(19) Евразийское патентное ведомство

(11) 036066 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2020.09.22

(21) Номер заявки
201792664

(22) Дата подачи заявки
2016.08.13

(51) Int. Cl. ***H04L 9/08*** (2006.01)

(54) СПОСОБ И СИСТЕМА ГЕНЕРИРОВАНИЯ КОДА ДЛЯ ИДЕНТИФИКАЦИИ ПРОДУКТОВ, ВЫРАБАТЫВАЕМЫХ НА ПРОИЗВОДСТВЕ

(31) **62/204,753**
(32) **2015.08.13**
(33) **US**
(43) **2018.07.31**
(86) **PCT/EP2016/069316**
(87) **WO 2017/025645 2017.02.16**

(71)(73) Заявитель и патентовладелец:
ИНЕКСТО СА (CH)

(72) Изобретатель:
Фраде Эрван, Шателен Филипп, Шане Патрик (CH)

(74) Представитель:
Медведев В.Н. (RU)

(56) US-A1-2013297929
US-A1-2013099901
GIUSEPPE ATENIESE ET AL.: "Untraceable RFID tags via insubvertible encryption", PROCEEDINGS OF THE 12TH. ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY. (CCS'05). ALEXANDRIA, VA, NOV. 7-11, 2005; [ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY], NEW YORK, NY: ACM, US, 7 November 2005 (2005-11-07), pages 92-101, XP058245589, DOI: 10.1145/1102120.1102134 ISBN: 978-1-59593-226-6 the whole document

(57) Изобретение и устройство относятся к реализации методики шифрования буквенно-числовых символов для маркировки продукции защищенными идентификационными кодами и проверки этих кодов, которые возможно использовать для проверки правильности уплаты налогов с доходов, проверки объемов производства и аутентификации изделий.

036066 B1

036066 B1

По данной заявке испрашивается приоритет предварительной патентной заявки США № 62/204753, поданной 13 августа 2015 г., содержание которой включено сюда посредством ссылки в полном объеме.

Настоящее изобретение относится, в целом, к методам шифрования буквенно-числовых символов в связи с маркировкой продуктов защищенными идентификационными кодами и проверкой этих кодов и также к системам и способам управления распространением защищенных инструкций конфигурации производства и генерирования защищенных идентификаторов продукта.

Существующие способы идентификации продукта обычно предусматривают нанесение уникального идентификатора на продукт во время упаковки. Эти системы не масштабируются эффективно в организациях, имеющих множественные производственные объекты, или на производственных линиях, способных упаковывать с очень высокой скоростью. Дополнительно существующие способы идентификации не обеспечивают достаточной защиты, поскольку они не связаны с защищенными инструкциями конфигурации производства и не несут дополнительной информации о продукте, полезной для регулирующих органов и торговых организаций.

Существует необходимость в улучшенных способе и устройстве для безопасного управления и авторизации производства изделий производства, а также маркировки изделий производства защищенными идентификаторами продукта, в частности, тех, которые можно использовать для проверки правильности уплаты налога с доходов, проверки объема производства и аутентификации изделий производства.

Существующие системы шифруют буквенно-числовые символы, используемые в качестве идентификаторов продукта на посимвольной основе. Это ограничивает эти системы, например, числами, в целом, от 0 до 9 или, если используются только буквы, ограничивает системы количеством букв используемого алфавита, умноженного на два (включающего в себя заглавные буквы и строчные буквы). Это изобретение разрешает эти недостатки.

Нижеследующие варианты осуществления изобретения являются иллюстративными и не призваны ограничивать объем изобретения. Хотя были описаны один или более вариантов осуществления настоящего изобретения, различные их изменения, добавления, перестановки и эквиваленты включены в объем изобретения. Нижеследующее описание вариантов осуществления приведено со ссылкой на прилагаемые чертежи, которые образуют его часть, где в порядке иллюстрации изображены конкретные варианты осуществления заявленного изобретения. Следует понимать, что можно использовать другие варианты осуществления, и что возможны изменения или альтернативы, например структурные изменения. Такие варианты осуществления, изменения или альтернативы не выходят за рамки объема заявленного изобретения. Хотя нижеследующие этапы могут быть представлены в определенном порядке, в ряде случаев упорядочение может изменяться таким образом, что определенные входные сигналы обеспечиваются в разные моменты времени или в другом порядке без изменения функции описанных систем и способов. Различные вычисления, которые описаны ниже, например, осуществляемые в процедурах инициализации кода, генерации и аутентификации, не обязаны осуществляться в раскрытом порядке, и легко реализовать другие варианты осуществления, где используются альтернативные упорядочения вычислений. Помимо переупорядочения вычисления также можно разложить на подвычисления с теми же результатами.

Варианты осуществления изобретения будут описаны в порядке примера со ссылкой на прилагаемые чертежи, на которых

фиг. 1 - иллюстративный способ вычисления идентификатора машины;

фиг. 2 - иллюстративный способ обфускации данных;

фиг. 3 - иллюстративный способ инициализации кода;

фиг. 4 - иллюстративный способ генерации кода;

фиг. 5 - иллюстративный способ авторизации кода.

Согласно варианту осуществления изобретения для способа обфускации данных, хранящихся в сети, способ содержит задание и сохранение информации, описывающей состояние вычислительной машины, как номера машины (MNUM), причем информация, описывающая состояние, включает в себя количество основ, содержащих информацию, описывающую состояние; генерирование машинного защищенного уникального идентификатора продукта (MSUPI) в качестве обратимого математического преобразования машинного уникального идентификатора продукта (MUPI) на основании информации, описывающей состояние вычислительной машины, причем этап вычисления MSUPI содержит задание количества этапов равным imax, для каждого этапа генерирование первого случайного числа в качестве ключа обфускации для генерации кода ($CGOK_{i,1}$) и второго случайного числа в качестве ключа обфускации для генерации кода ($CGOK_{i,2}$), причем генерирование содержит вычисление первого случайного числа ($CGOK_{i,1}$), взаимно простого с числом, основанным на информации, описывающей состояние вычислительной машины (MNUM); вычисление второго случайного числа ($CGOK_{i,2}$), имеющего равный или меньший битовый размер, как (MNUM); задание $m_{0,2}$=MUPI; вычисление для каждого элемента i от i=1 до imax - 1: $m_{i,1}=(m_{i-1,2}\times CGOK_{i,1}) \bmod (MNUM)$; $m_{i,2}=(m_{i,1} \bmod CGOK_{i,2})$; если $(m_{i,2} > MNUM) \rightarrow m_{i,2}=m_{i,1}$; задание $MSUPI=m_{imax,2}$; и сохранение машинного защищенного уникального идентификатора продукта (MSUPI) в электронном хранилище данных. Вышеописанный вариант осуществления, а также описанные здесь альтернативные и дополнительные варианты осуществления можно реализовать в ком-

пьютерно-реализуемом изобретении, компьютерной системе или компьютерном носителе данных.

Согласно альтернативному или дополнительному варианту осуществления информация, описывающая состояние вычислительной машины, содержит комбинацию информации времени и номера продукта. Согласно альтернативному или дополнительному варианту осуществления информация времени включает в себя юлианский год, юлианский день, производственный час и производственную минуту. Согласно альтернативному или дополнительному варианту осуществления информация, описывающая состояние, включает в себя значение инкрементного счетчика, сбрасываемого на периодической основе. Согласно альтернативному или дополнительному варианту осуществления число, основанное на информации, описывающей состояние вычислительной машины, вычисляется как 10×366×24×60×временной идентификатор. Согласно альтернативному или дополнительному варианту осуществления временной идентификатор задается как целое число 2210. Согласно альтернативному или дополнительному варианту осуществления защищенный уникальный идентификатор продукта (SUPI), 12-символьный буквенно-числовой код, получается таким образом, что SUPI=(p×m) mod (MNUM×mNoise×RunLim).

Согласно альтернативному или дополнительному варианту осуществления для генерирования кода для безопасной идентификации продуктов, вырабатываемых на производственном объекте, способ содержит электронный прием данных конфигурации из электронного хранилища данных; электронное хранение данных конфигурации для производственного периода, причем данные конфигурации для производственного периода задают параметры, используемые при производстве продуктов; передачу данных конфигурации на модуль авторизации; на модуле авторизации определение, авторизован ли производственный период; генерирование подтвержденных данных конфигурации, содержащих ключ, представление множества авторизованных идентификаторов продукта и маркер безопасности (security token); передачу подтвержденных данных конфигурации на модуль подписи; на модуле подписи подписание подтвержденных данных конфигурации; на модуле идентификации прием запроса идентификатора продукта и генерирования идентификатора продукта в ответ на запрос, причем генерирование идентификатора продукта осуществляется путем задания и сохранения информации, описывающей состояние вычислительной машины, как номера машины (MNUM), причем информация, описывающая состояние, включает в себя количество основ, содержащих информацию, описывающую состояние; генерирования машинного защищенного уникального идентификатора продукта (MSUPI) в качестве обратимого математического преобразования машинного уникального идентификатора продукта (MUPI), на основании информации, описывающей состояние вычислительной машины, причем этап вычисления MSUPI содержит задание количества этапов равных imax, для каждого этапа генерирование первого случайного числа в качестве ключа обфускации для генерации кода ($CGOK_{i,1}$) и второго случайного числа в качестве ключа обфускации для генерации кода ($CGOK_{i,2}$), причем генерирование содержит вычисление первого случайного числа ($CGOK_{i,1}$), взаимно простого с числом, основанным на информации, описывающей состояние вычислительной машины (MNUM); вычисление второго случайного числа ($CGOK_{i,2}$), имеющего равный или меньший битовый размер, как (MNUM); задание $m_{0,2}=m_{i-1,2}$; вычисление для каждого элемента i от i=1 до imax - 1: $m_{i,1}=(m_{i-1,2}\times CGOK_{i,1}) \bmod (MNUM)$; $m_{i,2}=(m_{i,1} \bmod CGOK_{i,2})$; если [$m_{i,2}$ > MNUM) $\rightarrow m_{i,2}=m_{i,1}$; задание $MSUPI=m_{imax,2}$; сохранение машинного защищенного уникального идентификатора продукта (MSUPI) в электронном хранилище данных в качестве идентификатора продукта; передачу идентификатора продукта от модуля идентификации на модуль подписи; снабжение идентификатора продукта цифрой подписью на модуле подписи и передачу идентификатора продукта, снабженного цифрой подписью, на модуль принтера.

Согласно альтернативному или дополнительному варианту осуществления способ дополнительно содержит электронный прием данных конфигурации из электронного хранилища данных; электронное хранение данных конфигурации для производственного периода, причем данные конфигурации для производственного периода задают параметры, используемые при производстве продуктов; передачу данных конфигурации на модуль авторизации; на модуле авторизации определение, авторизован ли производственный период; генерирование подтвержденных данных конфигурации, содержащих ключ, представление множества авторизованных идентификаторов продукта и маркер безопасности; передачу подтвержденных данных конфигурации на модуль подписи; и на модуле подписи подписание подтвержденных данных конфигурации.

Согласно альтернативному или дополнительному варианту осуществления запрашивается диапазон идентификаторов. Согласно альтернативному или дополнительному варианту осуществления способ дополнительно содержит определение, авторизованы ли данные конфигурации для производственного периода; если производственный период авторизован, генерирование маркера безопасности и связывание маркера с данными конфигурации; и снабжение данных конфигурации цифровой подписью путем генерирования цифровой подписи и связывания цифровой подписи с данными конфигурации.

Согласно альтернативному или дополнительному варианту осуществления машинный уникальный идентификатор продукта (MUPI) преобразуется без заполнения машинного уникального идентификатора продукта (MUPI) таким образом, что битовая длина машинного уникального идентификатора продукта (MUPI) равна битовой длине машинного защищенного уникального идентификатора продукта (MSUPI).

В альтернативном или дополнительном варианте осуществления способ проверки защищенного машинного уникального идентификатора продукта содержит модуль проверки принимает MSUPI для проверки; назначение MSUPI как $m_{0,2}$; модуль проверки извлекает первое случайное число $CGOK_{i,1}$ и второе случайное число $CGOK_{i,2}$, и imax, связанный с извлеченными случайными числами и принятым MSUPI; вычисление для каждого элемента i от i=1 до imax - 1: $m_{i,1}=(m_{i-1,2} \bmod CGOK_{i,2})$; если ($m_{i,2} >$ MNUM) $\rightarrow m_{i,1}=m_{i-1,2}$; $m_{i,2}=(m_{i,1}\times CGOK^{-1}{}_{i,1}) \bmod (MNUM)$; $m_{cg}=m_{imax,2}$; и проверку $MUPI=m_{cg}/mNoise$ и значения шума=$m_{cg} \bmod mNoise$, где MUPI основан на информации, описывающей состояние вычислительной машины.

Согласно альтернативному или дополнительному варианту осуществления машинный защищенный уникальный идентификатор продукта (MSUPI) преобразуется без заполнения машинного уникального идентификатора продукта (MUPI) таким образом, что битовая длина машинного уникального идентификатора продукта (MUPI) равна битовой длине машинного защищенного уникального идентификатора продукта (MSUPI). Согласно альтернативному или дополнительному варианту осуществления авторизации, принимаемые от модуля авторизации, могут передаваться на модуль проверки, что позволяет затем обрабатывать запросы проверки в отношении этих авторизаций, и при этом данные, передаваемые на модуль проверки, могут включать в себя машинный защищенный уникальный идентификатор продукта (MSUPI).

Описанные способы могут использоваться помимо или вместо шифрования и могут использоваться как способ обфускации чисел с использованием заданной основы. Способ может использоваться для любой конечной заданной основы. Способы могут использоваться на заранее заданной числовой основе, например от 0 до 9 при использовании чисел или от 0 до F в шестнадцатеричной системе. Этот способ работает на заданной основе, которая не ограничивается количеством символов, используемых в нормальном диапазоне символов для этой основы.

Для этого способа задается группа, из которой будут выбираться буквенно-числовые символы; каждая из этих групп называется основой. Примером будет $0 \rightarrow 52$ (включая 0 и 52). Каждое из этих чисел будет единичным "символом", который будет шифроваться. Альтернативно, можно задавать основу $0 \rightarrow 932$. Альтернативы допускают комбинацию букв и чисел. В порядке неограничительных примеров это может быть английский алфавит, кириллический алфавит или любой другой алфавит помимо чисел. Система позволяет задавать основу с использованием любого конечного набора или комбинацию наборов в качестве основ для каждого из тех, которые подлежат отсчету в качестве единичного "символа" при обфускации числа. Любой набор буквенно-числовых символов может использоваться при условии, что числовое значение назначается для каждого символа. Это может использоваться для объединения, например, наборов шестнадцатеричных чисел и алфавита.

Каждому символу назначается числовое значение с минимальным значением и максимальным значением, и затем они объединяются. Например, в случае комбинации шестнадцатеричных чисел и финского алфавита, который имеет 29 букв, можно назначать значения 0-15 для шестнадцатеричных чисел, таким образом, что 15 соответствует 0, 14 соответствует 1, вплоть до 1 соответствует B, и 0 соответствует A. Для финского алфавита, аналогично, соответствующие числа могут быть 1 с A до 29 с A (предполагая, что используются только заглавные буквы) или можно назначать 1 с L и отсчет, где 18 соответствует A, 19 соответствует A, и 29 назначается K.

Назначение не обязательно является линейным при условии, что сохраняется, какой символ или какое число назначается какому числовому значению. Это также может осуществляться динамически, также если желательна дополнительная обфускация, при условии, что назначения записываются для дальнейшего дешифрования. С примером использования шестнадцатеричной системы и 29-символьного алфавита диапазон может быть MAX=Hex(max) * Alphabet(max)+Alphabet(max), тогда как минимум MIN=Hex(min) * Alphabet(min)+Alphabet(min). В обоих этих примерах существует две основы. Этот пример предусматривает основу диапазона [1, 464]. Дело в том, что числа алфавита принимают значения от 1 до 29, а не от 0 до 28 для 29 символов. Альтернативно, одни и те же наборы могут объединяться как MAX=Alphabet(max) * Hex(max) +Hex(max) и MIN=Alphabet (min) * Hex(min)+Hex(min) и обеспечивать основу диапазона [0, 450]. Таким образом, с использованием одних и тех же компонентных основ можно создавать различные диапазоны для лучшей обфускации чисел, используемых в процессе.

В другом примере, где нужно создавать основу диапазона, основа диапазона может описывать состояние вычислительной машины, например комбинацию временных и числовых идентификаторов. В этом примере основу диапазона можно создавать с использованием множественных основ. В этом примере она состоит из пяти разных основ и является комбинацией усеченного юлианского года (JY) [0-10], объединенного с юлианской датой (JD) [0-366], часом дня (HR) [0-24], минутой часа (Mins) [0-60] и временным идентификатором (TI) [0-2210], дополнительным инкрементным счетчиком, сбрасываемым каждую минуту. Количество основ, которые используются для создания основы диапазона, задается как imax. Пример этого варианта осуществления представлен на фиг. 1.

Диапазон определяется путем преобразования буквенно-числовых символов в единичный диапазон. Например, в этом случае годы преобразуются в дни, затем полное количество дней в часы, полное коли-

чество часов в минуты и затем в инкрементные счетчики. Для достижения этого предполагается использовать максимальные количества каждого для получения верхней границы диапазона и минимальные количества каждого для определения нижней границы диапазона. Например, максимальное значение MAX=(((JY(max) * JD(max)+JD(max)) * HR(max)+HR(max)) * Mins(max)+Mins(max)) * TI(max)+ TI(max). Минимум диапазона равен MIN=(((JY(min) * JD(min)+JD(min)) * HR(min)+HR(min)) * Mins(min)+Mins(min)) * TI(min)+TI(min). В этом примере диапазон составляет [0, 12815659610].

С использованием диапазонов вышеприведенного примера можно задавать ашинно-уникальный идентификатор продукта (MUPI). Задание должно производиться в пределах значения таким образом, что MUPI=(((JY * JD(max)+JD) * HR(max)+HR) * Mins (max)+Mins) * TI(max)+ TI. Для лучшей обфускации числа можно добавлять случайный компонент. Это случайное число можно генерировать любым образом при условии, что известен диапазон случайного числа. Это случайное число может быть цифровой подписью, которая генерируется с использованием наборов секретного и динамического ключей. Это может осуществляться, например, с использованием кода аутентификации сообщения хэширования ключа. Например, MUPI, объединенный с динамическим ключом при использовании вырезающей функции, даст секретный ключ, и MUPI, объединенный с секретным ключом с использованием хэш-функции, будет использоваться для вычисления значения шума. Это позволяет задавать значение m_{cg}=MUPI * mNoise+шум. Это значение MUPI подлежит шифрованию с использованием ключа обфускации для генерации кода (CGOK).

Можно использовать два значения CGOK, где первый $CGOK_{i,1}$ является числом, взаимно простым с максимальным значением диапазона для MUPI. MNUM=JY(max) * JD(max) * HR(max) * Mins (max) * TI(max), которое в этом примере равно 10*366*24*60*2210. Второй $CGOK_{i,1}$, $CGOK_{i,2}$, является числом в диапазоне [MIN, MNUM-1] с битовым размером, меньшим или равным $CGOK_{i,1}$. Для проведения вычислений, $m_{0,2}$ задается равным MUPI и задание MSUPI равным максимальным элементом $m_{i,2}$, который равен $m_{imax,2}$. Если существуют 8 основ, содержащих основу диапазона, то элемент MSUPI=$m_{8,2}$. Затем MSUPI может объединяться с ID генератора кода, CGID. Это осуществляется сдвигом CGID на размер MSUPI таким образом, что m=CGID×(MNUM×mNoise)+MSUPI, где mNoise является максимальным возможным значением шума. Окончательный код, защищенный уникальный идентификатор продукта (SUPI), получается путем шифрования m с использованием глобального обфускационного кода, p, который может быть одинаковым для всех генераторов кода. SUPI задается как (p×m) mod (MNUM×mNoise×RunLim) и SUPI преобразуется в 12-символьный буквенно-числовой код. Пример этого варианта осуществления представлен на фиг. 2.

Способ обфускации является обратимым для проверки процесса и продуктов. Это осуществляется путем выполнения процесса обфускации в обратном порядке. Это возможно, поскольку CGOK является взаимно простым с MNUM, и используется функция Эйлера относительно MNUM. Это позволяет вычислять MUPI и MNUM из MSUPI. Таким образом, дешифрование SUPI осуществляется на следующих этапах, m=($\rho^{16}\times^{34^{11}-1}$×SUPI) mod (MNUM×mNoise×RunLim). Из m можно извлечь MSUPI и CGID, MSUPI=m mod (MNUM×mNoise) и CGID=m/(MNUM×mNoise). Таким образом, деобфускация MSUPI осуществляется с использованием обратной величины CGOK. Поскольку CGID известен, его можно использовать для извлечения правильных CGOK из базы данных. MUPI=m_{cg}/mNoise, и значение шума также можно проверять, поскольку шум=m_{cg} mod mNoise.

Иллюстративная реализация.

В другом аспекте изобретения описанные здесь способы могут осуществляться в вычислительном окружении, как описано здесь, с использованием исполнимых инструкций. Ниже приведен пример набора инструкций для генерирования идентификатора продукта, защищенного посредством обфускации.

```
//codeGenID
int id=122334;
int noise=345;
var gr=new int[12];
int noiseSize=1;
for (int i=0; i < 12; i++)
{
gr[i]=(id % numberOfGroups);
noiseSize=noiseSize * Groups[id % numberOfGroups].Length;
id=id/numberOfGroups;
}
var usedNoise=noise % noiseSize;
StringBuilder stb=new StringBuilder(12);
for (int i=0; i < 12; i++)
{
stb.Append(Groups[gr[i]][noise % Groups[gr[i]].Length]);
noise=noise/Groups[gr[i]].Length;
}
Console.WriteLine("Code=" +stb.ToString());
string code="GFL1BARARARA";
id=0;
usedNoise=0;
int carryOver=0;
for (int i=11; i >= 0; i--)
{
var ch=code[i];
for (int j=0; j < numberOfGroups; j++)
{
var index=Groups[j].IndexOf(ch);
if (index >= 0)
{
id=id * numberOfGroups+j;
usedNoise=usedNoise * carryOver+index;
carryOver=Groups[j].Length;
}
}
}
Console.WriteLine("Id="+id);
```

Алгоритмы симметричного ключа, например 3DES, AES и пр., действуют на блоках входных данных. Для этого длина входных данных должна быть в точности равна длине блока или кратному целому длины блока для этого алгоритма. В примере 128-битового шифрования AES длина блока может быть

равна 128 битам, т.е. 16 байтам. Шифруемые входные данные могут иметь размер, например, 20 байтов, на 4 байта больше длины блока в этом примере. Чтобы длина входных данных была кратна длине блока, входные данные необходимо снабжать заполнением. В этом случае заполнение вычисляется следующим образом: 20 байтов требует (16-(20-16))=12 байтов заполнения. Таким образом, это заполнение может значительно увеличивать размер зашифрованного набора данных, аналогично увеличению объема физического хранилища данных, необходимого для хранения зашифрованных данных. Согласно вышеприведенной иллюстративной реализации способ обфускации, отвечающий изобретению, может быть сконфигурирован для обфускации данных, например идентификаторов продукта, без необходимости в заполнении входных данных идентификатора продукта.

Объединение с защищенными производственными системами.

Вышеописанные системы и способы для обфускации данных выгодно использовать совместно с системами для аутентификации производства продуктов. В другом аспекте изобретения предусмотрен способ аутентификации производства продуктов, причем способ включает в себя электронное хранение данных конфигурации для производственного периода, причем данные конфигурации для производственного периода задают параметры, используемые при производстве продуктов; определение, авторизованы ли данные конфигурации для производственного периода; если производственный период авторизован, генерирование маркера безопасности и связывание маркера с данными конфигурации; и снабжение данных конфигурации цифровой подписью путем генерирования цифровой подписи и связывания цифровой подписи с данными конфигурации; прием данных конфигурации, снабженных цифровой подписью, и цифровой подписи на продукционной машине; на продукционной машине проверку цифровой подписи, связанной с данными конфигурации, снабженными цифровой подписью; вычисление набора защищенных идентификаторов продукта на основании данных конфигурации, снабженных цифровой подписью; выработку продуктов в течение производственного периода согласно данным конфигурациям, снабженным цифровой подписью; и печать набора защищенных идентификаторов продукта на продуктах согласно данным конфигурациям, снабженным цифровой подписью.

Используемый здесь термин "сущность" может означать i) лицо, например потребителя продукта; ii) группу, например группу людей, имеющих общий интерес, например, розничных торговцев; iii) вычислительное устройство; iv) вычислительный узел в сетевой системе; v) место хранения, например запоминающее устройство, где хранится документ; vi) виртуальную точку в сети, например представляющую бизнес-функцию коммерческого предприятия и пр. Дополнительно сущность может представлять точку в последовательности операций, например, для авторизации, которая может осуществляться лицом, отвечающим за этот аспект последовательности операций, или вычислительным устройством, которое обеспечивает автоматизированную обработку. Термин "сущность" не предполагает ограничения каким-либо из этих примеров и может распространяться на другие ситуации, согласующиеся с описанными здесь принципами.

Модули системы.

Ниже описаны различные модули. Любые модули могут быть физически совмещены или располагаться на удалении друг от друга. Дополнительно любые модули могут быть логически или физически объединены в единый модуль без отклонения от объема изобретения.

Модуль управления.

Согласно фиг. 3 модуль управления (также известный как "оркестратор") (110) может принимать входной сигнал от любого другого модуля или внешнего источника и может выдавать инструкции на другие модули системы на основании заранее сконфигурированных программ и/или вводов оператора. Он также может генерировать итоговую сводку состояния системы.

Сигнал, поступающий на модуль управления, может включать в себя некоторые или все данные (105) конфигурации. Подаваемые данные конфигурации могут указывать некоторые или все параметры, включающие в себя, но без ограничения, машину для производства, производственную линию, фабрику, вырабатываемый продукт и объем продукта. Данные конфигурации могут указывать, какие предметы (например, продукты) подлежат маркировке защищенными идентификаторами, и как эти предметы могут вырабатываться. Данные конфигурации могут указывать диапазон продуктов, например начальный и конечный идентификаторы продукта. В некоторых вариантах осуществления диапазон может быть набором идентификаторов продукта. Данные конфигурации могут предоставляться оператором системы или динамически или автоматически генерироваться. Данные конфигурации могут включать в себя дополнительные исполнимые инструкции или интерпретируемый алгоритм. Данные конфигурации могут базироваться на вводе оператора или выходном сигнале производственной системы или другой централизованной системы, предписывающей, как и что вырабатывать.

Модуль (110) управления может передавать данные конфигурации на любой модуль, в том числе, но без ограничения, модуль (130) авторизации, модуль (140) идентификации и модуль (145) подписи.

Модуль управления может запрашивать авторизацию от модуля авторизации для выполнения производственной операции. Этот процесс предусматривает передачу запроса (включающего в себя некоторые или все данные конфигурации) на модуль авторизации и прием подписанных или зашифрованных данных конфигурации. В некоторых вариантах осуществления модуль авторизации может возвращать

данные конфигурации на модуль управления, включающие в себя цифровую подпись, применяемую к этим данным конфигурации. Модуль авторизации определяет, авторизовать ли запрос от модуля управления на основании принимаемых им данных. Кроме того, информация, возвращаемая модулем авторизации, включенная в данные конфигурации, может использоваться для связывания генерируемых кодов с предоставленной авторизацией. Когда данные подписаны модулем авторизации, это предохраняет систему от изменения данных конфигурации. В порядке неограничительного примера изменение запроса на выработку одной марки вместо другой можно регулировать, разрешать или отклонять.

Авторизации, принятые от модуля авторизации, также могут передаваться на модуль проверки, что позволяет затем обрабатывать запросы проверки в отношении этих авторизаций. Данные, передаваемые на модуль проверки, могут включать в себя защищенный идентификатор, а также любые данные конфигурации. В некоторых примерах данные конфигурации, отправленные на модуль авторизации, могут включать в себя информацию диапазона продуктов.

Подписанные или подтвержденные данные конфигурации могут представлять собой некоторые или все из набора входных параметров модуля управления, проверенных и подтвержденных модулем авторизации, что остается в силе в ходе производства. Маркер безопасности может быть получен от модуля авторизации и/или из входного параметра модуля управления. Маркер безопасности может служить доказательством того, что идентификатор продукта соответствует подтвержденным данным конфигурации и, таким образом, авторизованному производству. Маркер безопасности может поступать на модуль подписи для генерирования подписи для единичного идентификатора продукта, или подписи единичного идентификатора продукта, или самого идентификатора продукта, или диапазона продуктов, или идентификаторов продукта. Маркер безопасности может представлять собой уникальный код, случайный код или псевдослучайный код. Маркер безопасности может быть образован любыми числовыми или буквенными символами или их комбинацией.

Модуль авторизации.

Модуль авторизации действует для подтверждения запросов авторизации для совершения действия в идентификационной системе. В некоторых вариантах осуществления он может действовать как менеджер лицензий.

Модуль авторизации может принимать данные конфигурации. Модуль авторизации также может принимать информацию диапазона и/или алгоритма. В некоторых вариантах осуществления модуль авторизации может принимать входные данные конфигурации от модуля управления. Выходной диапазон, в необязательном порядке, может идентифицировать диапазон продуктов, машины, фабрики, диапазоны или авторизованные объемы продукции. Выходной сигнал также может включать в себя информацию диапазона и/или включать в себя алгоритм, который содержит набор исполняемых или интерпретируемых инструкций, которые будут использоваться для генерирования маркера безопасности. Модуль авторизации может быть централизованным на уровне фабрики или децентрализованным на каждой производственной линии или комбинированным.

Модуль авторизации может хранить и/или генерировать один или более ключей шифрования. В некоторых вариантах осуществления, ключ, хранимый модулем авторизации, может быть личным открытым ключом шифрования согласно инфраструктуре открытого ключа (PKI). В некоторых вариантах осуществления на модуле авторизации хранится только копия личного ключа. В других вариантах осуществления модуль авторизации распределен по нескольким экземплярам, которые дублируют ключи между собой. В случае PKI, модуль авторизации может выводить подписанные данные конфигурации. В некоторых вариантах осуществления модуль авторизации может шифровать данные конфигурации и/или подписывать выходные данные конфигурации.

В некоторых вариантах осуществления система сконфигурирована таким образом, что только модуль авторизации может считывать защищенные входные параметры модуля управления, необходимые для генерации маркера безопасности. В некоторых вариантах осуществления ключ поступает на модуль авторизации из другого источника.

Модуль авторизации может быть реализован в виде аппаратного модуля безопасности (HSM) или физического вычислительного устройства другого типа, которое защищает и администрирует цифровые ключи для сильной аутентификации и обеспечения криптографической обработки. Функционал модуля авторизации может осуществляться компьютером со встроенной платой с помощью ключа шифрования или личного ключа PKI. Модуль может обладать такими особенностями, что попытки осуществления доступа к данным сделают их нечитаемыми или недоступными.

Если на модуль авторизации поступают диапазон и алгоритм, модуль авторизации может выводить идентификатор в диапазоне авторизации и маркер безопасности идентификатора. Например, выходной идентификатор может быть диапазоном от 0 до 1000 с маркером безопасности для каждого элемента в диапазоне.

Модуль авторизации может генерировать ключ из любого параметра, используемого в модуле управления. В некоторых вариантах осуществления модуль авторизации может генерировать или выводить ключ из существующего ключа из любого параметра, используемого в модуле управления таким образом, что только конкретный модуль авторизации может использовать этот ключ. Аппаратная и про-

граммная реализация этого метода открытого ключа может быть воплощена в асимметричной криптосистеме.

Модуль авторизации может выводить информацию, например данные конфигурации и, в необязательном порядке, один или более маркеров безопасности, с цифровой подписью, обеспеченной модулем подписи. Альтернативно, модуль авторизации может выводить данные конфигурации, зашифрованные в ключ, хранящийся в модуле авторизации. Выходной сигнал модуля авторизации может поступать на модуль управления.

Согласно варианту осуществления способ аутентификации производства продуктов включает в себя электронное хранение данных конфигурации для производственного периода, причем данные конфигурации для производственного периода задают параметры, используемые при производстве продуктов; определение, авторизованы ли данные конфигурации для производственного периода; если производственный период авторизован, генерирование маркера безопасности и связывание маркера с данными конфигурации; и снабжение данных конфигурации цифровой подписью путем генерирования цифровой подписи и связывания цифровой подписи с данными конфигурации; прием данных конфигурации, снабженных цифровой подписью, и цифровой подписи на продукционной машине; на продукционной машине проверку цифровой подписи, связанной с данными конфигурации, снабженными цифровой подписью; вычисление набора защищенных идентификаторов продукта на основании данных конфигурации, снабженных цифровой подписью; выработку продуктов в течение производственного периода согласно данным конфигурациям, снабженным цифровой подписью; и печать набора защищенных идентификаторов продукта на продуктах согласно данным конфигурациям, снабженным цифровой подписью.

В альтернативном или дополнительном варианте осуществления данные конфигурации представляют диапазон вырабатываемых продуктов. В альтернативном или дополнительном варианте осуществления данные конфигурации представляют диапазон продуктов, машины, фабрики, диапазоны или авторизованные объемы продукции. Альтернативные или дополнительные варианты осуществления могут включать в себя прием запроса проверки, причем запрос содержит идентификатор продукта и определение, авторизованы ли данные конфигурации для производственного периода, со ссылкой на менеджер лицензий. Альтернативные или дополнительные варианты осуществления могут включать в себя генерирование маркера безопасности для диапазона продуктов; и связывание маркера безопасности с диапазоном продуктов.

Модуль подписи.

Модуль подписи может принимать данные конфигурации, ключ авторизации, маркер безопасности или любую их комбинацию, а также уникальный идентификатор продукта, генерируемый модулем идентификации. В некоторых вариантах осуществления модуль подписи может принимать, кроме того, одну или более внутренних характеристик машины и/или продукта и/или характеристики экземпляра продукта. Модуль подписи может создавать цифровую подпись на основании некоторых или всех из этих входных сигналов, в целом именуемых здесь данными конфигурации.

Для генерирования цифровой подписи в некоторых вариантах осуществления сначала модуль подписи может генерировать сборник или другое представление данных конфигурации. В некоторых вариантах осуществления сборник может генерироваться путем вычисления значения криптографического хэша данных конфигурации согласно алгоритму цифровой подписи, обеспеченному модулем подписи, выполняющим алгоритм цифровой подписи. В порядке неограничительных примеров хэш можно вычислять согласно функциям MD5, SHA-1, SHA-2, SHA-3/Keccak. Затем сборник можно шифровать с использованием личного ключа, полученного модулем подписи для генерирования цифровой подписи.

В некоторых вариантах осуществления цифровая подпись может использовать технологию инфраструктуры открытого ключа (PKI) для установления аутентичности данных конфигурации. Системы PKI используют сертификаты и ключи для идентификации сущностей, индивидов или организаций. Модуль аутентификации использует личный ключ для подписания данных конфигурации и связывает данные конфигурации с сертификатом, включающим в себя открытый ключ, используемый модулем аутентификации.

Модуль получателя использует открытый ключ для проверки цифровой подписи и, таким образом, аутентичность подписанных данных конфигурации. Поддерживающие технологии могут использоваться для установления других признаков нерасторжения, например времени подписания и состояния ключей подписания. Открытый ключ может передаваться получающей сущности напрямую или путем публикации в онлайновом хранилище или реестре.

Модуль идентификации.

Модуль идентификации может принимать данные конфигурации и генерировать идентификаторы для маркируемых предметов. Модуль идентификации может принимать цифровую подпись, генерируемую модулем подписи, которая будет объединяться с уникальным идентификатором для генерирования составного уникального идентификатора.

Идентификаторы могут включать в себя или основываться на дате и/или времени производства маркируемого продукта и цифровой подписи, принятой от модуля подписи. В некоторых вариантах осуществления генерируемые защищенные идентификаторы могут быть уникальными или, по существу,

уникальными. В некоторых вариантах осуществления защищенные идентификаторы могут быть маркерами безопасности.

В случае диапазонов модуль идентификации может генерировать идентификатор диапазона и набор идентификаторов в генерируемом диапазоне.

Созданные идентификаторы могут выводиться на модуль управления печатью для направления печати на продукт или могут подвергаться дополнительной обработке для генерирования другого кода, который печатается на упаковке продукта.

Модуль проверки.

Согласно фиг. 5 модуль (150) проверки может принимать проверенные данные конфигурации и на основании этих подтвержденных данных конфигурации подтверждать запрос авторизации (305) для фабрики, машины, продукта или сообщаемого объема производства. Данные, поступающие на модуль проверки, могут включать в себя некоторые или все из проверенных данных конфигурации, выходного сигнала модуля подписи, идентификаторов, маркеров безопасности и/или информации диапазона. Модуль проверки может генерировать информацию для модуля авторизации с этими параметрами для проверки/подтверждения идентификатора продукта.

Модуль проверки может генерировать дешифрование (320) запроса, которое включает в себя один или более идентификаторов или диапазонов идентификаторов (315) и данные (310) подписи, включающие в себя один или более маркеров безопасности.

Если маркер безопасности поступает на модуль проверки, модуль проверки может возвращать информацию, относящуюся к авторизации, данным конфигурации и/или диапазонам. Если единичный маркер безопасности используется для диапазона продуктов, маркер безопасности может поступать на модуль проверки для проверки параметров, связанных с диапазоном продуктов, а не отдельными продуктами. Этот вариант осуществления может быть особенно полезен в отношении регулировки экспорта.

Процессы системы.

Инициализация идентификационного кода.

Инициализация идентификационного кода может осуществляться для подтверждения авторизации и параметров. В некоторых вариантах осуществления по причинам производительности это может осуществляться один раз в начале производства. Согласно фиг. 3 модуль (110) управления может осуществлять доступ к хранилищу (115) данных в отношении дополнительных параметров, или дополнительные параметры могут поступать на модуль. Параметры и данные конфигурации, один раз подписанные модулем (130) авторизации, образуют подтвержденные данные (135) конфигурации. Модуль управления принимает проверенные данные конфигурации, как описано выше, в ответ на его запрос модулю (130) авторизации.

Авторизация может быть авторизацией для выработки продукта или для маркировки продукта с определенным ID или обоих. Данные конфигурации и дополнительные параметры передаются на модуль авторизации и используются модулем авторизации для генерирования маркера безопасности. Модуль авторизации может подписывать данные конфигурации и дополнительные параметры, образующие подписанные данные конфигурации. Как рассмотрено выше, данные конфигурации могут указывать определенный производственный период или другие продукты и действия. Модуль авторизации может генерировать блок авторизации, включающий в себя ключ, авторизованные идентификаторы и маркер безопасности. В некоторых вариантах осуществления ключ может генерироваться модулем авторизации или может поступать на него. Модуль авторизации может передавать блок авторизации на модуль управления. Модуль управления может передавать подтвержденные данные конфигурации и другую информацию, например список идентификаторов, диапазон идентификаторов и/или один или более маркеров безопасности, на модуль (145) подписи. Модуль подписи может подписывать данные и отправлять подписанные данные и подпись на модуль управления. Затем модуль (140) идентификации может принимать от модуля управления блок инициализации, включающий в себя идентификаторы и/или диапазоны идентификаторов для продуктов.

Вариант осуществления изобретения может включать в себя способ инициализации процесса для безопасного управления производственным объектом, содержащий электронный прием данных конфигурации из электронного хранилища данных; электронное хранение данных конфигурации для производственного периода, причем данные конфигурации для производственного периода задают параметры, используемые при производстве продуктов; передачу данных конфигурации на модуль авторизации; на модуле авторизации определение, авторизован ли производственный период; генерирование подтвержденных данных конфигурации, содержащих ключ, представление множества авторизованных идентификаторов продукта и маркер безопасности; передачу подтвержденных данных конфигурации на модуль подписи; и на модуле подписи подписание подтвержденных данных конфигурации.

Альтернативные или дополнительные варианты осуществления могут включать в себя определение, авторизованы ли данные конфигурации для производственного периода; если производственный период авторизован, генерирование маркера безопасности и связывание маркера с данными конфигурации; и снабжение данных конфигурации цифровой подписью путем генерирования цифровой подписи и связывания цифровой подписи с данными конфигурации.

Альтернативные или дополнительные варианты осуществления могут включать в себя прием данных конфигурации, снабженных цифровой подписью, и цифровой подписи на продукционной машине; на продукционной машине проверку цифровой подписи, связанной с данными конфигурации, снабженными цифровой подписью; и вычисление набора защищенных идентификаторов продукта на основании данных конфигурации, снабженных цифровой подписью.

Альтернативные или дополнительные варианты осуществления могут включать в себя выработку продуктов в течение производственного периода согласно данным конфигурациям, снабженным цифровой подписью; и печать набора защищенных идентификаторов продукта на продуктах согласно данным конфигурациям, снабженным цифровой подписью.

Альтернативные или дополнительные варианты осуществления могут включать в себя определение, авторизован ли производственный период, дополнительно содержит извлечение данных лицензирования из сервера лицензирования.

Генерация идентификационного кода.

Согласно фиг. 4 процесс генерации кода генерирует коды в ходе производственного процесса. Процесс генерации идентификационного кода может начинаться с запроса модулю (140) идентификации на предмет идентификатора или диапазона идентификаторов, которые затем возвращаются на модуль (110) управления. Затем идентификаторы отправляются на модуль (145) подписи, который подписывает идентификаторы и возвращает подписанные идентификаторы на модуль управления. Модуль подписи может принимать маркер безопасности. В некоторых вариантах осуществления модуль подписи не требует управления внешними инструкциями, и если какой-либо идентификационный код подлежит отсчету, код может быть связан с единичным маркером безопасности. Модуль подписи может управляться модулем авторизации. Затем модуль управления может отправлять выходные данные на модуль управления печатью в модуле принтера (210). Выходные данные, отправленные на модуль управления печатью, могут шифроваться до передачи. Данные конфигурации могут передаваться на модуль (150) проверки для обработки последующих запросов проверки.

Вариант осуществления изобретения включает в себя способ генерирования кода для безопасной идентификации продуктов, вырабатываемых на производственном объекте, включающий в себя электронный прием данных конфигурации из электронного хранилища данных; электронное хранение данных конфигурации для производственного периода, причем данные конфигурации для производственного периода задают параметры, используемые при производстве продуктов; передачу данных конфигурации на модуль авторизации; на модуле авторизации определение, авторизован ли производственный период; генерирование подтвержденных данных конфигурации, содержащих ключ, представление множества авторизованных идентификаторов продукта и маркер безопасности; передачу подтвержденных данных конфигурации на модуль подписи; на модуле подписи подписание подтвержденных данных конфигурации; на модуле идентификации прием запроса идентификатора продукта и генерирования идентификатора продукта в ответ на запрос; передачу идентификатора продукта от модуля идентификации на модуль подписи; снабжение идентификатора продукта цифрой подписью на модуле подписи и передачу идентификатора продукта, снабженного цифрой подписью, на модуль принтера.

Альтернативные или дополнительные варианты осуществления могут включать в себя электронный прием данных конфигурации из электронного хранилища данных; электронное хранение данных конфигурации для производственного периода, причем данные конфигурации для производственного периода задают параметры, используемые при производстве продуктов; передачу данных конфигурации на модуль авторизации; на модуле авторизации определение, авторизован ли производственный период; генерирование подтвержденных данных конфигурации, содержащих ключ, представление множества авторизованных идентификаторов продукта и маркер безопасности; передачу подтвержденных данных конфигурации на модуль подписи; на модуле подписи подписание подтвержденных данных конфигурации.

В альтернативных или дополнительных вариантах осуществления запрашивается диапазон идентификаторов.

Альтернативные или дополнительные варианты осуществления могут включать в себя определение, авторизованы ли данные конфигурации для производственного периода; если производственный период авторизован, генерирование маркера безопасности и связывание маркера с данными конфигурации; и снабжение данных конфигурации цифровой подписью путем генерирования цифровой подписи и связывания цифровой подписи с данными конфигурации.

Проверка идентификационного кода.

Модуль проверки может принимать запрос проверки. Запрос может включать в себя один или более идентификационных кодов. Модуль проверки может дешифровать или иначе деобфусцировать принятый идентификационный код. Результирующая информация, будучи дешифрованной, может включать в себя компоненту подписи и идентификатор. Затем результирующий идентификатор может связываться с исходными данными конфигурации, ранее сохраненными совместно с идентификатором. Связанные данные могут включать в себя другие идентификаторы в диапазоне, маркер безопасности и другую информацию, сохраненную в связи с производством продукта, несущую этот идентификационный код.

Некоторые варианты осуществления могут включать в себя дополнительный функционал для обра-

ботки идентификаторов, поступающих на модуль проверки, на основании стороны, запрашивающей проверку кода. Разные стороны могут снабжаться разными средствами для осуществления доступа к модулю проверки. Например, розничный торговец или другая форма торговой организации может быть снабжен(а) иным порталом или каналом связи, чем потребитель. Розничному торговцу также может потребоваться аутентифицировать себя модулю проверки.

В некоторых вариантах осуществления система может быть сконфигурирована таким образом, что проверка потребителем приводит к тому, что идентификатор маркируется как проверенный. Система дополнительно может быть выполнена с возможностью хранения этих кодов, проверка которых запрашивается потребителем. Любые последующие запросы для проверки этих раннее проверенных кодов могут быть отклонены или иначе обрабатываться по-разному.

Экспортные функции.

Варианты осуществления изобретения могут применяться в отношении экспорта кода третьим сторонам. Эти варианты осуществления могут включать в себя экспортную функцию, сконфигурированную для генерирования отдельного кода с этой целью. Экспортированный код можно генерировать путем сбора одного или более идентификаторов продукта и/или маркеров безопасности, и подписания этих идентификаторов и/или маркеров. Идентификаторы и/или маркеры можно собирать в любой момент в производственном процессе. Подписанные идентификаторы и/или маркеры в форме экспортированных кодов могут сообщаться третьей стороне, которая может хранить их и осуществлять проверку действительности идентификаторов и/или маркеров.

Системные архитектуры.

Описанные здесь системы и способы могут быть реализованы в программном обеспечении или оборудовании или любой их комбинации. Описанные здесь системы и способы могут быть реализованы с использованием одного или более вычислительных устройств, которые могут быть или не быть физически или логически отдельными друг от друга. Дополнительно различные аспекты описанных здесь способов могут объединяться или вливаться в другие функции. В некоторых вариантах осуществления проиллюстрированные элементы системы могут объединяться в единое аппаратное устройство или делиться на множественные аппаратные устройства. Если используются множественные аппаратные устройства, аппаратные устройства могут физически располагаться вблизи или на удалении друг от друга.

Способы могут быть реализованы в компьютерном программном продукте, доступном с компьютерно-используемого или компьютерно-считываемого носителя данных, который обеспечивает программный код для использования компьютером или любой системой исполнения инструкций или совместно с ним/ней. Компьютерно-используемый или компьютерно-считываемый носитель данных может представлять собой любое устройство, которое может содержать или хранить программу для использования компьютером или системой, устройством или оборудованием исполнения инструкций или совместно с ним/ней.

Система обработки данных, пригодная для хранения и/или выполнения соответствующего программного кода, может включать в себя по меньшей мере один процессор, подключенный прямо или косвенно к компьютерным устройствам хранения данных, например элементам памяти. Устройства ввода/вывода (I/O) (включающие в себя, но без ограничения, клавиатуры, дисплеи, указательные устройства и т.д.) могут быть подключены к системе. Сетевые адаптеры также могут быть подключены к системе, чтобы система обработки данных могла подключаться к другим системам обработки данных или удаленным принтерам или запоминающим устройствам через промежуточные частные или публичные сети. Для обеспечения взаимодействия с пользователем признаки могут быть реализованы на компьютере с устройством отображения, например CRT (электронно-лучевой трубкой), LCD (жидкокристаллическим дисплеем) или монитором другого типа для отображения информации пользователю, и клавиатура и устройство ввода, например мышь или шаровой манипулятор, с помощью которого пользователь может обеспечивать ввод в компьютер.

Компьютерная программа может представлять собой набор инструкций, который может использоваться, прямо или косвенно, на компьютере. Описанные здесь системы и способы могут быть реализованы с использованием таких языков программирования, как Flash™, JAVA™, C++, C, C#, Visual Basic™, JavaScript™, PHP, XML, HTML и т.д., или комбинации языков программирования, включающих в себя компилируемые или интерпретируемые языки, и могут быть установлены в любой форме, включающей в себя в качестве самостоятельной программы или в качестве модуля, компонента, подпрограммы или другого модуля, пригодного для использования в вычислительном окружении. Программное обеспечение может включать в себя, но без ограничения, программно-аппаратное обеспечение, резидентное программное обеспечение, микрокод и т.д. В реализации интерфейсов между модулями программирования можно использовать такие протоколы, как SOAP/HTTP. Описанные здесь компоненты и функции могут осуществляться на любой настольной операционной системе, выполняющейся в виртуализированном или невиртуализированном окружении, с использованием любого языка программирования, пригодного для разработки программного обеспечения, включающего в себя, но без ограничения, разные версии Microsoft Windows™, Apple™ Mac™, iOS™, Unix™/×-Windows™, Linux™ и т.д.

Пригодные процессоры для выполнения программных инструкций включают в себя, но без ограничения, микропроцессоры общего и специального назначения и единственный процессор или один из множественных процессоров или ядер компьютера любого рода. Процессор может принимать и хранить инструкции и данные из компьютерного устройства хранения данных, например постоянной памяти, оперативной памяти, обеих или любой комбинации описанных здесь устройств хранения данных. Процессор может включать в себя любую схему обработки или схему управления, выполненную с возможностью управления работой и рабочими характеристиками электронного устройства.

Процессор также может включать в себя одно или более устройств хранения данных или может в ходе работы подключаться для осуществления связи с ними для хранения данных. Такие устройства хранения данных могут включать в себя в порядке неограничительных примеров магнитные диски (в том числе внутренние жесткие диски и сменные диски), магнитооптические диски, оптические диски, постоянную память, оперативную память и/или хранилище на основе флеш-технологий. Запоминающие устройства, пригодные для материального воплощения инструкций компьютерной программы и данных, также могут включать в себя все формы энергонезависимой памяти, включающие в себя, например, полупроводниковые запоминающие устройства, например EPROM, EEPROM и запоминающие устройства на основе флеш-технологий; магнитные диски, например внутренние жесткие диски и сменные диски; магнитооптические диски и диски CD-ROM и DVD-ROM. Процессор и память могут дополняться ASIC (специализированными интегральными схемами) или входить в их состав.

Описанные здесь системы, модули и способы могут быть реализованы с использованием любой комбинации программных или аппаратных элементов. Описанные здесь системы, модули и способы могут быть реализованы с использованием одной или более виртуальных машин, действующих самостоятельно или совместно друг с другом. Любое применимое решение виртуализации может использоваться для инкапсулирования физической платформы вычислительной машины в виртуальную машину, которая выполняется под управлением программного обеспечения виртуализации, выполняющегося на аппаратной вычислительной платформе или хосте. Виртуальная машина может иметь как виртуальное оборудование системы, так и гостевое программное обеспечение операционной системы.

Описанные здесь системы и способы могут быть реализованы в компьютерной системе, которая включает в себя невидимый компонент, например сервер данных, или которая включает в себя промежуточный программный компонент, например сервер приложений или интернет-сервер, или которая включает в себя интерфейсный компонент, например компьютер-клиент, имеющий графический пользовательский интерфейс или интернет-браузер, или любую их комбинацию. Компоненты системы могут быть соединены посредством любой формы или среды передачи цифровых данных, например сети связи. Примеры сетей связи включают в себя, например, LAN, WAN и компьютеры и сети, которые образуют интернет.

Один или более вариантов осуществления изобретения можно практически применять с другими конфигурациями компьютерной системы, включающими в себя карманные устройства, микропроцессорные системы, микропроцессорную или программируемую бытовую электронику, миникомпьютеры, универсальные компьютеры и т.д. Изобретение также можно практически применять в распределенных вычислительных окружениях, где задачи осуществляются удаленными устройствами обработки, связанными через сеть.

Хотя были описаны один или более вариантов осуществления изобретения, различные их изменения, добавления, перестановки и эквиваленты включены в объем изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ генерирования кода для идентификации продуктов, вырабатываемых на производственном объекте, содержащий этапы, на которых

электронно принимают из электронного хранилища данных и электронно сохраняют данные конфигурации для производственного периода, причем данные конфигурации для производственного периода задают параметры, используемые при производстве продуктов;

передают данные конфигурации на модуль авторизации;

на модуле авторизации

определяют, авторизован ли производственный период;

генерируют подтвержденные данные конфигурации, содержащие ключ, представление множества авторизованных идентификаторов продукта и маркер безопасности;

передают подтвержденные данные конфигурации на модуль подписи;

на модуле подписи подписывают подтвержденные данные конфигурации;

на модуле идентификации принимают запрос идентификатора продукта и генерируют идентификатор продукта в ответ на запрос, причем генерирование идентификатора продукта осуществляют путем

задания и сохранения информации, описывающей состояние вычислительной машины, как номера машины (MNUM), причем информация, описывающая состояние, включает в себя количество основ, содержащих информацию, описывающую состояние;

генерирования машинного защищенного уникального идентификатора продукта (MSUPI) в качестве обратимого математического преобразования машинного уникального идентификатора продукта (MUPI) на основании информации, описывающей состояние вычислительной машины, причем этап вычисления MSUPI содержит этапы, на которых

задают количество этапов, равным imax, для каждого этапа генерируют первое случайное число в качестве ключа обфускации для генерации кода ($CGOK_{i,1}$) и второе случайное число в качестве ключа обфускации для генерации кода ($CGOK_{i,2}$), причем

генерирование содержит этапы, на которых

вычисляют первое случайное число ($CGOK_{i,1}$), взаимно простое с числом, основанным на информации, описывающей состояние вычислительной машины (MNUM);

вычисляют второе случайное число ($CGOK_{i,2}$), имеющее равный или меньший битовый размер, как (MNUM);

задают $m_{0,2}$=MUPI;

вычисляют для каждого элемента i от i=1 до imax - 1:

$m_{i,1}=(m_{i-1,2}\times CGOK_{i,1}) \bmod (MNUM)$;

$m_{i,2}=(m_{i,1} \bmod CGOK_{i,2})$;

если $(m_{i,2} > MNUM) \rightarrow m_{i,2}=m_{i,1}$;

задают $MSUPI=m_{imax,2}$;

передают машинный защищенный уникальный идентификатор продукта от модуля идентификации на модуль подписи;

снабжают цифровой подписью машинный защищенный уникальный идентификатор продукта на модуле подписи и

передают машинный защищенный уникальный идентификатор продукта, снабженный цифровой подписью, на модуль принтера.

2. Способ по п.1, в котором информация, описывающая состояние вычислительной машины, содержит комбинацию информации времени и номера продукта.

3. Способ по одному или более из предыдущих пунктов, в котором информация времени включает в себя юлианский год, юлианский день, производственный час и производственную минуту.

4. Способ по одному или более из предыдущих пунктов, в котором информация, описывающая состояние, включает в себя значение инкрементного счетчика, сбрасываемого на периодической основе.

5. Способ по одному или более из предыдущих пунктов, в котором упомянутое число, основанное на информации, описывающей состояние вычислительной машины, вычисляют как 10×366×24×60×временной идентификатор.

6. Способ по одному или более из предыдущих пунктов, в котором временной идентификатор задают как целое число 2210.

7. Способ по одному или более из предыдущих пунктов, в котором защищенный уникальный идентификатор продукта (SUPI), 12-символьный буквенно-числовой код, получают таким образом, что SUPI= (p×m) mod (MNUM×mNoise×RunLim).

8. Способ по одному или более из предыдущих пунктов, дополнительно содержащий этап, на котором сохраняют машинный защищенный уникальный идентификатор продукта (MSUPI) в электронном хранилище данных в качестве идентификатора продукта.

9. Способ по одному или более из предыдущих пунктов, в котором запрашивают диапазон идентификаторов.

10. Способ по одному или более из предыдущих пунктов, дополнительно содержащий этапы, на которых

определяют, авторизованы ли данные конфигурации для производственного периода;

если производственный период авторизован, генерируют маркер безопасности и связывают упомянутый маркер с данными конфигурации; и

снабжают данные конфигурации цифровой подписью путем генерирования цифровой подписи и связывания цифровой подписи с данными конфигурации.

11. Способ по одному или более из предыдущих пунктов, в котором машинный уникальный идентификатор продукта (MUPI) преобразуют без заполнения машинного уникального идентификатора продукта (MUPI) таким образом, что битовая длина машинного уникального идентификатора продукта (MUPI) равна битовой длине машинного защищенного уникального идентификатора продукта (MSUPI).

12. Система для генерирования кода для идентификации продуктов, вырабатываемых на производственном объекте, содержащая компьютерный процессор, выполненный с возможностью выполнения машиночитаемых команд для осуществления способа по п.1.

13. Система по п.12, в которой информация, описывающая состояние вычислительной машины, содержит комбинацию информации времени и номера продукта.

14. Система по п.12, в которой информация времени включает в себя юлианский год, юлианский день, производственный час и производственную минуту.

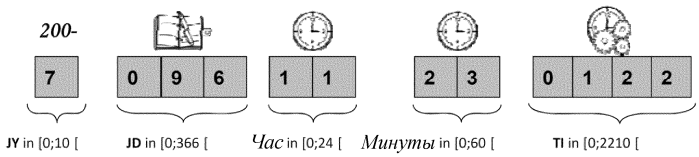
15. Система по п.12, в которой информация, описывающая состояние, включает в себя значение инкрементного счетчика, сбрасываемого на периодической основе.

16. Система по п.12, в которой упомянутое число, основанное на информации, описывающей состояние вычислительной машины, вычисляется как 10×366×24×60×временной идентификатор.

17. Система по п.12, в которой временной идентификатор задается как целое число 2210.

18. Система по п.12, в которой защищенный уникальный идентификатор продукта (SUPI), 12-символьный буквенно-числовой код, получается таким образом, что SUPI=(p×m) mod (MNUM× mNoise×RunLim).

19. Система по п.12, в которой компьютерный процессор дополнительно выполнен с возможностью выполнения инструкций для сохранения машинного защищенного уникального идентификатора продукта (MSUPI) в электронном хранилище данных в качестве идентификатора продукта.

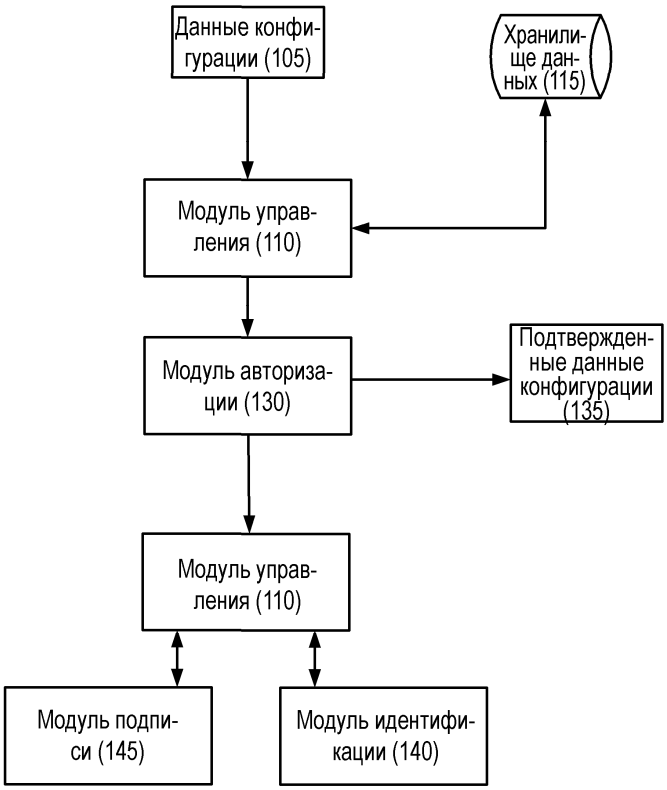


$$MUPI = \left(\left(\left(JY \times 366 + JD\right) \times 24 + \ час \ \right) \times 60 + минуты\right) \times 2210 + TI$$

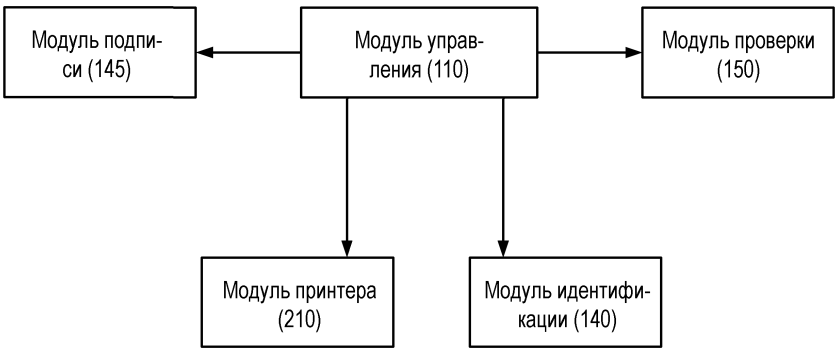
Фиг. 1

$$\begin{cases} m_{0,2} = MUPI \\ m_{i,1} = \left(m_{i-1,2} \times CGOK_{i,1}\right) \bmod \left(10 \times 366 \times 24 \times 60 \times 2210\right) \\ m_{i,2} = \left(m_{i,1} \oplus CGOK_{i,2}\right) \\ IF\left(m_{i,2} > 10\text{x}366\text{x}24\text{x}60\text{x}1100\text{x}2210\right) \rightarrow m_{i,2} = m_{i,1} \\ MSUPI = m_{8,2} \end{cases}$$

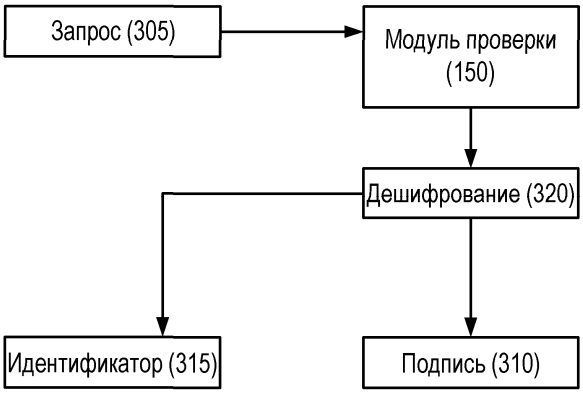
Фиг. 2



Фиг. 3


Модуль подпи-
си (145)
Модуль управ-
ления (110)
Модуль проверки
(150)
Модуль принтера
(210)
Модуль идентифи-
кации (140)

Фиг. 4


Запрос (305)
Модуль проверки
(150)
Дешифрование (320)
Идентификатор (315)
Подпись (310)

Фиг. 5