении производительности работы РСЛОС типа Фибоначчи при использовании вычислительной системы, позволяющей параллельно вычислять k одинаковых линейных функций от разных аргументов. Технический результат достигается за счет способа работы регистра сдвига с линейной обратной связью (РСЛОС) в вычислительной системе, включающего задание конечного поля P с операцией сложения «+», операцией умножения «x», нулевым элементом θ и единичным элементом e; выбор вычислительной системы, имеющей процессор с SIMD-архитектурой, задание натурального числа n; задание натурального числа k, $k \le n$; задания РСЛОС в конфигурации Фибоначчи, задания количества тактов работы РСЛОС - m, где $m \ge 1$, $m=kv+w$, где v, w - целые неотрицательные числа, $0 \le w \le k-1$; осуществление m тактов работы РСЛОС.

Патент РФ № 2773010

Способ обнаружения аномалий в многомерных данных

Авторы:
Гузев О.Ю.
Гурина А.О.

Заявка РФ
№ 2021126424
от 08.09.2021 г.

Изобретение относится к способу обнаружения аномалий в многомерных данных в вычислительной системе. Технический результат заключается в сокращении времени подготовки автокодировщика к обнаружению аномалий и в уменьшении количества ошибок первого (false positive) и второго рода (false negative) при обнаружении аномалий. В способе запускают персональный компьютер в режиме контролируемой нормальной работы ;формируют обучающую выборку, представляющую собой двухмерный числовой массив; выбирают минимальное и достаточное для обучения автокодировщика количество строк обучающей выборки Nmin; если количество строк сформированной обучающей выборки N превышает Nmin, то сжимают обучающую выборку, выполняя следующие действия: вычисляют коэффициент сжатия Kcmp=N/Nmin; создают пустой двухмерный числовой массив Tcmp; находят количество повторов Ri каждой уникальной строки в обучающей выборке, где i - номер уникальной строки; для каждой уникальной строки i вычисляют Rmini=Ri /Kcmp и округляют получившийся Rmini до ближайшего целого числа, при этом, если в результате округления Rmini оказывается равным 0, то устанавливают Rmini=1; каждую уникальную строку i добавляют Rmini раз в конец массива Tcmp; в качестве обучающей выборки используют массив Tcmp; далее формируют первый автокодировщик, содержащий входной слой, по крайней мере один скрытый слой и выходной слой, причем размеры входного и выходного слоев совпадают, размер скрытого слоя меньше размера входного слоя; обучают первый автокодировщик с использованием обучающей выборки; выбирают точность округления значений IRE; вычисляют мгновенную ошибку реконструкции IREj для каждой строки j обучающей выборки и округляют IREj с выбранной точностью округления; на основании полученных значений IRE формируют два одномерных числовых массива: массив IREu, содержащий только уникальные значения IRE в порядке возрастания, массив IREc, содержащий количества повторов уникальных значений IRE для обучающей выборки; если массив IREu содержит менее трех элементов, и первый элемент массива равен 0, то устанавливают первый элемент массива равным 0.01; устанавливают порог мгновенной ошибки реконструкции IREm равным IREu0 , где 0 - номер первого элемента массива; если массив IREu содержит более одного элемента, то выполняют следующие действия: выбирают значение критерия выброса Kout; если массив IREu содержит два элемента, и при этом IREu1 -IREu0≤Kout, то устанавливают IREm равным IREu1 ; если массив IREu содержит более двух элементов, то выполняют следующие действия: находят наибольшее значение CNTm массива IREc; вычисляют одномерный массив метрик M п о формуле:

$$M_k = \frac{IREu_k \times CNTm}{IREc_k}$$

, где k - номер элемента массива IREu;

получают массив Msrt путем сортировки элементов массива M по возрастанию; устанавливают порог мгновенной ошибки реконструкции IREm равным значению последнего элемента массива IREu, при этом переменной Kan присваивают значение 0; выполняют проверку элементов массива IREu, начиная с третьего от начала и до последнего, где k - номер текущего элемента массива, нумерацию начинают с 0, причем, если для k-го элемента массива одновременно выполняются два условия:

$$\frac{IREu_k - IREu_o}{IREu_{k-1} - IREu_o} > \frac{IREu_k + Kout}{IREu_k} \quad \text{и}$$

$$\frac{Msrt_k - Msrt_o}{Msrt_{k-1} - Msrt_o} > \frac{IREu_k + Kout}{IREu_k}, \quad \text{то}$$

проверку массива IREu прекращают, при этом текущее значение k присваивают переменной Kan; если Kan>0, то выполняют проверку элементов массива IREu в обратном порядке, начиная с последнего элемента и до элемента с номером Kan, где n - номер текущего элемента массива, причем, если для n-го элемента массива выполняется условие Mn≥MsrtKan, то устанавливают IREm равным IREun-1, иначе проверку массива IREu прекращают; удаляют из обучающей выборки выбросы - строки, для которых IREj>IREm, где j - номер строки обучающей выборки; удаляют из обучающей выборки дубликаты строк; удаляют первый автокодировщик; формируют второй автокодировщик, содержащий входной слой, по крайней мере один скрытый слой и выходной слой, причем размеры входного и выходного слоев совпадают, размер скрытого слоя меньше размера входного слоя; обучают второй автокодировщик с использованием полученной обучающей выборки; вычисляют мгновенную ошибку реконструкции IREj для каждой строки j обучающей выборки и округляют IREj с выбранной точностью округления; устанавливают порог мгновенной ошибки реконструкции IREm равным наибольшему значению IRE для обучающей выборки; формируют тестовую выборку, представляющую собой двухмерный числовой массив; выполняют реконструкцию тестовой выборки обученным вторым автокодировщиком; вычисляют IRE для каждой строки тестовой выборки и округляют с выбранной точностью округления; если IRE строки тестовой выборки превышает IREm, то данная строка считается аномальной и помечается; формируют отчет об обнаруженных в тестовой выборке аномальных строках.

Повышение надежности и производительности компьютерных систем

Зарубежные патенты

Патент США № 9507817

Method for synchronizing access to shared resources of a computing system and detecting and eliminating deadlocks using lock files

Автор:
Мардугаллямов Р.Т.

Заявка США
№ 13/938660
от 10.07.2013 г.

The disclosure generally relates to computer engineering, in particular, to a method for synchronizing access to shared resources of a computing system, and for detecting and eliminating deadlocks using lock files. The disclosure advantageously improves reliability of detection and elimination of deadlocks. The method grants access to a shared resource to other processes and ensures that there will be no deadlock in cases where the process, whose data is indicated in the lock file, does not currently exist in the computing system (for example, an application was aborted from RAM by the operating system due to an internal software failure). The method can be preferably implemented in POSIX-compatible operating systems, in particular, the GNU/Linux operating system.

Патент США № 9177149

Method of detecting malware in an operating system kernel

Авторы:
Ольшанов К.Д.,
Череменцев С.Н.

Заявка США
№ 14/391763
от 10.10.2014 г.

The present invention relates to means for detecting malware. The method is realized on a computer with an operating system (OS) installed thereon, and comprises a step in which a point of interrupt is established when a system call is made by a user application requesting the transfer of control via an address in the kernel of the loaded OS. Next, the data structure of the loaded OS is checked. As this check is carried out, the address of the command in the random-access memory of the computer, by means of which command control will be transferred during the system call, is determined and the addresses of the commands to be executed during the system call are checked to see if they belong to the normal range of addresses of the OS kernel and OS kernel modules in the random-access memory. The presence of malware is then detected in the event that a command address does not belong to the normal range of addresses. The proposed method includes a dynamic check of the execution of the OS kernel code in order to detect the illegal interception and alteration of the code in the kernel and in the kernel modules (drivers) that are to be loaded. The proposed method enables the detection of both known and previously unregistered malware in an OS kernel and in OS kernel modules that are to be loaded.

Патент Германия № 112013002012

Авторы:
Тумоян Е.П.,
Ольшанов К.Д.,
Череменцев С.Н.

Заявка Германии
№ 112013002012.2
от 10.10.2014 г.

Hauptanspruch: Ein Verfahren eines Erkennens von Schadsoftware in einem Betriebssystemkern eines auf einem Computer installierten Betriebssystems, OS, wobei das Verfahren die Schritte umfasst: durch Erzeugen eines Bilds des Betriebssystemkerns, Erhalten eines Referenzabbilds des Betriebssystemkerns und eines normalen Bereichs von Adressen eines Programcodes des Betriebssystemkerns und von Betriebssystemkern-Modulen auf dem Arbeitsspeicher, RAM, des Computers, wobei der normale Bereich von Adressen ein Satz von Arbeitsspeicher-Adressbereichen ist, welcher ein Referenzabbild des Betriebssystemkern-Programmcodes und von Betriebssystemkern-Modulen nach dem Booten des Referenzbetriebssystem-Abbilds in Abwesenheit von Schadsoftware beherbergt; falls eine Unterbrechung ausgeführt wird, wenn eine Benutzer-Anwendung einen Systemaufruf ausführt, wobei eine Übertragung einer Steuerung zu dem Betriebssystemkern des geladenen Betriebssystems, OS, auftritt, Ausführen eines dynamischen Überprüfens einer Ausführung des geladenen Betriebssystem-Programmcodes durch Ausführen der folgenden Schritte: ein Bestimmen einer Adresse in dem Arbeitsspeicher eines jeden Befehls, zu welchem die Steuerung während des Systemaufrufs übertragen werden wird, und ein Überprüfen, ob die Adressen der während des Systemaufrufs auszuführenden Befehle zu dem normalen Bereich von Adressen gehören; und ein Identifizieren einer Anwesenheit von Schadsoftware, falls eine Adresse eines Befehls aus den Adressen der Befehle nicht zu dem normalen Bereich der Adressen gehört.


Bundesrepublik Deutschland

Urkunde

über die Erteilung des
Patents Nr. 11 2013 002 012

Bezeichnung:
Verfahren eines Erkennens von Schadsoftware in einem Betriebssystemkern

IPC:
G06F 21/56

Inhaber/Inhaberin:
Joint Stock Co. "InfoTeCS", Moskau, RU

Erfinder/Erfinderin:
Olshanov, Konstantin Dmitrievich, Taganrog, RU; Tumoyan, Evgeny Petrovich, Taganrog, RU; Cherementsev, Sergei Nikolaevich, Sochi, RU

Tag der Anmeldung:
27.03.2013

Tag der Veröffentlichung der Patenterteilung:
28.04.2022

Priorität:
11.04.2012 RU 2012113963

Die Präsidentin des Deutschen Patent- und Markenamts

Cornelia Rudloff-Schäffer

München, 28.04.2022

Патент РФ № 2510075

Способ обнаружения вредоносного программного обеспечения в ядре операционной системы

Авторы:
Тумоян Е.П.,
Ольшанов К.Д.,
Череменцев С.Н.

Заявка РФ
№ 2012113963
от 11.04.2012 г.

Изобретение относится к вычислительной технике и к обеспечению информационной безопасности автоматизированных и информационно-вычислительных систем, в частности к средствам обнаружения вредоносного программного обеспечения (ПО). Техническим результатом является повышение эффективности обнаружения вредоносного ПО за счет обеспечения возможности обнаружения нелегальных перехватов и изменения кода в ядре и загружаемых модулях ядра ОС. Способ реализуется на компьютере с установленной на нем операционной системой (ОС) и заключается в том, что формируют точку прерывания при выполнении системного вызова пользовательского приложения на возникновение передачи управления по адресу в ядре загруженной ОС, проводят проверку структуры данных загруженной ОС, выполняя следующие действия: определяют адрес команды в оперативной памяти компьютера, которой будет передано управление в ходе системного вызова; проверяют принадлежность адресов команд, выполняемых в ходе системного вызова, к нормальному диапазону адресов ядра и модулей ядра ОС в оперативной памяти; судят о наличии вредоносного ПО при отсутствии принадлежности адреса команды к нормальному диапазону адресов.

Патент РФ № 2526282

Способ синхронизации доступа к разделяемым ресурсам вычислительной системы и обнаружения и устранения повисших блокировок с использованием блокировочных файлов

Автор:
Мардугаллямов Р.Т.

Заявка РФ
№ 2012140253
от 21.09.2012 г.

Изобретение относится к способу обнаружения и устранения повисших блокировок с использованием блокировочных файлов. Технический результат заключается в повышении надежности обнаружения и устранения повисших блокировок. Ассоциируют разделяемый ресурс с блокировочным файлом. Вызывают системный вызов атомарного эксклюзивного создания и открытия временного файла с уникальным именем и в той же файловой системе. Помещают во временный файл информацию о текущем процессе, который пытается обратиться к разделяемому ресурсу. Осуществляют системный вызов создания жесткой ссылки с именем блокировочного файла на временный файл. Если системный вызов создания жесткой ссылки выполнен успешно, то удаляют жесткую ссылку на временный файл и обеспечивают выполнение текущим процессом операций с разделяемым ресурсом. Если текущий процесс в системе не существует, то выполняют устранение повисшей блокировки, осуществляя следующие действия: удаляют из существующего блокировочного файла предыдущие данные несуществующего процесса; заносят в существующий блокировочный файл данные текущего процесса. Снимают файловую блокировку записи с существующего блокировочного файла. Обеспечивают выполнение текущим процессом операций с разделяемым ресурсом. Удаляют существующий блокировочный файл.

Патент РФ № 2543961

Способ кодирования и вычисления даты с использованием упрощенного формата в цифровых устройствах

Авторы:
Белевский В.А.,
Курочкин Н.Н.,
Селеверстов И.А.

Заявка РФ
№ 2013101808
от 16.01.2013 г.

Изобретение относится к способам кодирования и преобразования даты для хранения. Технический результат заключается в снижении необходимого объема памяти для хранения даты. Выделяют для хранения данных о дате, включающей год, месяц и день, целое число длиной K бит. Устанавливают для отсчета фиксированную дату как первое января определенного года Y0. Вводят значения текущего года Y, месяца M, дня D. Вычисляют целое число N для хранения данных о дате по формуле N=D+(M-1)*32+(Y-Y0)*384. Сохраняют число N в двоичном формате. Вычисляют, при необходимости, дату по формулам D=N mod 32, M=(N div 32) div 12+1, Y=Y0+(N div 384), где div – операция целочисленного деления (деления с отбрасыванием дробной части), mod – операция взятия остатка от целочисленного деления.

Патент РФ № 2577200

Способ синхронизации доступа к разделяемым ресурсам вычислительной системы под управлением POSIX-совместимой ОС и обнаружения и устранения повисших блокировок с использованием блокировочных файлов

Автор:
Мардугаллямов Р.Т.

Заявка РФ
№ 2014143964
от 31.10.2014 г.

Изобретение относится к способу обнаружения и устранения повисших блокировок с использованием блокировочных файлов. Технический результат заключается в повышении надежности обнаружения и устранения повисших блокировок. Ассоциируют разделяемый ресурс с блокировочным файлом. Вызывают системный вызов атомарного эксклюзивного создания и открытия временного файла с уникальным именем и в той же файловой системе. Осуществляют системный вызов создания жесткой ссылки с именем блокировочного файла на временный файл. Если системный вызов создания жесткой ссылки выполнен успешно, то удаляют жесткую ссылку на временный файл и обеспечивают выполнение текущим процессом операций с разделяемым ресурсом. Если текущий процесс в системе не существует, то выполняют устранение повисшей блокировки, осуществляя следующие действия: удаляют из существующего блокировочного файла предыдущие данные несуществующего процесса; заносят в существующий блокировочный файл данные текущего процесса. Снимают файловую блокировку записи с существующего блокировочного файла. Обеспечивают выполнение текущим процессом операций с разделяемым ресурсом. Удаляют существующий блокировочный файл.

Патент РФ № 2615336

Способ кодирования и вычисления даты с использованием упрощенного формата в цифровых устройствах

Автор:
Лапин В.Г.

Заявка РФ
№ 2016114982
от 19.04.2016 г.

Изобретение относится к вычислительной технике и может быть использовано для кодирования и преобразования даты в цифровых устройствах. Техническим результатом является увеличение диапазона возможных значений даты. Способ содержит этапы, на которых выделяют для хранения данных о дате, включающей год, месяц и день, целое число длиной K бит; устанавливают для отсчета фиксированную дату как первое января определенного года Y0; вводят значения текущего года Y, месяца M, дня D; вычисляют целое число N для хранения данных о дате по формуле N=D+M*31+(Y-Y0)*372-32; сохраняют число N в двоичном формате; вычисляют при необходимости дату по формулам D=((N mod 372) mod 31)+1, M=((N mod 372) div 31) +1, Y=Y0+(N div 372), где div – операция целочисленного деления (деления с отбрасыванием дробной части); mod – операция взятия остатка от целочисленного деления.

Патент РФ № 2630591

Способ управления конфигурацией прикладного программного обеспечения в компьютере пользователя

Авторы:
Ерыгин А.В.,
Селеверстов И.А.

Заявка РФ
№ 2016122023
от 03.06.2016 г.

Изобретение относится к управлению конфигурацией прикладного программного обеспечения (ПО) в компьютере пользователя. Технический результат заключается в снижении количества ошибок пользователя, сокращении трудозатрат пользователя в ходе проведения конфигурации ПО; упрощении процесса конфигурации ПО для пользователя. Предложен способ, в котором средство управления и конфигурирования ПО выполнено с возможностью автоматически формировать средство контроля параметров конфигурации ПО со стороны пользователя; причем ПО выполнено с возможностью предоставления сведений о параметрах конфигурации и пределах их изменений; в котором предоставляют пользователю с помощью средства контроля возможность просмотра и изменения параметров конфигурации ПО; передают из средства контроля в средство управления измененные пользователем параметры конфигурации ПО; проверяют в средстве управления правильность измененных пользователем параметров конфигурации ПО; при необходимости, корректируют в средстве управления измененные пользователем параметры конфигурации ПО; передают из средства управления скорректированные параметры конфигурации в ПО; информируют пользователя о проведенной коррекции измененных пользователем параметров конфигурации ПО.

Патент РФ № 2630421

Способ кодирования и вычисления даты с использованием упрощенного формата в цифровых устройствах

Автор:
Лапин В.Г.

Заявка РФ
№ 2016142693
от 31.10.2016 г.

Изобретение относится к вычислительной технике и может быть использовано для кодирования и преобразования даты в цифровых устройствах. Техническим результатом является увеличение диапазона возможных значений даты. Способ содержит этапы, на которых выделяют для хранения данных о дате, включающей год, месяц и день, целое число длиной K бит; устанавливают для отсчета фиксированную дату как первое января определенного года Y0; вводят значения текущего года Y, месяца M, дня D; если D<31, то вычисляют целое число N для хранения данных о дате по формуле: N=367×(Y-Y0)+(M-1) ×30+D; иначе вычисляют целое число N для хранения данных о дате по формуле: N=367×(YY0)+361+(M div 10+M)div2, где div – операция целочисленного деления (деления с отбрасыванием дробной части); сохраняют число N в двоичном формате; вычисляют, при необходимости, дату по формулам Y=Y0+(N-1) div 367; вычисляют промежуточную величину A=(N-1)mod 367+1, где mod - операция взятия остатка от целочисленного деления; если A>360, то вычисляют: M=(A-360)×2-1-(A-360)div 5; D=31; иначе вычисляют: M=(A-1)div 30+1; D=(A-1)mod 30+1.

Патент РФ № 2639669

Способ кодирования и вычисления даты с использованием упрощенного формата в цифровых устройствах

Автор:
Лапин В.Г.

Заявк РФ
№ 2017110023
от 27.03.2017 г.

Изобретение относится к вычислительной технике и, в частности, к способу кодирования и преобразования даты для хранения. Технический результат заключается в увеличение диапазона значений даты практически до максимального, при сравнимой простоте и скорости вычислений, а также компактности хранений. Технический результат достигается за счет выделения для хранения данных о дате, включающей год, месяц и день, целое число длиной K бит, установки для отсчета фиксированной даты как первое января определенного года Y0, ввода значения текущего года Y, месяца M, дня D, и если D<31, то вычисляют целое число N для хранения данных о дате по формуле: N=366×(Y-Y0)+(M-1)×30+D, иначе при M=1 вычисляют целое число N по формуле: N=366×(Y-Y0)+60, а при M>1 вычисляют целое число N по формуле: N=366×(Y-Y0)+360+(M div 10+M) div 2, где div – операция целочисленного деления.

Патент РФ № 2673019

Способ обеспечения доступа к разделяемому ресурсу в распределенной вычислительной системе

Автор:
Шишкин Е.С.

Заявка РФ
№ 2017143803
от 14.12.2017 г.

Изобретение относится к способу обеспечения доступа к разделяемому ресурсу в распределенной вычислительной системе. Технический результат заключается в обеспечении управления доступом к разделяемому ресурсу. Способ заключается в том, что если узел впервые обращается за доступом к разделяемому ресурсу или узел восстанавливается после временного прекращения работоспособности, то назначают уникальный идентификатор для каждого активного процесса в системе с учетом возможности сравнения идентификаторов через отношение «меньше – больше»; при необходимости получения доступа к разделяемому ресурсу посылают запрос на получение доступа к разделяемому ресурсу от процесса-клиента в средстве блокирования, ожидают в средстве блокирования получения разрешения на доступ к разделяемому ресурсу от всех процессов из списка процессов-претендентов на доступ к разделяемому ресурсу; если доступ к разделяемому ресурсу перестал быть необходимым, делают запрос из процесса-клиента в средстве блокирования на освобождение разделяемого ресурса.

Патент № 2658894

Способ управления доступом к данным с защитой учетных записей пользователей

Авторы:
Иванова Е.В.,
Копелев М.А.

Заявка РФ
№ 2017126662
от 26.07.2017 г.

Изобретение относится к области информационной безопасности. Технический результат – обеспечение децентрализованного контроля над правами доступа к данным. Способ заключается в том, что со стороны администратора защищаемого объекта с данными объекта генерируют уникальный идентификатор ИД защищаемого объекта, генерируют случайный симметричный ключ КА администрирования объекта, получают симметричный ключ шифрования данных объекта КО путем вычисления производного ключа от ключа КА с использованием идентификатора ИД в качестве модификатора, зашифровывают данные защищаемого объекта на ключе КО, получая зашифрованные данные ШДО, формируют блок данных служебной информации, содержащий идентификатор ИД, сведения о защищаемом объекте и спецификацию использующихся криптографических функций, формируют список доступа к объекту, состоящий из учетных записей пользователей, которым предоставляется доступ к защищаемому объекту, причем по крайней мере одна из учетных записей принадлежит администратору объекта, выполняя для каждой учетной записи следующие действия: получают у выбранного пользователя, имеющего асимметричную пару ключей в составе открытого ключа и секретного ключа, его открытый ключ, генерируют случайное число, принимают его в качестве временного идентификатора, формируют идентификатор учетной записи, принимая в качестве его значения временный идентификатор, генерируют случайную асимметричную пару ключей в составе открытого ключа и секретного ключа, генерируют случайный симметричный ключ КЗ учетной записи, вычисляют общий симметричный ключ КЗП из секретного ключа и открытого ключа, зашифровывают ключ КЗ на ключе КЗП, получая зашифрованный ключ, принимают решение о наделении пользователя полномочиями администратора, формируют значение параметра, характеризующего наличие у пользователя полномочий администратора, формируют блок данных, зашифровывают его на ключе КЗ, получая зашифрованные данные, формируют текстовое описание учетной записи выбранного пользователя, формируют блок проверочных данных администрирования, зашифровывают его на ключе КА, получая зашифрованные данные, формируют учетную запись выбранного пользователя, сохраняют совместно зашифрованные данные ШДО, служебную информацию, список доступа к объекту.

Патент № 2715293

Способ защиты данных в вычислительной системе

Автор:
Елфимов А.В.

Заявка РФ
№ 2019121713
от 11.07.2019 г.

Изобретение относится к области защиты данных. Техническим результатом является повышение защищенности о т несанкционированного доступа к файлам внутри области защищенного хранения файлов. Способ защиты данных в вычислительной системе заключается в том, что формируют ключ для шифрования данных в области защищенного хранения файлов; вычисляют значение хэш-функции для ключа; формируют метаданные, содержащие значение хэш-функции; сохраняют метаданные; зашифровывают данные в файлах области защищенного хранения файлов с использованием ключа; если получают запрос пользовательского приложения, включающий ключ, на чтение данных файла из области защищенного хранения файлов, то с использованием управляющего приложения получают ключ для доступа к области защищенного хранения файлов; вычисляют значение хэш-функции для ключа; если значение хэш-функции ключа совпадает со значением хэш-функции ключа, сохраненным в метаданных, то определяют наличие доступа прикладной программы, иначе - отсутствие доступа; если у пользовательского приложения отсутствует доступ, то возвращают данные без расшифрования; если у пользовательского приложения имеется доступ, то расшифровывают данные с использованием ключа; возвращают расшифрованные данные пользовательскому приложению.

Интернет вещей (Internet of Things, IoT)

Российский патент

Патент РФ № 2703329

Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности из локальной сети и предотвращения исходящих от них распределенных сетевых атак

Авторы:
Гурина А.О.,
Елисеев В.Л.

Заявка РФ
№ 2018142311,
от 30.11.2018 г.

Изобретение относится к области вычислительной техники. Техническим результатом является обнаружение несанкционированного использования сетевых устройств ограниченной функциональности из локальной сети и предотвращение исходящих от них распределенных сетевых атак на сетевые узлы в глобальной сети непосредственно в источнике атаки. Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности и предотвращения распределенных атак заключается в том, что устройства ограниченной функциональности отправляют в модуль анализа шлюза защищенное от подмены сообщение, содержащее собственный сетевой адрес, при обнаружении собственной аномальной активности; в модуле анализа проверяют, являются ли сообщения аутентичными; вычисляют параметр, характеризующий взаимосвязь между аутентичными сообщениями; проверяют в модуле анализа выполнение условия несанкционированного использования устройств ограниченной функциональности, и если условие выполнено, то формируют список сетевых адресов устройств ограниченной функциональности, для которых сделан вывод об их несанкционированном использовании, запрашивают у шлюза сетевой трафик перечисленных в списке устройств, анализируют сетевую активность перечисленных в списке устройств на предмет признаков исходящей распределенной атаки, в случае обнаружения которой формируют правила фильтрации сетевого трафика, применяют правила фильтрации в шлюзе, предотвращая скоординированную распределенную сетевую атаку со стороны сетевых устройств ограниченной функциональности до тех пор, пока в модуле анализа шлюза выполняется условие несанкционированного использования устройств.

ПРОМЫШЛЕННЫЕ ОБРАЗЦЫ

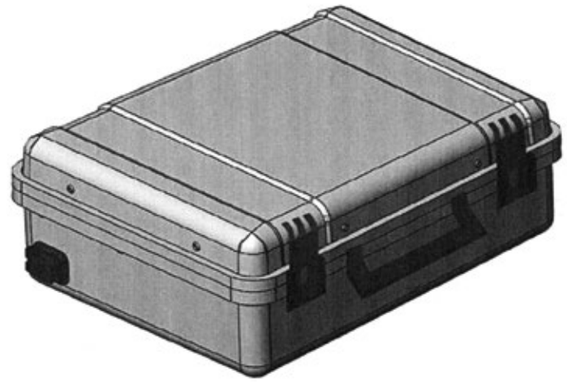
Российские патенты

Патент РФ № 117152

Переносной программно-аппаратный комплекс защиты информации

Авторы:
Чефранова А.О.,
Кузьмин О.В.

Заявка РФ
№ 2019500991
от 14.03.2019 г.

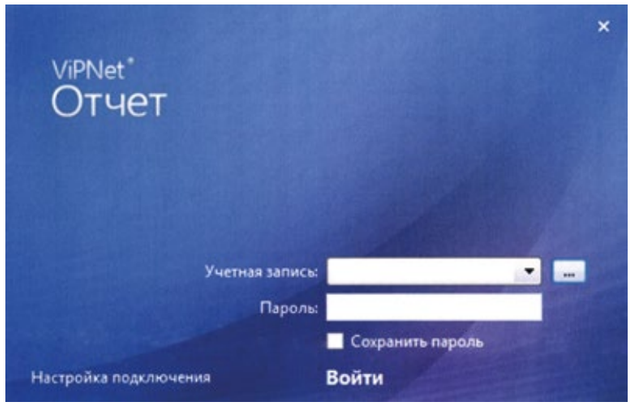


Патент РФ № 91468

Пользовательский интерфейс экрана аутентификации для специализированного программного обеспечения

Автор:
Кийко А.С.

Заявка РФ
№ 2013500629
от 26.02.2013 г.



Патент РФ № 91298

Значок для графического интерфейса

Автор:
Кийко А.С.

Заявка РФ
№ 2014500228
от 27.01.2014 г.

Патент РФ № 91297

Значок для графического интерфейса

Автор:
Кийко А.С.

Заявка РФ
№ 2014500229
от 27.01.2014 г.

Патент РФ № 91638

Значок для графического интерфейса

Автор:
Кийко А.С.

Заявка РФ
№ 2014500230
от 27.01.2014 г.

ПОЛЕЗНЫЕ МОДЕЛИ

Российский патент

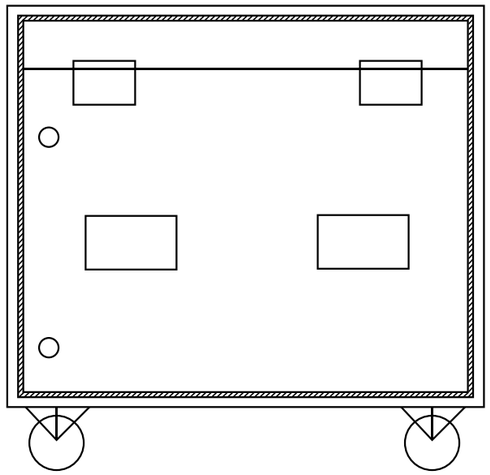
Патент РФ № 175672

Мобильный контейнер-составной элемент стенда

Автор:
Мелиссин А.В.

Заявка РФ
№ 2017105146
от 17.02.2017 г.

Предполагаемая полезная модель относится к области экспозиционного и транспортировочного оборудования, в частности к устройствам выставочных стендов, и может быть использована для демонстрации и транспортировки различных видов товаров или экспонатов. Техническим результатом является расширение эксплуатационных возможностей и повышение удобства эксплуатации. Для этого предложен мобильный контейнер-составной элемент стенда, который включает: корпус, имеющий боковые стенки и дно; фиксаторы в верхней части боковых стенок для крепления съемной крышки; крепежные узлы, расположенные на одной боковой стенке вдоль вертикального ребра корпуса и не выступающие за пределы боковой стенки; съемную крышку, имеющую боковые стенки и дно, причем у двух противоположных боковых стенок ширина равна высоте корпуса; крепежные узлы, установленные на двух противоположных боковых стенках и не выступающие за пределы боковой стенки; фиксаторы в нижней части для крепления съемной крышки к корпусу; причем количество крепежных узлов съемной крышки в два раза больше количества крепежных узлов корпуса, а крепежные узлы крышки выполнены с возможностью соединения с крепежными узлами корпуса. Кроме того, в контейнере на боковых стенках съемной крышки могут быть установлены дополнительные крепежные узлы, обеспечивающие соединение одинаковых съемных крышек между собой со стороны боковых стенок. Помимо этого, в контейнере внутренняя поверхность корпуса и съемной крышки может иметь слой из ударопоглощающего материала. Для удобства перемещения в контейнере на дне корпуса снаружи могут быть установлены съемные вращающиеся колеса. Также для удобства перемещения (переноски) в контейнере на боковых стенках корпуса могут быть установлены складные ручки. Расширение эксплуатационных возможностей предложенного контейнера расширяются за счет: 1) увеличения внутреннего полезного объема контейнера; 2) возможности формировать стенд большого размера, при использовании нескольких контейнеров. Повышение удобства эксплуатации предложенного контейнера достигается за счет: 1) отсутствия отдельных элементов конструкции, используемых при сборке стенда и размещаемых внутри контейнера; 2) упрощения процесса сборки и разборки конструкции.



Патент РФ № 215524

Устройство для защиты оптических систем от мощного лазерного излучения

Авторы:
Алферов С.В.,
Бугай К.Е.,
Паргачев И.А.

Заявка РФ
№ 2022123786
от 07.09.2022 г.

Предполагаемая полезная модель относится к области защиты оптических систем, в том числе волоконно-оптических систем с квантовым распределением ключей, от мощного лазерного излучения, а также от атак с лазерным повреждением компонентов. Техническим результатом является:

1. упрощение конструкции

2. упрощение настройки и эксплуатации

3. снижение габаритных размеров

4. обеспечение возможности использования в волоконно-оптических системах

Для этого предлагается устройство для защиты оптических систем от мощного лазерного излучения, содержащее волоконно-оптический светоделитель с коэффициентом деления света, равным 50/50; зеркало с заданными коэффициентом отражения и пороговой мощностью разрушения, установленное на первом выходе светоделителя; поглотитель света, установленный на втором выходе волоконно-оптического светоделителя. Дополнительно устройство может включать детектор LDA атаки и электронное устройство управления, соединенное с детектором.