(19) Евразийское патентное ведомство

(11) 035011 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2020.04.16

(21) Номер заявки
201690730

(22) Дата подачи заявки
2014.10.03

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

(54) СПОСОБ УПРАВЛЕНИЯ, ОБЪЕДИНЕНИЯ И РАСПРОСТРАНЕНИЯ КЛЮЧЕЙ ШИФРОВАНИЯ

(31) **61/887,662; 61/950,362**
(32) **2013.10.07; 2014.03.10**
(33) **US**
(43) **2016.09.30**
(86) **PCT/US2014/059187**
(87) **WO 2015/054083 2015.04.16**

(71)(73) Заявитель и патентовладелец:
ФОРНЕТИКС ЭлЭлСи (US)

(72) Изобретатель:
Уайт Чарльз, Брэнд Джозеф, Эдвардс Стивен (US)

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

(56) US-B1-8213620
US-A1-20130044882
US-A1-20090092252
US-A1-20130114812
US-A1-20090175452

(57) Настоящее изобретение относится к генерированию, управлению, распространению и/или объединению объектов безопасности, используемых в системах связи. Предложен способ управления информационным объектом безопасности, содержащий этапы, на которых задают и сохраняют множество политик, связанных, по меньшей мере отчасти, с информационным объектом безопасности, в базе данных, соединенной со средством обработки политик; принимают с помощью средства обработки политик информационный объект безопасности для его распространения по меньшей мере в одно устройство связи и по меньшей мере один атрибут объекта, связанный с информационным объектом безопасности; определяют с помощью средства обработки политик основывающуюся на соображениях криптографии пригодность информационного объекта безопасности, чтобы определить, является ли информационный объект безопасности достаточно безопасным, основываясь, по меньшей мере отчасти, на этом по меньшей мере одном атрибуте объекта и по меньшей мере одной из упомянутого множества политик, соответствующей этому по меньшей мере одному атрибуту объекта; и распространяют тот информационный объект безопасности, который был принят, в упомянутое по меньшей мере одно устройство связи, связанное со средством обработки политик, в качестве реакции на определение того, что информационный объект безопасности является пригодным, причем это по меньшей мере одно устройство связи устанавливает связь, основываясь, по меньшей мере отчасти, на информационном объекте безопасности. Технический результат относится к усовершенствованной подготовке информационных объектов безопасности, которая обеспечивает возможность, по меньшей мере, избежать раскоординации между управлением безопасностью и управлением осуществлением связи.

035011 B1

035011 B1

Перекрестная ссылка к соотнесенным патентным заявкам

Данная заявка испрашивает приоритет согласно предварительной заявки № 61/887662, поданной 7 октября 2013, и предварительной заявки № 61/950362, поданной 10 марта 2014, содержание которых полностью включено в данную работу посредством ссылки.

Уровень техники

Область техники, к которой относится изобретение

Варианты осуществления настоящего изобретения относятся в общем случае к объектам безопасности, используемым в системах связи, а более конкретно к генерации, управлению, распространению, объединению и/или подготовке объектов безопасности.

Предшествующий уровень техники

В системах обеспечения безопасности ключ шифрования относится к параметру или данным, которые указывают, как простые данные могут преобразовываться в зашифрованные данные во время процесса шифрования, а зашифрованные данные - в простые данные во время процесса расшифровки. Как правило, ключ шифрования делают доступным обоим из устройства-источника (например, передающего устройства) и устройства-адресата (например, приемного устройства) в операции связи. Учитывая, что ключи шифрования используются повсеместно, эффективное управление ключами шифрования (а также другими объектами безопасности) для защиты и реагирования на угрозы по отношению к системам обеспечения безопасности имеет первостепенную важность.

Традиционно управление ключами шифрования инициируется и выполняется на уровне устройства (например, с помощью устройства-источника и/или устройства-адресата, которые вовлечены в операцию связи). Управлением осуществлением связи, с другой стороны, традиционно централизованно управляют на более высоком уровне (например, с помощью сервера для устройства-источника и устройства-адресата). Конечным результатом может быть то, что управление шифрованием формально не синхронизируется с управлением связью. Таким образом, это может привести к потере контроля над ключами шифрования, как демонстрируется в случаях существующей инфраструктуры открытых ключей (PKI). Кроме того, может также произойти потеря контроля над симметричными ключами, генерируемыми и распространяемыми в предприятии. Соответственно конечным результатом может быть нарушение в управлении связью или в обеспечении безопасности связи. С аналогичными проблемами сталкиваются другие типы объектов шифрования.

Сущность раскрытия

Существующее раскрытие описывает варианты осуществления, относящиеся к подготовке объекта безопасности, включающей в себя, но не ограниченной ими, управление, распространение и объединение объектов безопасности. Объекты безопасности могут включать в себя ключи шифрования и другие объекты безопасности, но не ограничены ими (такие как информация идентификатора пользователя, сертификаты, биометрические данные, данные генератора случайных чисел, определенные данные генератора случайных чисел, неопределенные данные генератора случайных чисел, информация аутентификации пользователя, компоненты политики, другие компоненты, связанные с компонентой обеспечения безопасности организации и/или т.п., но которые не ограничены ими).

Предложен способ управления информационным объектом безопасности, при этом способ содержит, но не в ограничительном смысле, этапы, на которых: задают и сохраняют множество политик, связанных, по меньшей мере отчасти, с информационным объектом безопасности, в базе данных, соединенной со средством обработки политик; принимают с помощью средства обработки политик информационный объект безопасности для его распространения по меньшей мере в одно устройство связи и по меньшей мере один атрибут объекта, связанный с информационным объектом безопасности; определяют с помощью средства обработки политик основывающуюся на соображениях криптографии пригодность информационного объекта безопасности, чтобы определить, является ли информационный объект безопасности достаточно безопасным, основываясь, по меньшей мере отчасти, на этом по меньшей мере одном атрибуте объекта и по меньшей мере одной из упомянутого множества политик, соответствующей этому по меньшей мере одному атрибуту объекта; и распространяют тот информационный объект безопасности, который был принят, в упомянутое по меньшей мере одно устройство связи, связанное со средством обработки политик, в качестве реакции на определение того, что информационный объект безопасности является пригодным, причем это по меньшей мере одно устройство связи устанавливает связь, основываясь, по меньшей мере отчасти, на информационном объекте безопасности.

В некоторых вариантах осуществления объект безопасности является ключом шифрования. В различных вариантах осуществления по меньшей мере один атрибут объекта содержит характеристики по меньшей мере одного из объекта безопасности, первого устройства, генерирующего объект безопасности, второго устройства, передающего объект безопасности, третьего устройства, принимающего объект безопасности, первого пользователя, связанного с первым устройством, второго пользователя, связанного со вторым устройством, и третьего пользователя, связанного с третьим устройством.

Согласно некоторым вариантам осуществления по меньшей мере один атрибут объекта содержит по меньшей мере одно из размера объекта безопасности, времени, когда объект безопасности генерируется, георасположения, где объект безопасности генерируется, классификации объекта безопасности,

роли, связанной с источником ключа, роли, связанной с устройством-источником, и роли, связанной с устройством-адресатом.

В некоторых вариантах осуществления множество политик содержит подтверждение пригодности объекта безопасности, когда размер объекта безопасности находится в пределах предопределенного диапазона размеров. В различных вариантах осуществления множество политик содержит подтверждение пригодности объекта безопасности, когда время, когда объект безопасности генерируется, находится в пределах предопределенного интервала времени.

В некоторых вариантах осуществления множество политик содержит подтверждение пригодности объекта безопасности, когда георасположение, где объект безопасности генерируется, находится в пределах предопределенной области. Как воплощается в некоторых вариантах осуществления, множество политик содержит подтверждение пригодности объекта безопасности, когда классификация объекта безопасности связана с предопределенной группой классификаций объекта безопасности. В некоторых вариантах осуществления множество политик содержит подтверждение пригодности объекта безопасности, когда роль, связанная с источником ключа, устройством-источником или устройством-адресатом, связана с предопределенной группой ролей.

Способ дополнительно включает в себя передачу указателя отклонения к источнику ключа; и передачу к источнику ключа подсказки, сообщающей о несоответствии объекта безопасности, причем объект безопасности принимается из источника ключа.

В некоторых вариантах осуществления прием с помощью средства обработки политик объекта безопасности включает в себя прием с помощью средства обработки политик запроса о генерации объекта безопасности и генерацию с помощью средства обработки политик объекта безопасности.

Предложен способ управления информационным объектом безопасности, при этом способ содержит, но не в ограничительном смысле, этапы, на которых задают и сохраняют первое множество политик, связанных, по меньшей мере отчасти, с информационным объектом безопасности, в первой базе данных первого устройства подготовки ключей, причем первая база данных связана с первым предприятием; принимают с помощью первого устройства подготовки ключей, связанного с первым предприятием, информационный объект безопасности для его распространения в по меньшей мере одно устройство связи и по меньшей мере один атрибут объекта, связанный с информационным объектом безопасности, из второго устройства подготовки ключей, связанного со вторым предприятием; определяют с помощью первого устройства подготовки ключей основывающуюся на соображениях криптографии пригодность информационного объекта безопасности, чтобы определить, является ли информационный объект безопасности достаточно безопасным, основываясь, по меньшей мере отчасти, на этом по меньшей мере одном атрибуте объекта и по меньшей мере одной из первого множества политик, соответствующей этому по меньшей мере одному атрибуту объекта; и распространяют тот информационный объект безопасности, который был принят, в первое устройство связи, связанное с первым предприятием.

Как описано в некоторых вариантах осуществления, способ дополнительно включает в себя определение и сохранение второго множества политик во второй базе данных второго устройства подготовки ключей. По меньшей мере, первая часть первого множества политик и вторая часть второго множества политик являются одинаковыми.

В некоторых вариантах осуществления способ дополнительно включает в себя передачу из первого устройства подготовки ключей на второе устройство подготовки ключей объекта безопасности и распространение объекта безопасности ко второму устройству связи, связанному со вторым предприятием, причем первое устройство связи и второе устройство связи могут устанавливать связь, основываясь на данном объекте безопасности.

В различных вариантах осуществления способ дополнительно включает в себя передачу из первого устройства подготовки ключей на второе устройство подготовки ключей объекта безопасности, определение с помощью второго устройства подготовки ключей пригодности объекта безопасности, основываясь, по меньшей мере частично, по меньшей мере на одном атрибуте объекта и по меньшей мере на одной из второго множества политик, соответствующих по меньшей мере одному атрибуту объекта, и распространение объекта безопасности ко второму устройству связи, связанному со вторым предприятием. Первое устройство связи и второе устройство связи могут устанавливать связь, основываясь на объекте безопасности.

Как воплощается в различных вариантах осуществления, прием объекта безопасности и по меньшей мере одного атрибута объекта, связанного с объектом безопасности, из второго устройства подготовки ключей включает в себя прием с помощью первого устройства подготовки ключей из второго устройства подготовки ключей запроса о генерации объекта безопасности и генерацию с помощью источника ключа, связанного с первым предприятием, объекта безопасности в ответ на данный запрос.

В некоторых вариантах осуществления считываемый компьютером носитель содержит считываемые компьютером команды, так, что когда они выполняются, это побуждает процессор определять множество политик в базе данных, принимать объект безопасности и по меньшей мере один атрибут объекта, связанный с объектом безопасности, определять пригодность объекта безопасности, основываясь, по меньшей мере частично, на этом по меньшей мере одном атрибуте объекта и по меньшей мере одной из

упомянутого множества политик, соответствующей этому по меньшей мере одному атрибуту объекта; и распространять объект безопасности по меньшей мере к одному устройству связи, связанному с процессором, когда определено, что объект безопасности является пригодным. Это по меньшей мере одно устройство связи устанавливает связь, основываясь, по меньшей мере частично, на данном объекте безопасности. В некоторых вариантах осуществления объект безопасности является ключом шифрования.

В различных вариантах осуществления по меньшей мере один атрибут объекта содержит по меньшей мере одно из размера объекта безопасности, времени, когда объект безопасности генерируется, георасположения, где объект безопасности генерируется, классификации объекта безопасности, роли, связанной с источником ключа, роли, связанной с устройством-источником, и роли, связанной с устройством-адресатом.

Как воплощается в некоторых вариантах осуществления, множество политик содержит подтверждение пригодности объекта безопасности, когда выполняется по меньшей мере одно условие: размер объекта безопасности находится в пределах предопределенного диапазона размеров, время, когда объект безопасности генерируется, находится в пределах предопределенного интервала времени, георасположение, где объект безопасности генерируется, находится в пределах предопределенной области, классификацию объекта безопасности включает в себя предопределенная группа классификаций объекта безопасности, и роль, связанная с источником ключа, устройством-источником или устройством-адресатом, связана с предопределенной группой ролей.

Краткое описание чертежей

Фиг. 1 - схематическая структурная схема, показывающая пример обобщенной системы подготовки ключей шифрования согласно различным вариантам осуществления.

Фиг. 2 - схематическая структурная схема, показывающая пример системы подготовки ключей шифрования согласно различным вариантам осуществления.

Фиг. 3 - схематическая структурная схема, показывающая пример системы объединения ключей шифрования, которая воплощается в различных вариантах осуществления.

Фиг. 4 - схематическая структурная схема, показывающая пример устройства связи, использующего услугу подготовки ключей согласно некоторым вариантам осуществления.

Фиг. 5 - последовательность операций процесса, показывающая пример процесса аутентификации запроса для выдачи запросов и приема ключей шифрования согласно некоторым вариантам осуществления.

Фиг. 6 - последовательность операций процесса, показывающая пример процесса регистрации устройства связи, воплощаемого в различных системах подготовки ключей согласно различным вариантам осуществления.

Фиг. 7 - последовательность операций процесса, показывающая пример процесса управления и распространения ключей согласно различным вариантам осуществления.

Фиг. 8 - последовательность операций процесса, показывающая пример процесса объединения ключей согласно различным вариантам осуществления.

Фиг. 9 - последовательность операций процесса, показывающая пример процесса управления и распространения ключей шифрования согласно различным вариантам осуществления.

Подробное описание

В последующем описании различных вариантов осуществления ссылка сделана на сопроводительные чертежи, которые являются частью данного документа и в которых показаны посредством иллюстрации конкретные варианты осуществления, в которых может применяться данное изобретение. Нужно подразумевать, что могут использоваться другие варианты осуществления, и структурные изменения могут быть сделаны без отступления от объема различных вариантов осуществления, раскрытых в настоящем раскрытии.

Варианты осуществления, описанные в данной работе, в общем случае относятся к подготовке объекта безопасности. Подготовка объекта безопасности может включать в себя управление, распространение и объединение объектов безопасности. Объекты безопасности могут включать в себя ключи шифрования и другие важные объекты (такие как информация идентификатора пользователя, сертификаты, биометрические данные, данные генератора случайных чисел, определенные данные генератора случайных чисел, неопределенные данные генератора случайных чисел, информация аутентификации пользователя, компоненты политики, другие компоненты, связанные с компонентой обеспечения безопасности организации и/или т.п., но которые не ограничены ими). В настоящем раскрытии основанная на ключе шифрования подготовка описана в различных вариантах осуществления в качестве примеров систем и способов подготовки объекта безопасности. Нужно признать, что данные системы и способы подготовки могут применяться подобным образом к другим объектам безопасности, которые включают в себя те, которые описаны выше.

В данной работе "подготовка ключей" может относиться к комбинации действий управления ключами, объединения ключей и распространения ключей в одном или большем количестве предприятий. Например, описанные варианты осуществления могут связываться с подготовкой информации ключа шифрования, коррелированной с использованием шифрования в одном или большем количестве предприятий. "Управление ключами предприятия" может включать в себя управление и/или наблюдение за

множеством использований асимметричных и симметричных ключей, требуемых для шифрования данных, подписи электронной почты, аутентификации веб-служб и/или другого возможного использования. Оно может также включать в себя управление шифрованием для систем связи, которые включают в себя системы радиосвязи, сотовой связи, спутниковой связи и связи на основе Интернет-протокола. "Объединение ключей предприятия" может включать в себя координирование и согласование объединения информации ключей для множества отличающихся платформ подготовки ключей (каждая связана с отличающимися организациями, участвующими в объединении), основываясь на установленном доверии между организациями, участвующими в объединении (например, предприятиями). "Распространение ключей" может относиться к централизованному распространению (например, принудительному отправлению или перенаправлению) ключевого материала для поддержания операции шифрования в пределах локального предприятия и/или внешнего предприятия. В частности, распространение ключей может относиться к назначению или передаче иным образом соответствующих ключей шифрования на соответствующим образом связанное устройство (например, на устройство связи, которое может быть или устройством-источником, или устройством-адресатом).

Варианты осуществления подготовки ключей (например, устройство подготовки ключей, такое как средство обработки запроса управления, соединенное со средством обработки запроса и с различными поддерживаемыми базами данных) могут обеспечивать контроль управления, объединения и распространения ключей шифрования через централизованный пользовательский интерфейс. Такие устройства подготовки ключей могут обеспечивать централизованные системы и/или способы управления ключами шифрования, связанными с осуществлением связи, инфраструктурой и приложениями. Такие устройства подготовки ключей могут также управлять присоединением устройств, мониторингом исправности устройств, относящейся к возможностям шифрования, и мониторингом состояния для действий подготовки ключей. Такие возможности могут предоставлять возможность надежной передачи сообщений об операциях для поддержки аудиторской деятельности, связанной с управлением осуществлением связи, приложениями и инфраструктурой.

Подготовка ключей может использоваться для дополнительных систем, других, чем системы связи. Другие воплощения подготовки ключей могут включать в себя управление шифрованием приложений, управление шифрованием виртуализации, управление шифрованием запоминающего устройства и/или управление шифрованием идентификатора пользователя. Короче говоря, если приложения, осуществление связи или инфраструктуры запрашивают использование шифрования (или других типов механизмов обеспечения безопасности, используя объекты безопасности) и ключей (или объектов безопасности), то подготовка может применяться для обеспечения преимуществ, которые описаны. Системы связи могут включать в себя оборудование радиосвязи, сотовой связи, связи на основе протокола управления передачей/Интернет-протокола (TCP/IP), спутниковой связи и т.п., но не ограничены ими. Системы приложений могут включать в себя, но не ограничены ими, приложения передачи голоса по Интернет-протоколу VOIP, виртуализации, идентификации и аутентификации, обмена сообщениями, локального хранения. Системы инфраструктуры могут включать в себя решения хранения, физическую инфраструктуру обеспечения безопасности и медицинское оборудование, но не ограничены ими.

В конкретных вариантах осуществления устройство подготовки ключей может предоставлять возможность выполнения действий жизненного цикла ключа шифрования по множеству типов устройств связи централизованным образом. Устройство подготовки ключей может использовать промышленные стандарты для управления ключами для функциональной совместимости с существующими системами и может использовать, например, протоколы для применяемого управления ключами как часть подготовки ключей. Различие между применяемой подготовкой ключей и одним только управлением ключами может быть продемонстрировано при управлении ключами шифрования и распространении ключей для систем связи. Учитывая требование создания новых подключений шифрования до разрыва существующих подключений, обычные системы связи не могут использовать команды повторного создания ключей, поскольку они разорвали бы связи до того, как будут выполнены этапы управления для установки новых линий связи. Однако команды повторного создания ключей могут работать для инфраструктуры, которая включает в себя решения хранения, приложений и виртуализации, причем услуги могут повторно устанавливаться без потери централизованного контроля возможности управления.

Структурная схема системы подготовки ключей может конфигурироваться для учета использования основанного на стандарте подхода для поддерживаемых систем, таких как протокол взаимодействия для управления ключами (KMIP), например, но также и возможность разрабатывать интерфейсы поддержки для нестандартных систем, таких как физическая инфраструктура обеспечения безопасности, приложения виртуализации, системы спутниковой связи и медицинское оборудование. Это может достигаться с помощью архитектурного отделения обработки сообщений от интерфейсов поддержки. Используя просто пример KMIP, запоминающее устройство может принимать команду "повторного создания ключей", оборудование связи может принимать команды "назначения-и-уведомления" и сотовые устройства могут запрашивать команды "уведомления" с организацией очередей, сообщающие сотовым устройствам послать "получить сообщения" на устройство подготовки ключей, которая должна ретранслироваться к компонентам системы генерации и управления ключами. Примерные системы, воплощающие такие осо-

бенности, обсуждаются ниже.

Варианты осуществления, описанные в данной работе, могут включать в себя устройство подготовки ключей для воплощения централизованного управления сверху донизу ключами шифрования предприятия (например, такими как симметричный ключ шифрования, асимметричный ключ шифрования и т.п., но которые не ограничены ими), а также другими объектами безопасности, используемыми в системах обеспечения безопасности. Такой централизованный сверху донизу контроль шифрования может выполняться для заданного предприятия. Варианты осуществления могут включать в себя воплощение координируемого KMIP по отношению к управлению ключами предприятия, системы связи, приложения и инфраструктуру для функций жизненного цикла ключа шифрования, воплощающих по меньшей мере одно из: регистрации устройства, регистрации пользователя, инициализации системы и пользователя, инсталляции ключевого материала, установления ключа, регистрации ключа, рабочего использования, сохранения ключа, распространения ключа, обновления ключа, восстановления ключа, отмены регистрации ключа, уничтожения ключа, аннулирования ключа и т.п.

В данной работе "атрибут ключа" (атрибут, атрибут шифрования и/или т.п.), связанный с ключом шифрования, может относиться к характеристике, связанной с ключом шифрования, к криптографическим характеристикам или характеристикам обеспечения безопасности ключей шифрования, криптографическим алгоритмам ключей шифрования, к устройству, генерирующему/передающему/принимающему ключи шифрования, к пользователю устройства и/или т.п. Каждый ключ шифрования может связываться по меньшей мере с одним атрибутом ключа. Ключ шифрования может передаваться и/или приниматься со связанными с ним атрибутами ключа, предоставленными в значениях данных.

В данной работе "политика" может быть правилом, управляющим ключом шифрования, основываясь на атрибуте(ах) ключа, связанным с этим ключом шифрования. В конкретных вариантах осуществления политика может указывать, является или нет конкретный ключ шифрования пригодным ключом шифрования.

Такая пригодность может основываться на соображениях по безопасности и криптографии относительно того, может или нет ключ шифрования (например, как видно из атрибутов ключа, связанных с ключом шифрования) быть достаточно безопасным. Другими словами, ключ шифрования, генерируемый для конкретной операции связи, может предоставляться для анализа с помощью политики, которая будет оценивать, должно ли использование данного ключа шифрования быть разрешено или запрещено для этой операции связи.

Некоторые варианты осуществления включают в себя интерфейс для подготовки ключей для устройств мобильной связи (например, беспроводного устройства и/или т.п.) или обеспечивают интерфейс для подготовки ключей для систем беспроводной/спутниковой связи, которые включают в себя телеметрическую информацию и полезную нагрузку при спутниковой связи. Конкретные воплощения вариантов осуществления могут включать в себя интерфейсы для банковских приложений, таких как банкоматы (ATM), интерфейсы банковского счета и т.п., но которые не ограничены ими. Интерфейсы для банковских приложений могут воплощаться на любых мобильных или немобильных устройствах. Варианты осуществления могут обеспечивать интерфейс для подготовки ключей для приложений, которые включают в себя виртуализацию или обеспечение интерфейса для подготовки ключей для сетевой инфраструктуры, которая включает в себя маршрутизаторы, коммутаторы, технические средства виртуальной частной сети (VPN), межсетевые экраны, системы обнаружения вторжения (IDS), системы предотвращения вторжения (IPS), генераторы меток и/или т.п.

Например, централизованное управление шифрованием может обеспечиваться для симметричных ключей шифрования или асимметричных ключей шифрования и в частных, и в общих контекстах. В некоторых вариантах осуществления информация о существующей инфраструктуре сети может использоваться для распространения ключей шифрования, основываясь на активном/неактивном состоянии инфраструктуры сети, или для распространения и управления ключами шифрования для инфраструктуры сети, основываясь на оборудовании, которое может легко подтверждать пригодность ключей шифрования (например, существующее оборудование/программное обеспечение может устанавливаться на оборудовании для подтверждения пригодности ключей шифрования).

Варианты осуществления могут ставить в очередь информацию об операции с ключом шифрования для устройств связи, не доступных в момент заданной операции управления шифрованием (например, при событии принудительной отправки ключа). Кроме того, варианты осуществления, описанные в данной работе, могут централизованно отображать информацию жизненного цикла ключа шифрования (для поддерживаемой инфраструктуры) и успешные операции управления ключами шифрования. В дополнение или в качестве альтернативного варианта могут отображаться сообщение о неудачном завершении и/или причина неудачных операций управления ключами шифрования.

В некоторых вариантах осуществления может обеспечиваться интерфейс услуги для устройства связи для получения новых асимметричных ключей по времени. Кроме того, может обеспечиваться интерфейс услуги для устройства связи для получения новых симметричных ключей по времени. В некоторых вариантах осуществления может обеспечиваться интерфейс услуги для устройства связи для получения новых асимметричных ключей по инициативе пользователя. В различных вариантах осуществле-

ния может обеспечиваться интерфейс услуги для устройства связи для получения новых симметричных ключей по инициативе пользователя. Кроме того, может обеспечиваться объединенное распространение ключей шифрования, основываясь на установленном основанном на доверии обмене ключами между двумя или большим количеством устройств подготовки и управления ключами, как описано.

В некоторых вариантах осуществления может обеспечиваться распространение объединенного симметричного ключа к локальной инфраструктуре предприятия, основываясь на конфигурациях для распространения объединенного симметричного ключа. В различных вариантах осуществления может обеспечиваться распространение объединенного асимметричного ключа к локальной инфраструктуре предприятия, основываясь на конфигурациях для распространения объединенного асимметричного ключа. Кроме того, воплощение объединенной модели доверия при использовании множества устройств и распространение разделенного на части ключа может обеспечиваться для установления доверия между двумя недоверенными субъектами, которым необходимо безопасно обеспечивать связь.

Устройство подготовки ключей (например, средство обработки запроса управления и связанные компоненты) может включать в себя субмодули, включающие в себя модуль бизнес-логики, модуль аутентификации и авторизации, модуль принудительного установления политики, модуль непротиворечивости системы/проверки достоверности и/или т.п. для выполнения функций, описанных в данной работе.

Фиг. 1 - принципиальная схема примера обобщенной системы 100 подготовки ключей шифрования, которая воплощается в различных вариантах осуществления. В различных вариантах осуществления устройство 110 подготовки ключей может соединяться по меньшей мере с одним устройством-источником 150a и по меньшей мере с одним устройством-адресатом 150b. Устройство 110 подготовки ключей может содержать по меньшей мере один настольный компьютер, универсальный компьютер, переносной компьютер, устройство-планшет, устройство-смартфон или т.п., конфигурируемое с оборудованием и программным обеспечением для выполнения операций, описанных в данной работе. Например, устройство 110 подготовки ключей может содержать вычислительные системы, имеющие подходящие возможности обработки, память, возможности пользовательского интерфейса (например, устройство отображения и устройство ввода) и возможности осуществления связи, конфигурируемые с подходящим программным обеспечением для выполнения операций, описанных в данной работе. Таким образом, конкретные варианты осуществления могут воплощаться, используя устройства обработки данных, которые часто уже присутствуют во многих коммерческих инфраструктурах и инфраструктурах организаций, с помощью конфигурирования таких устройств с подходящими программными процессами, описанными в данной работе. Соответственно такие варианты осуществления могут воплощаться с минимальной дополнительной стоимостью оборудования. Однако другие варианты осуществления устройства 110 подготовки ключей могут относиться к системам и процессам, которые воплощаются со специализированным аппаратным оборудованием/устройствами, конкретно сконфигурированными для выполнения операций, описанных в данной работе.

В общем случае устройство-источник 150a может быть устройством связи, передающим данные (или инициирующим осуществление связи), для которого шифрование (и поэтому ключ шифрования) может требоваться или быть предпочтительным. Устройство-адресат 150b может быть устройством связи для приема данных, которые, возможно, были зашифрованы (например, с ключом шифрования). Согласно различным вариантам осуществления устройство-источник 150a и/или устройство-адресат 150b могут быть АТМ. Устройство-источник 150a и/или устройство-адресат 150b могут также быть любым сервером или устройством для хранения информации банковского счета и выполнения банковских функций. В конкретных вариантах осуществления каждое устройство-источник 150a и устройство-адресат 150b могут включать в себя мобильный смартфон (такой как iPhone™, телефон Android™ или т.п., но который не ограничен ими) или другие беспроводные устройства мобильной связи с подходящими возможностями обработки и шифрования. Типичные современные устройства мобильной связи включают в себя электронное оборудование телефонной связи, а также некоторое электронное оборудование обработки, одно или большее количество устройств отображения и клавиатуру и/или другое пользовательское устройство ввода информации. В дополнительных вариантах осуществления каждое устройство-источник 150a и устройство-адресат 150b могут содержать мобильный телефон любого подходящего типа и/или переносное электронное устройство связи другого типа, такое как электронное интеллектуальное устройство-планшет (такое как iPad™, но не ограничено им), переносной компьютер или т.п., но не ограничены ими. Нужно отметить, что ключ шифрования может создаваться или в устройстве-источнике 150a, или в устройстве-адресате 150b, и/или в обоих. Другими словами, любое из устройства-источника 150a или устройства-адресата 150b может быть источником 170 ключей. Устройство-источник 150a и устройство-адресат 150b могут быть связаны с тем же самым предприятием или с отдельными предприятиями. В других вариантах осуществления один или оба из устройства-источника 150a и устройства-адресата 150b может быть проводным устройством, подходящим для осуществления связи с проводным или беспроводным устройством.

В некоторых вариантах осуществления устройство 110 подготовки ключей может быть частью предприятия, связанного с устройством-источником 150a и устройством-адресатом 150b. Предприятие

может быть организацией или структурным подразделением обеспечения безопасности, имеющим влияние по меньшей мере на одно устройство-источник 150a и/или устройство-адресат 150b. Относительно связи между устройством-источником 150a и устройством-адресатом 150b, связанными с отличающимися предприятиями, устройство-источник 150a может быть связано с первым предприятием, а устройство-адресат 150b может быть связано со вторым отличающимся предприятием. Предприятие может быть компанией, подгруппой в пределах компании, автономным и независимым субъектом, группой осуществления связи, поставщиком обеспечения безопасности, различными субъектами, организациями и/или т.п. Каждое устройство 110 подготовки ключей может выполнять действия по подготовке ключей для множества устройств, таких как устройство-источник 150a и устройство-адресат 150b, устанавливая иерархическую модель для подготовки ключей.

В других вариантах осуществления устройство 110 подготовки ключей может быть сторонним сервером, соединенным с предприятием, связанным с устройством-источником 150a и/или с устройством-адресатом 150b. Таким образом, различные варианты осуществления могут влиять на централизацию подготовки ключей шифрования в существующих системах и протоколах связи предприятия. Другими словами, устройство 110 подготовки ключей может воплощаться для взаимодействия с существующей технологией шифрования для осуществления связи, приложений и инфраструктуры. Подготовка ключей (например, с помощью стороннего или иного устройства) может взаимодействовать и с источниками, и с адресатами информации ключа (например, ключа шифрования и связанных с ним атрибутов 160 ключа). Соответственно контроль сверху донизу подготовки ключей может быть достигнут, поддерживая модель запроса, в которой устройство-источник 150a и устройство-адресат 150b могут запрашивать информацию ключа.

В некоторых вариантах осуществления источник 170 ключей может соединяться с устройством 110 подготовки ключей. Источник 170 ключей может быть любым источником, с помощью которого могут генерироваться ключи шифрования (или любые объекты безопасности других типов). В некоторых вариантах осуществления источник 170 ключей может быть частью устройства 110 подготовки ключей (например, модулем или базой данных в пределах устройства 110 подготовки ключей или соединенным с устройством 110 подготовки ключей). В других вариантах осуществления источник 170 ключей может быть источником, внешним к устройству 110 подготовки ключей. Источник 170 ключей может включать в себя устройство-источник 150a и/или устройство-адресат 150b, один или большее количество из которых может иметь возможность генерации ключей шифрования для осуществления связи между ними. Альтернативно или дополнительно источник 170 ключей может быть устройством, генерирующим ключи (другим, чем устройство-источник 150a и устройство-адресат 150b), внутренним или внешним по отношению тому же самому предприятию, как устройство-источник 150a и/или устройство-адресат 150b. В этих случаях источник 170 ключей может быть существующим специализированным устройством генерации ключей, воплощаемым отдельно от устройства 110 подготовки ключей (например, устройством 230 генерации и управления ключами на фиг. 2). Другие примеры источника 170 ключей могут включать в себя пользовательский интерфейс 220 управления на фиг. 2 (например, ключи шифрования могут генерироваться вручную через пользовательский интерфейс 220 управления), интерфейс 260 объединения ключей на фиг. 2 (например, ключей шифрования, генерируемых в отличающемся предприятии), различные базы данных, сохраняющие генерируемые ключи шифрования и/или т.п.

В различных вариантах осуществления запрос 175 можно посылать в устройство 110 подготовки ключей. Запрос 175 может быть запросом о генерации ключа шифрования. Например, устройство 110 подготовки ключей может само генерировать (или извлекать из базы данных, соединенной с устройством 110 подготовки ключей) ключи шифрования в ответ на запрос 175. В других примерах устройство 110 подготовки ключей может запрашивать ключ шифрования из других устройств (например, из источника 170 ключей) в пределах того же самого или отличающегося предприятия.

Запрос 175 может исходить из устройства-источника 150a, устройства-адресата 150b, самого устройства 110 подготовки ключей, стороннего устройства в пределах того же самого предприятия (например, из пользовательского интерфейса 220 управления, интерфейса 240 управления ключами и т.п.), стороннего устройства в отличающемся предприятии (например, из интерфейса 260 объединения ключей на фиг. 2) и/или т.п. Варианты осуществления устройства 110 подготовки ключей могут поэтому служить промежуточным устройством между устройством-источником 150a, устройством-адресатом 150b, устройством запроса (которое выдает запрос 175), источником 170 ключей и/или т.п. Соответственно управлением, распространением и объединением ключей можно эффективно управлять для различных устройств в том же самом или отличающемся предприятии.

Различные компоненты в пределах обобщенной системы 100 подготовки ключей шифрования (например, устройство 110 подготовки ключей, устройство-источник 150a, устройство-адресат 150b, само устройство 110 подготовки ключей, устройство 175, которое выдает запрос, источник 170 ключей и/или т.п.) могут подключаться через любую подходящую проводную или беспроводную сеть. Сеть может быть безопасной или небезопасной. Например, сеть может быть глобальной сетью связи, такой как Интернет, или одна или большее количество корпоративных сетей (интранет), локальных сетей (LAN), сетей стандарта Ethernet, общегородских сетей (MAN), глобальных сетей связи (WAN), их комбинаций или

т.п., но не ограничена ими. В конкретных вариантах осуществления сеть может представлять одну или большее количество безопасных сетей, сконфигурированных с соответствующими особенностями безопасности, такими как межсетевые экраны, шифрование или другое программное обеспечение или конфигурации оборудования, которые блокируют доступ к сетям связи неавторизованному персоналу или субъектам, но которые не ограничены ими.

В некоторых вариантах осуществления атрибуты 160 ключа могут относиться в общем случае к характеристикам, связанным с самим ключом шифрования, к характеристиками устройства, связанного с ключом шифрования, и/или т.п. Другими словами, атрибуты 160 ключа могут относиться к тому, когда, где, как, для чего, с помощью какого устройства ключ шифрования сгенерирован или его собираются генерировать. Примеры атрибутов 160 ключа могут включать в себя, но не ограничены ими, размер ключа шифрования, классификацию ключа шифрования, время, когда ключ шифрования сгенерирован или его собираются генерировать (например, с помощью источника 170 ключей), расположение, в котором ключ шифрования сгенерирован или его собираются генерировать (например, с помощью источника 170 ключей), роль, связанная с источником 170 ключей, роль, связанная с устройством-источником 150a, роль, связанная с устройством-адресатом 150b, роль, связанная с генерацией/сохранением ключа, роль, связанная с пользователем устройства-источника 150a, устройства-адресата 150b, устройства генерации/сохранения ключа, источника 170, их комбинации и/или т.п.

В некоторых вариантах осуществления атрибуты 160 ключа могут включать в себя размер ключа. Как правило, чем больше размер ключа (то есть чем длиннее ключ шифрования), тем больше безопасности может обеспечиваться для осуществления связи. Атрибуты 160 ключа могут также включать в себя классификацию ключа шифрования. В различных вариантах осуществления классификация ключа шифрования может относиться к его использованию, например, для чего может использоваться ключ шифрования. Примеры использования могут включать в себя (например, для систем связи), является или нет ключ шифрования глобальным скачкообразно изменяющимся ключом, является или нет ключ шифрования секретным ключом, является ли ключ шифрования симметричным или асимметричным, их комбинацию и/или т.п.

В некоторых вариантах осуществления атрибуты 160 ключа могут включать в себя время и/или расположение, в котором ключ шифрования сгенерирован или его собираются генерировать. Как описано, время и/или расположение, в котором может генерироваться ключ шифрования, могут определяться с позиции устройства-источника 150a, устройства-адресата 150b и/или любых других источников 170 ключей. Например, когда ключ шифрования генерируется (и/или посылается, принимается), может определяться соответствующее время устройства (например, источника 170 ключей), генерирующего (и/или посылающего, принимающего) ключ шифрования. Ключ шифрования может передаваться/сохраняться с временной меткой, представляющей время. Аналогично, когда ключ шифрования генерируется (и/или посылается, принимается), может определяться соответствующее георасположение устройства (например, источника 170 ключей), генерирующего (и/или посылающего, принимающего) ключ шифрования. Ключ шифрования может передаваться/сохраняться с георасположением.

В различных вариантах осуществления атрибуты 160 ключа могут включать в себя роль(и), связанную с устройством-источником 150a, устройством-адресатом 150b, источником 170 ключей, другим устройством генерации/сохранения ключа, а также связанного с ними пользователя. В частности, роль может относиться к группе/классификации (например, основываясь на предопределенном назначении, времени, георасположении устройства, генерирует или нет устройство ключи шифрования, передает или нет устройство ключи шифрования, принимает или нет устройство ключи шифрования и/или т.п.), в которую назначают устройство/пользователя, уровень допуска в системе безопасности, тип устройства/пользователя, их комбинация и/или т.п. В конкретных примерах каждое устройство/пользователь может связываться по меньшей мере с одной группой безопасности (например, назначенной серверу). В пределах каждой группы безопасности могут существовать подгруппы для дополнительного подразделения устройств/пользователей. Группы/подгруппы могут предопределяться с помощью любого подходящего персонала. В других или в дополнительных вариантах осуществления группы/подгруппы могут определяться, когда генерируется ключ шифрования (например, основываясь на существующих характеристиках устройства, таких как георасположение, время дня и/или т.п.).

Специалисты должны признать, что один или большее количество атрибутов 160 ключа могут связываться с заданным ключом шифрования. Фактически, как воплощается в различных вариантах осуществления, ключ шифрования может связываться с множеством атрибутов 160 ключа. Ключ шифрования может передаваться вместе со связанными с ним атрибутами 160 ключа к устройству (например, к устройству 110 подготовки ключей). Ключ шифрования и атрибуты 160 ключа, связанные с ключом шифрования, могут анализироваться согласно по меньшей мере одной политике, относящейся к атрибутам 160 ключа. Такой процесс может упоминаться как "отыскание неисправностей" атрибутов 160 ключа по отношению к соответствующим политикам или "предоставление" атрибутов 160 ключа для "анализа" с помощью политики.

Ключами шифрования можно в общем случае управлять с помощью набора политик 115. Как воплощается в различных вариантах осуществления, политика может относиться, по меньшей мере, к оп-

ределенному правилу, управляющему критериями для атрибутов 160 ключа. В некоторых вариантах осуществления средство обработки политик (например, которое внедрено в устройство 110 подготовки ключей и/или в другие устройства, которые описаны в данной работе) может принимать ключ шифрования и атрибуты 160 ключа, связанные с ключом шифрования, в качестве вводимой информации. Средство обработки политик может выводить ответ относительно того, является или нет ключ шифрования допустимым, основываясь на атрибутах 160 ключа. В конкретных вариантах осуществления средство обработки политик может выводить двоичный ответ (например, подтверждена пригодность или запрещено).

Ключ шифрования и связанные с ним атрибуты 160 ключа могут предоставляться для анализа один или большее количество раз за операцию связи. В некоторых вариантах осуществления ключ шифрования и связанные с ним атрибуты 160 ключа, возможно, должны предоставляться для анализа с помощью политики 115 один раз за операцию связи (например, на стадии инициирования перед тем, как происходит операция связи, но после того, как ключ шифрования сгенерирован). В других или дополнительных вариантах осуществления ключ шифрования и связанные с ним атрибуты 160 ключа, возможно, должны предоставляться для анализа с помощью политик 115 периодически и/или каждый раз, когда ключ шифрования изменяется для заданной операции связи. В некоторых случаях несколько ключей шифрования могут предоставляться для анализа с помощью политик 115 для заданной операции связи.

Средство обработки политик может идентифицировать принятые атрибуты 160 ключа. Средство обработки политик может извлекать соответствующую политику 115 из локальной или удаленной базы данных хранения. В других вариантах осуществления средство обработки политик может анализировать конкретные атрибуты 160 ключа (или иногда все атрибуты 160 ключа), связанные с ключом шифрования, когда средство обработки политик определяет пригодность, основываясь на предопределенном наборе политик 115. Например, средство обработки политик может определять, основываясь на соответствующей политике 115, является или нет ключ шифрования пригодным для операции связи, для которой может генерироваться ключ шифрования.

В одном не являющемся ограничивающим примере политики 115 могут указывать, что размер ключа шифрования должен находиться в пределах предопределенного диапазона (например, размер ключа шифрования должен превышать и/или быть меньше 128 бит, 192 бит, 256 бит и/или т.п.). В некоторых случаях политика 115 может указывать, что размер ключей шифрования должен быть конкретным размером ключа (например, 256-битовым и/или т.п.).

Политики 115 могут требовать, чтобы атрибут георасположения из атрибутов 160 ключа был связан (или не связан) с предопределенным расположением и/или находился в пределах (или вне пределов) предопределенной области. Например, когда атрибут георасположения ключа шифрования (например, который определяется с помощью георасположения устройства генерации, передачи и/или приема ключа шифрования) связан с "опасной" зоной, средство обработки политик может запрещать ключ шифрования. Это происходит потому, что может существовать высокая вероятность того, что ключ шифрования может быть скомпрометирован в опасной зоне. С другой стороны, когда атрибут георасположения ключа шифрования связан с "безопасной" зоной, тогда ключ шифрования может быть разрешен для операции связи. Это происходит потому, что может быть самое большее низкая вероятность компрометации ключей безопасности. В дополнительных вариантах осуществления "нейтральная" зона может быть безопасной зоной или альтернативно зоной, связанной с промежуточной вероятностью компрометации ключей безопасности.

В другом не являющемся ограничивающим примере политики 115 могут требовать, чтобы атрибут времени из атрибутов 160 ключа находился в пределах (или вне пределов) предопределенного периода времени. Политика 115 может запрещать ключ шифрования на том основании, что атрибут времени (например, временная метка), связанный с созданием, передачей и/или приемом данного ключа шифрования, может находиться за пределами предопределенного периода времени (например, в 3:00, причем пригодное время создания, передачи и/или приема ключа шифрования может быть между 9:00 утра - 17:00).

В различных вариантах осуществления политики 115 могут разрешать ключ шифрования, когда атрибут роли из атрибутов 160 ключа связан с устройством генерации/передачи/приема ключей шифрования (и с пользователем, связанным с данным устройством) в пределах предопределенной группы с подтвержденной пригодностью. В некоторых примерах устройство-источник 150a (устройство-адресат 150b или другие устройства-источники 170), связанный с первой группой безопасности в пределах предприятия, может генерировать ключ шифрования и предоставлять ключ шифрования для анализа с помощью политики 115. Средство обработки политик может определять, может или нет первая группа безопасности быть частью группы с подтвержденной пригодностью. Когда средство обработки политик определяет, что устройство-источник 150a (устройство-адресат 150b или другие устройства-источники 170) является частью группы с подтвержденной пригодностью (например, первая группа безопасности находится в пределах группы с подтвержденной пригодностью), ключ шифрования может быть разрешен для операции связи, для которой было создано шифрование.

Специалисты должны признать, что множество политик 115 может действовать совместно для схемы всестороннего управления ключами шифрования. Это подразумевает, что множество политик 115,

каждая из которых может регулировать по меньшей мере один отличающийся атрибут 160 ключа, может объединяться в набор политик 115 для регулирования ключей шифрования, предоставленных к средству обработки политик.

В других примерах другие источники 170 ключей (например, другие, чем устройство-источник 150a и устройство-адресат 150b) могут генерировать ключ шифрования, который будет распространяться (или принудительно отправляться) в устройство-источник 150a и/или устройство-адресат 150b для операции осуществления связи между этими устройствами. Средство обработки политик (например, устройство 110 подготовки ключей) может анализировать атрибуты 160 ключа для определения, является или нет ключ шифрования допустимым. В ответ на определение, что ключ шифрования является допустимым, устройство 110 подготовки ключей может определять, что следует распространить ключ шифрования к устройству-источнику 150a и/или к устройству-адресату 150b для операции связи.

В различных вариантах осуществления, когда средство обработки политик запрещает ключ шифрования, средство обработки политик может передавать указатель отклонения (например, сообщение "запрещено") к источнику 170 ключей. Устройство генерации ключей может повторно разрабатывать второй ключ шифрования, который будет предоставлен (вместе с атрибутами 160 ключа, связанными со вторым ключом шифрования) к средству обработки политик для второго цикла анализа. В других вариантах осуществления, когда средство обработки политик запрещает ключ шифрования, средство обработки политик может передавать сообщение "запрещено" к источнику 170 ключей вместе с причиной запрета (например, подсказкой) относительно того, какой атрибут 160 ключа привел к запрету и/или каким он должен быть.

Например, ключ шифрования с атрибутами 160 ключа, включающими в себя атрибут времени 4:49 утра, атрибут георасположения "безопасная зона" и атрибут роли "группа A безопасности", может предоставляться к набору политик 115. Средство обработки политик может разрешать ключ шифрования, когда ключ шифрования сгенерирован между 5:00 утра - 9:00 пополудни, в любой из "безопасной зоны" или "нейтральной зоны" и для групп безопасности A-C. Такой ключ шифрования может быть запрещен, учитывая, что он сгенерирован не между 5:00 утра - 9:00 пополудни. Средство обработки политик может передавать сообщение "запрещено" вместе с подсказкой атрибута времени (например, сгенерировать ключ шифрования после 5:00 утра, через 11 мин).

Соответственно устройство 110 подготовки ключей может конфигурироваться для управления ключами шифрования и распространения ключей шифрования. Другими словами, устройство 110 подготовки ключей может служить посредником между устройствами-источниками 150a, устройствами-адресатами 150b, другими источниками 170 ключей и/или т.п., поскольку эти сами устройства могут испытывать недостаток в возможности распространения и управления шифрованием таким образом, как сформулировано по отношению к устройству 110 подготовки ключей. Устройство 110 подготовки ключей может включать в себя множество модулей (или может соединяться с удаленными модулями) для каждой особенности, которая описана в данной работе. Кроме того, обобщенная система 100 подготовки ключей шифрования может соединяться по меньшей мере с одной другой аналогичной обобщенной системой 100 подготовки ключей шифрования для составления схемы объединения ключей шифрования, которая описана в данной работе.

Фиг. 2 - принципиальная схема, показывающая пример системы 200 подготовки ключей шифрования согласно различным вариантам осуществления. В некоторых вариантах осуществления система 200 подготовки ключей шифрования может показывать детализированное воплощение обобщенной системы 100 подготовки ключей шифрования. С точки зрения архитектуры варианты осуществления, которые показаны для системы 200 подготовки ключей шифрования, могут центрироваться вокруг передачи и хранения сообщений и функциональной совместимости с технологией генерации ключей, других устройств подготовки ключей, поддерживаемых систем связи, приложений и инфраструктуры.

Устройство 110 подготовки ключей может включать в себя, по меньшей мере, средство 205 обработки запроса управления, средство 210 обработки запроса, структуру 215 поддержки, интерфейс 260 объединения ключей, а также связанные базы данных (например, локальную базу 270 данных ключей, базу 275 данных операций, базу 280 данных политик, локальный репозиторий 285 пользователей, базу 290 данных конфигураций, базу 295 данных инвентаризации устройств).

В различных вариантах осуществления средство 205 обработки запроса управления может включать в себя (или быть им) средство обработки политик, которое может воплощаться для основанного на политике управления, распространения и объединения ключей шифрования. Поскольку средство 205 обработки запроса управления может быть промежуточным уровнем между различными описанными компонентами, быстрое интегрирование управления, распространения и объединения ключей шифрования, основанного на политике, может добавляться к существующей системе без необходимости производить изменения в обработке сообщений уровня системы. Средство 205 обработки запроса управления может обеспечивать управление сверху донизу для различных устройств связи (например, сотового устройства 250a, сетевого устройства 250b, ..., устройства N 250n и/или т.п.), связанных с заданным предприятием. В различных вариантах осуществления каждое сотовое устройство 250a, сетевое устройство 250b, ..., и устройство N 250n может быть устройством-источником 150a или устройством-адресатом 150b в зависи-

мости от конкретной операции связи, для которой генерируется ключ шифрования.

Средство 205 обработки запроса управления и средство 210 обработки запроса могут иметь отношения "агент-интерфейс". Таким образом, средство 210 обработки запроса может служить интерфейсом между средством 205 обработки запроса управления и различными устройствами связи, связанными с предприятием (например, сотовым устройством 250a, сетевым устройством 250b, ..., устройством N 250n и/или т.п.). Связь между средством 205 обработки запроса управления и средством 210 обработки запроса может облегчаться структурой 215 поддержки. Структура 215 поддержки может обеспечивать подходящий протокол связи, приложение управления, инфраструктуру, прикладной программный интерфейс (API) связи, конфигурации, преобразования и/или т.п. для взаимодействия между средством 205 обработки запроса управления и средством 210 обработки запроса.

Средство 210 обработки запроса может принимать запросы 175 о генерации ключей и/или ключей шифрования из различных устройств связи и передавать их к средству 205 обработки запроса управления с помощью структуры 215 поддержки. Средство 210 обработки запроса может также передавать ответ средства 205 обработки запроса управления (включающий в себя подсказки в некоторых вариантах осуществления) и/или ключи шифрования на различные устройства связи с помощью структуры 215 поддержки.

В различных вариантах осуществления средство 205 обработки запроса управления может принимать запрос 175 о генерации ключей шифрования. Различные компоненты могут иметь возможность передавать запрос 175 на средство 205 обработки запроса управления. В некоторых вариантах осуществления средство 205 обработки запроса управления может принимать запрос 175 из различных устройств связи, связанных с предприятием (например, из сотового устройства 250a, сетевого устройства 250b, ..., устройства N 250n и/или т.п.). Запрос 175 может рассматриваться с помощью средства 210 обработки запроса, которое может служить интерфейсом между устройствами и средством обработки запроса управления, как описано. Интерфейс 260 объединения ключей, пользовательский интерфейс 220 управления и интерфейс 240 управления ключами могут также передавать запрос 175 на средство обработки запроса управления.

В "не управляемых запросом" вариантах осуществления средство 205 обработки запроса управления может принимать ключи шифрования по меньшей мере из одного источника 170 ключей. Источник 170 ключей может быть устройством 230 генерации и управления ключами, которое может быть любым подходящим существующим устройством генерации ключей шифрования, воплощаемым в пределах предприятия. Другими словами, устройство 230 генерации и управления ключами может представлять любые существующие схемы, внутренние или внешние по отношению к системам связи предприятия. Например, устройство 230 генерации и управления ключами может иметь любой подходящий собственный протокол, связанный с безопасным сетевым оборудованием.

Варианты осуществления интерфейса 240 управления ключами могут предоставлять внутреннее интегрирование возможностей генерации ключей и управления ключами, а также внешнего интерфейса, с существующими решениями. Это происходит потому, что интерфейс 240 управления ключами можно балансировать между устройством 230 генерации и управления ключами (которое может генерировать ключи шифрования) и средством 205 обработки запроса управления (которое анализирует атрибуты 160 ключа из ключей шифрования, основываясь на политиках 115). Например, интерфейс 240 управления ключами может быть интерфейсом преобразования, который поддерживает стандартный язык обмена сообщениями управления шифрованием с устройством 110 подготовки ключей. Это может предоставлять возможность совместимости предприятий с существующими решениями (например, с устройством 230 генерации и управления ключами) и с платформой подготовки ключей (например, со средством 205 обработки запроса управления). Соответственно основанные на политиках системы и способы подготовки ключей шифрования могут воплощаться с различными типами протоколов генерации объекта безопасности (например, ключа шифрования).

Дополнительно или альтернативно в управляемых запросом вариантах осуществления пользовательский интерфейс 220 управления может передавать запрос 175 на средство 210 обработки запроса управления. Пользовательский интерфейс 220 управления может использовать тот же самый API, как другие компоненты, описанные в данной работе, чтобы гарантировать функциональную совместимость. Пользовательский интерфейс 220 управления может включать в себя подходящие пользовательские устройства ввода и отображения для приема и отображения данных определенному управляющему пользователю. В конкретных вариантах осуществления пользовательский интерфейс 220 управления может включать в себя мобильное устройство, такое как смартфон или планшет. Пользовательский интерфейс 220 управления может также включать в себя проводное устройство.

В некоторых вариантах осуществления интерфейс 260 объединения ключей может передавать запрос 175 на средство 205 обработки запроса управления. Интерфейс 260 объединения ключей может осуществлять связь со вторым интерфейсом объединения ключей (таким как интерфейс 260 объединения ключей, но который не ограничен им), связанным с отличающимся предприятием (который может использовать те же самые или аналогичные описанные системы и способы подготовки ключей). Когда одно из различных устройств связи (например, сотовое устройство 250a, сетевое устройство 250b, ..., устрой-

ство N 250n и/или т.п.) хочет осуществлять связь с другим устройством из отличающегося предприятия (или наоборот), запрос 175 может передаваться (от интерфейса 260 объединения ключей из второго предприятия) к интерфейсу 260 объединения ключей существующего предприятия. В некоторых вариантах осуществления запрос 175 может непосредственно передаваться на средство 205 обработки запроса управления, когда интерфейс 260 объединения ключей определяет, что отношения между предприятиями являются доверительными.

В некоторых вариантах осуществления вместо или в дополнение к запросу 175 ключи шифрования, а также сообщения "разрешено" и "запрещено" могут передаваться и приниматься между интерфейсами 260 объединения ключей (существующего и второго предприятия). Ключ шифрования и связанные с ним атрибуты 160 могут сохраняться в локальной базе 270 данных ключей, которая может быть доступной с помощью средства 205 обработки запроса управления (для анализа с помощью политики) и/или средства 210 обработки запроса (для распространения).

Запрос 175 может передаваться с дополнительными командами, относящимися к генерации ключей шифрования. Дополнительные команды включают в себя источник ключей шифрования, сами ключи шифрования, атрибуты 160 ключа, связанные с ключами шифрования, и/или т.п., но не ограничены ими.

В различных вариантах осуществления в ответ на прием запроса 175 средство 205 обработки запроса управления может генерировать или облегчать генерацию ключа шифрования. Например, когда запрос 175 может быть без указания того, где ключ шифрования должен генерироваться (например, источника 170 ключей), само средство 205 обработки запроса управления может генерировать ключ шифрования. Средство 205 обработки запроса управления может генерировать ключ шифрования, основываясь на наборе политик 115, сохраненных в базе 280 данных политик. Другими словами, средство 205 обработки запроса управления может генерировать ключи шифрования с атрибутами 160 ключа, которые не будут нарушать политики 115, сформулированные в базе 280 данных политик.

Когда запрос 175 не указывает, где ключ шифрования должен генерироваться (например, источник 170 ключей), или когда определяет конкретный источник 170 ключей для генерации ключей шифрования, средство 205 обработки запроса управления может извлекать или иначе запрашивать ключ шифрования из подходящего источника 170 ключей. Средство 205 обработки запроса управления может запрашивать ключи шифрования из пользовательского интерфейса 220 управления, интерфейса 260 объединения ключей, устройства связи (например, сотового устройства 250a, сетевого устройства 250b, ..., устройства N 250n, устройства-источника 150a и устройства-адресата 150b), интерфейса 240 управления ключами и/или т.п.

Средство 205 обработки запроса управления может извлекать ключи шифрования из определенной базы данных, хранящей ключи шифрования (например, из локальной базы 270 данных ключей). Локальная база 270 данных ключей может соединяться с другим источником 170 ключей (например, с сотовым устройством 250a, сетевым устройством 250b, ..., устройством N 250n, устройством-источником 150a, устройством-адресатом 150b, устройством 230 генерации и управления ключами, интерфейсом 260 объединения ключей и/или т.п.) и хранить кэшированные ключи шифрования в интересах других источников 170 ключей. Средство 205 обработки запроса управления может извлекать ключи шифрования из локальной базы 270 данных ключей вместо того, чтобы запрашивать ключи шифрования из источников 170 ключей. Это происходит потому, что время операции для извлечения/генерации ключей шифрования может улучшаться и что проблемы сети не будут препятствовать возможности средства 205 обработки запроса управления получать ключи шифрования, при условии, что локальная база данных ключей может быть локальной (например, постоянно находиться в том же самом узле сети) для средства 205 обработки запроса управления. Поскольку средство 205 обработки запроса управления извлекает ключи шифрования из локальной базы 270 данных ключей, запрос проверки можно посылать к источнику 170 ключей, чтобы убедиться, был или нет ключ шифрования, который будет извлекаться, изменен с помощью источника 170 ключей. Подтверждение или обновленный ключ шифрования можно посылать в ответ в локальную базу 270 данных ключей так, чтобы средство 205 обработки запроса управления могло соответствующим образом принимать ключ шифрования.

В некоторых вариантах осуществления средство 205 обработки запроса управления после приема ключей шифрования (или запрашиваемого, или нет) любым способом, как описано, может кэшировать ключ шифрования вместе с идентификатором источника ключа и связанными атрибутами 160 ключа в локальной базе 270 данных ключей. Ключ шифрования, идентификатор источника ключа и атрибуты 160 ключа могут сохраняться в случае, когда связь потеряна или когда источник ключа шифрования не является заслуживающим доверия. При этом в некоторых вариантах осуществления ключ шифрования может не передаваться с атрибутами 160 ключа. В таких вариантах осуществления средство 205 обработки запроса управления может определять атрибуты 160 ключа из различных источников, таких как локальный репозиторий 285 пользователей, база 295 данных инвентаризации устройств и/или т.п., но которые не ограничены ими.

Средство 205 обработки запроса управления может затем анализировать атрибуты 160 ключа, связанные с принятым ключом шифрования, основываясь на наборе политик 115, сохраненных в базе 280 данных политик. Средство 205 обработки запроса управления может извлекать все политики 115 или

только соответствующие политики (например, основываясь на некоторых или на всех атрибутах 160 ключа) из базы 280 данных политик. В некоторых вариантах осуществления ключи шифрования, генерируемые с помощью самого средства 205 обработки запроса управления или по указанию средства 205 обработки запроса управления, могут освобождаться от анализа с помощью политик 115, когда они создаются, основываясь на политиках 115. В других вариантах осуществления все ключи шифрования, генерируемые с помощью средства 205 обработки запроса управления или в направлении средства 205 обработки запроса управления, могут анализироваться с помощью политик 115. Ключи шифрования, допустимые, основываясь на политиках 115, могут разрешаться, в то время как недопустимые ключи шифрования могут запрещаться описанным образом. Средство 205 обработки запроса управления может конфигурироваться для обновления или добавления политик, сохраненных в базе 280 данных политик (например, как предписывается с помощью пользовательского интерфейса 220 управления).

Локальный репозиторий 285 пользователей может быть базой данных, хранящей информацию, относящуюся к локальным пользователям устройств связи (например, сотового устройства 250a, сетевого устройства 250b, ..., устройства N 250n и/или т.п.) в пределах предприятия. В различных вариантах осуществления локальный репозиторий 285 пользователей может хранить характеристики/информацию о пользователях, которые формируют атрибуты 160 ключа. Характеристики включают в себя привилегии, группы безопасности, назначенные роли, их комбинации и/или т.п., но не ограничены ими. Группы безопасности могут сохраняться в иерархическом дереве. Средство 205 обработки запроса управления может получать доступ к локальному репозиторию 285 пользователей для таких характеристик и использовать их в качестве атрибутов 160 ключа, связанных с запрашиваемыми ключами шифрования, переданными или принятыми этим устройством, соответствующим таким характеристикам. Средство 205 обработки запроса управления может добавлять или изменять информацию, хранящуюся в локальном репозитории 285 пользователей. Копию информации, хранящейся в локальном репозитории 285 пользователей, можно посылать в локальную базу 270 данных ключей в качестве атрибутов 160 ключа для сохранения в локальной базе 270 данных ключей.

В некоторых вариантах осуществления база 275 данных операций может хранить различные операции осуществления связи или возможные операции осуществления связи. В некоторых вариантах осуществления база 275 данных операций может хранить конкретные случаи передачи ключей шифрования (то есть конкретные случаи, когда ключи шифрования должны распространяться) на одно или большее количество устройств. Например, когда конкретный ключ шифрования ни по какой причине не может/не должен направляться (например, принудительно отправляться в устройство связи), операция отправления (например, задание) может ставиться в очередь или иначе сохраняться в пределах базы 275 данных операций для более позднего направления ключа шифрования. База 275 данных операций может также хранить состояние каждого конкретного случая передачи ключа шифрования, который может позже считываться с помощью средства 210 обработки запроса. Например, средство 210 обработки запроса может позднее пытаться передать все или некоторые ключи шифрования на соответствующие устройства связи для всех «неотправленных» случаев передачи ключа шифрования. База 275 данных операций может соединяться с локальной базой 270 данных ключей для получения доступа к ключам, которые будут направлены к каждому устройству связи, для которого может генерироваться ключ шифрования.

В дополнительных вариантах осуществления база 275 данных операций может соединяться со средством 210 обработки запроса и может сохранять операции осуществления связи (для которой ключ шифрования можно запрашиваться, передаваться или приниматься) и/или связанные атрибуты 160 ключа. Например, средство 210 обработки запроса может передавать такую информацию к базе 275 данных операций. База 275 данных операций может соединяться с локальной базой 270 данных ключей. Операции осуществления связи (как связанные с ней подробности) могут связываться с ключами шифрования, сохраненными в локальной базе 270 данных ключей. Средству 205 обработки запроса управления может требоваться получать доступ только к локальной базе 270 данных ключей для ключей шифрования и связанных атрибутов 260 ключей.

База 290 данных конфигураций может хранить команды поддержки для системы 200 подготовки ключей шифрования. В некоторых вариантах осуществления база 290 данных конфигураций может хранить внутреннюю сеть, конфигурацию клиентов, конфигурацию приложений, распределение IP-адресов, конфигурации различных компонент, привилегии устройства, маршруты осуществления связи устройства, регистрационные данные и/или т.п. База 290 данных конфигураций может соединяться со средством 205 обработки запроса управления, которому могут потребоваться команды, сохраненные в пределах базы 290 данных конфигураций, для операций. Средство 205 обработки запроса управления может также добавлять или изменять информацию, хранящуюся в базе 290 данных конфигураций.

В некоторых вариантах осуществления база 295 данных инвентаризации устройств может хранить информацию, относящуюся к устройствам связи, связанным с заданным предприятием. Например, хранящаяся информация может включать в себя группу безопасности, уровень безопасности, георасположение, идентификационный номер, внутреннюю классификацию, спецификацию устройства, временную метку, когда шифрование было создано, их комбинации и/или т.п., но не ограничена ими. Средство 210 обработки запроса может соединяться с базой 295 данных инвентаризации устройств для сохранения в

ней таких данных. Средство 205 обработки запроса управления может соединяться с базой 295 данных инвентаризации устройств для получения доступа к такой информации об устройстве. База 295 данных инвентаризации устройств предназначена для связи конкретных кэшированных ключей с соответствующей информацией об устройстве в качестве атрибутов 160 ключа. Копию информации, хранящейся в базе 295 данных инвентаризации устройств, можно посылать в локальную базу 270 данных ключей в качестве атрибутов 160 ключа.

Интерфейс 260 объединения ключей может предоставлять возможность одному устройству 110 подготовки ключей объединять информацию ключа шифрования с одним или большим количеством других устройств 110 подготовки ключей (через связанные с ними соответствующие интерфейсы 260 объединения ключей), основываясь на установленных доверительных отношениях. Каждое предприятие может включать в себя устройство 110 подготовки ключей. Также интерфейс 260 объединения ключей может поддерживать доверительные отношения с системами связи по меньшей мере одного другого предприятия. Другими словами, это шлюз для расширения доверия.

Фиг. 3 показывает пример системы 300 объединения ключей шифрования, которая воплощается в различных вариантах осуществления. Система 300 объединения ключей может воплощать устройство 110 подготовки ключей, которое формулируется относительно фиг. 1-2. Система 300 объединения ключей может основываться на отношениях осуществления связи вне предприятия и объединении ключей, разрешенном с помощью устройства 110 подготовки ключей (например, средства 205 обработки запроса управления и связанных компонент).

Ключи шифрования (например, асимметричные ключи шифрования, симметричные ключи шифрования и/или т.п.), генерируемые с помощью компонент в пределах одного предприятия (например, предприятия A 390a), могут распространяться к отличающемуся устройству подготовки ключей (например, к устройству 110 подготовки ключей, средству 205 обработки запроса управления и связанным с ними компонентам и/или т.п.) другого предприятия (например, предприятия B 390b) в соответствии с анализом с помощью политик 115 любого (или обоих) предприятия. Это может предоставлять возможность обеспечения связи или обмена данными с внешними объектами (например, предприятиями), основываясь на объединенной модели доверия. Это может также предоставлять возможность управлению шифрованием параллельно управлять осуществлением связи для поддержки внешних связей для предоставления возможности шифрования с симметричным ключом при осуществлении связи. Соответственно производительность платформы осуществления связи может улучшаться при условии, что использование асимметричного шифрования может быть дорогим с точки зрения обработки по сравнению с симметричным шифрованием.

В системе 300 объединения ключей каждое предприятие (например, предприятие A 390a или предприятие B 390b) может связываться с соответствующим устройством A 310a подготовки ключей и устройством B 310b подготовки ключей). Каждое устройство A 310a подготовки ключей и устройство B 310b подготовки ключей может быть устройством 110 подготовки ключей. Устройство A 310a подготовки ключей и устройство B 310b подготовки ключей могут связываться друг с другом через любую подходящую сеть. В частности, интерфейсы объединения ключей (например, интерфейс 260 объединения ключей) каждого устройства A 310a подготовки ключей и устройства B 310b подготовки ключей могут связываться друг с другом.

В различных вариантах осуществления сервер A 330a управления ключами и сервер B 330b управления ключами могут быть устройством, таким как устройство 230 генерации и управления ключами и интерфейс 240 управления ключами, но которое не ограничено ими. Каждый сервер A 330a управления ключами и сервер B 330b управления ключами может соединяться с соответствующим ему интерфейсом 206 объединения ключей в пределах соответствующих им предприятий описанным образом.

Устройство A 350a и устройство B 350b могут пытаться получить ключ шифрования для осуществления связи между ними. Каждое устройство A 350a и устройство B 350b может быть устройством-источником 150a, устройством-адресатом 150b, сотовым устройством 250a, сетевым устройством 250b, ..., устройством N 250n, их комбинацией и/или т.п.

Ключ шифрования может генерироваться в пределах одного предприятия (например, предприятия A 390a) с помощью любого подходящего источника 170 ключей описанным образом. Ключ шифрования может генерироваться с помощью предприятия A 390a (например, источника 170 ключей в предприятии A 390a) с запросом 170 или без него или из предприятия B 390b, или в пределах предприятия A. Ключ шифрования может также генерироваться с помощью предприятия B 390b аналогичным образом. Ключ шифрования и связанные с ним атрибуты 160 ключа могут предоставляться к средству обработки политик предприятия A 390a (например, к устройству A 310a подготовки ключей, которое может включать в себя средство 205 обработки запроса управления и связанные с ним компоненты) для анализа описанным образом. В ответ на то, что средство обработки политик предприятия A 390a определяет, что ключ шифрования пригоден, основываясь на атрибутах 160 ключа шифрования, устройство 310a подготовки ключей (например, интерфейс 260 объединения ключей) предприятия A 390a может информировать о ключе шифрования, а также о связанных с ним атрибутах 160 ключа, устройство B 310b подготовки ключей (например, интерфейс 260 объединения ключей) предприятия B 390b.

После приема ключа шифрования и связанных с ним атрибутов 160 ключа ключ шифрования и связанные с ним атрибуты 160 ключа могут предоставляться к средству обработки политик предприятия B 390b (например, к устройству B 310b подготовки ключей, которое может также включать в себя средство 205 обработки запроса управления и связанные с ним компоненты) для анализа описанным образом. Ключ шифрования может направляться и к устройству A 350a, и к устройству B 350b, когда устройство B 310b подготовки ключей определяет, что ключ шифрования совместим со своими политиками 115, определенными для предприятия B 390b. Другими словами, ключ шифрования (который определяется с помощью его атрибутов 160 ключа) может быть разрешен, только если он совместим с набором политик 115 предприятия A 390a так же хорошо, как с набором политик предприятия B 390b. По меньшей мере часть набора политик 115 предприятия A 390a может отличаться по меньшей мере от части набора политик 115 предприятия B 390b. При условии, что ключ шифрования найден недопустимым или с помощью устройства A 310a подготовки ключей, или с помощью устройства B 310b подготовки ключей, ключ шифрования может возвращаться назад к источнику 170 ключей с сообщением "запрещено" и/или с подсказкой описанным образом.

В других вариантах осуществления подтверждение пригодности с помощью политик 115, связанных только с одним предприятием (например, или с предприятием A 390a, или с предприятием B 390b), может быть достаточным для того, чтобы ключ шифрования был разрешен. В таких случаях доверие простирается на некоторые или иногда на все политики 115. Кроме того, каждое предприятие может включать в себя набор политик 115 для конкретных случаев объединения (например, каждое предприятие, возможно, пришло к соглашению с другим относительно набора политик 115, используемых, когда должно происходить осуществление связи между устройствами связи предприятий. Соответственно каждое предприятие может хранить (например, в каждой соответствующей базе 280 данных политик) одинаковое множество объединенных (совместных и двусторонних) политик для объединенных схем. Объединенные политики могут быть одинаковыми и для предприятия A 390a, и для предприятия B 390b. Таким образом, разрешение с помощью одного устройства подготовки ключей, связанного с одним предприятием, может быть достаточным для того, чтобы ключ шифрования был направлен для использования для осуществления связи между обоими предприятиями.

В различных вариантах осуществления политики объединения предприятия могут сохраняться в пределах каждой базы 280 данных политик. Политики объединения предприятия могут определять способ, которым ключи шифрования могут объединяться. Например, политики объединения предприятия могут определять объединенные политики, какое устройство подготовки ключей может анализировать атрибуты 160 ключа, какое предприятие может выдавать запрос 175 о ключе шифрования, какое предприятие может генерировать ключ шифрования, их комбинацию и/или т.п. Политики объединения предприятия предоставляют возможность гибкости при определении политики. Например, политики объединения предприятия могут определять, что каждое из предприятий может включать в себя свои собственные политики 115 в дополнение к объединенным политикам, причем по меньшей мере часть политики 115 каждого предприятия может отличаться.

В некоторых вариантах осуществления платформа A 320a осуществления связи и платформа B 320b осуществления связи каждого соответствующего предприятия могут осуществлять связь друг с другом через любую подходящую сеть. Такая связь между платформами осуществления связи может быть зашифрованной связью, причем ключ шифрования, соответствующий такой связи, может также предоставляться для анализа с помощью политик 115, аналогично описанному по отношению к устройствам (например, к устройству A 350a, устройству B 350b и/или т.п.). Каждая платформа осуществления связи может осуществлять связь с соответствующим устройством так, что можно обмениваться конфигурациями, относящимися к системам подготовки ключей.

Фиг. 4 показывает пример устройства 400 связи, использующего услуги подготовки ключей как часть предприятия согласно некоторым вариантам осуществления. Что касается фиг. 1-4, устройство 400 связи может быть таким устройством, как устройство-источник 150a, устройство-адресат 150b, сотовое устройство 250a, сетевое устройство 250b, ..., устройство N 250n, устройство A 350a, устройство B 350b, их комбинация и/или т.п., но не ограничено ими. В некоторых вариантах осуществления устройство 400 связи использует подготовку ключей для приема в устройстве 400 связи ключей шифрования (или обновлений ключей), связанных с приложениями, такими как приложение 410a электронной почты (E-mail), приложение 410b передачи голоса по Интернет-протоколу (VOIP), шифрование 410c запоминающего устройства и/или другие приложения 410d шифрования, но которые не ограничены ими.

Устройство 400 связи может регистрироваться на платформе подготовки ключей для приема услуги подготовки ключей. Устройство 400 связи может обеспечивать интерфейс 420 приложений, конфигурируемый для приема распространяемых ключей шифрования и сообщений управления ключами шифрования (например, сообщения "разрешено", сообщения "запрещено", подсказки и/или т.п.) из устройства 110 подготовки ключей. Интерфейс 420 приложений может соединяться с каждым из приложения 410a электронной почты (E-mail), приложения 410b передачи голоса по Интернет-протоколу (VOIP), шифрования 410c запоминающего устройства и/или других приложений 410d шифрования для направления им принятого ключа шифрования.

Это устройство 400 связи может также использовать KMIP с помощью прокси-сервера 430 KMIP для приема команд типа KMIP из устройства 110 подготовки ключей. Прокси-сервер 430 KMIP может подключаться к хранилищу 440 ключей для управления ключами шифрования, сохраненными в нем. Прокси-сервер 430 KMIP может также подключаться к криптографическому блоку 450 на стороне устройства. Криптографический блок 450 на стороне устройства может конфигурироваться для генерации ключей шифрования. В ответ на сообщение "запрещено" криптографический блок 450 на стороне устройства может генерировать другой ключ шифрования для предоставления к средству обработки политик для анализа. Если подсказка задается, то криптографический блок 450 на стороне устройства может генерировать другой ключ шифрования, основываясь на подсказке. Криптографический блок 450 на стороне устройства может кэшировать свои ключи шифрования в хранилище 440 ключей. Криптографический блок 450 на стороне устройства может соединяться с интерфейсом 420 приложений. Интерфейс 420 приложений может передавать генерируемые ключи шифрования вместе с атрибутами 160 ключей к средству обработки политик и направлять ответ средства обработки политик к криптографическому блоку 450 на стороне устройства, например, когда ответ является отрицательным.

Соответственно может достигаться анализ с помощью политики на уровне операции. Учитывая, что устройство 400 связи может иметь возможность взаимодействовать со средством обработки политик по отношению к ключам шифрования, может обеспечиваться возможность обслуживать запрос о ключе шифрования (или анализировать ключ шифрования) с помощью стороннего устройства (например, средства обработки политик, постоянно находящегося в устройстве 110 подготовки ключей), действующего в качестве средства администрирования. Запрос 175 ключа шифрования или ключ шифрования может обслуживаться каждую операцию связи.

Фиг. 5 показывает пример процесса 500 аутентификации запроса для выдачи запросов 175 о ключах шифрования в различных системах подготовки ключей шифрования согласно некоторым вариантам осуществления. Процесс 500 аутентификация запроса может быть внутренним по отношению к устройству 110 подготовки ключей, когда устройство 110 подготовки ключей (например, средство 205 обработки запроса управления, устройство A 310a подготовки ключей, устройство B 310b подготовки ключей и/или т.п.) само генерирует ключи шифрования. В других вариантах осуществления процесс 500 аутентификации запроса может быть внешним по отношению к устройству 110 подготовки ключей для поддержания интеграции с существующей инфраструктурой управления ключами и генерации ключей (например, с помощью устройства 230 генерации и управления ключами, сервера A 330a управления ключами, сервера B 330b управления ключами и/или т.п.).

Сначала на этапе B510 устройство 110 подготовки ключей может обеспечивать информацию аутентификации к источнику 170 ключей. Как описано, такой источник 170 ключей может быть самим устройством 110 подготовки ключей, устройством 230 генерации и управления ключами, пользовательским интерфейсом 220 управления, интерфейсом 260 объединения ключей, устройством связи (например, сотовым устройством 250a, сетевым устройством 250b, ..., устройством N 250n, устройством-источником 150a, устройством-адресатом 150b, устройством A 350a, устройством B 350b, устройством 400 связи, их комбинацией и/или т.п.) и/или другими внешними источниками ключа. Информация аутентификации может быть любым подходящим способом аутентификации, таким как запрос имени пользователя/кода доступа, алгоритмы безопасного установления связи, биометрический запрос, их комбинация и/или т.п.

Затем на этапе B520 устройство 110 подготовки ключей может принимать ответ аутентификации из источника 170 ключей. Устройство 110 подготовки ключей может аутентифицировать ответ и устанавливать доверительные отношения между источником 170 ключей и устройством 110 подготовки ключей. Затем на этапе B530 устройство 110 подготовки ключей, пользовательский интерфейс 220 управления, устройство 230 генерации и управления ключами, устройства связи и другие вызовы API могут выдавать запрос об управлении/генерации ключей (например, запрос 175) к источнику 170 ключей. В некоторых вариантах осуществления устройство 110 подготовки ключей может направлять запрос 175 из доверенного стороннего устройства (например, из устройства связи, пользовательского интерфейса 220 управления, интерфейса 260 объединения ключей и/или других сторонних устройств) к источнику 170 ключей. В некоторых вариантах осуществления запрос 175 можно непосредственно посылать к источнику 170 ключей. Устройство 110 подготовки ключей может конфигурироваться для определения, генерировать ли ключи шифрования самостоятельно или направлять запрос к другому источнику 170 ключей, когда запрос 175 не идентифицирует источник 170 ключей. Затем на этапе B540 устройство 110 подготовки ключей может принимать ответ (например, ключи шифрования, которые запрашивались) из источника 170 ключей.

Впоследствии ключи шифрования, полученные с помощью устройства 110 подготовки ключей, могут оцениваться описанным образом, основываясь на атрибутах 160 ключей и политиках 115. Когда разрешено, ключи шифрования могут распространяться к устройствам связи, связанным с соответствующей операцией связи. Когда запрещено, устройство 110 подготовки ключей может передавать сообщение "запрещено" (и в некоторых случаях, подсказку) и ожидать новых ключей шифрования.

В некоторых вариантах осуществления множество запросов можно посылать во множество источников 170 ключей, каждый запрос может соответствовать одной операции связи. В ответ множество от-

ветов (например, ключей шифрования) могут приниматься из источников 170 ключей. В других вариантах осуществления множество запросов можно посылать во множество источников 170 ключей, причем два или большее количество запросов могут соответствовать той же самой операции связи. Поскольку устройство 110 подготовки ключей может принимать два или большее количество ключей шифрования из источников 170 ключей, устройство 110 подготовки ключей может определять один из этих двух или большего количества ключей шифрования для операции связи, основываясь на политиках 115 (например, самый безопасный из этих двух или большего количества ключей шифрования).

Соответственно крупномасштабное распространение с помощью устройства 110 подготовки ключей возможно в системах, включающих в себя по меньшей мере один источник ключей шифрования и множество устройств связи - получателей.

Фиг. 6 - последовательность операций процесса, показывающая пример процесса 600 регистрации устройства связи, воплощаемого в различных системах подготовки ключей согласно различным вариантам осуществления. Этапы B610, B620, B630 могут выполняться одновременно или последовательно в заданном порядке. Сначала на этапе B610 устройство связи может обнаруживаться (например, с помощью средства 210 обработки запроса). Средство 210 обработки запроса может автоматически обнаруживать, что устройство связи присутствует в пределах предприятия (например, сетей, связанных с предприятием).

На этапе B620 устройство связи может регистрироваться (например, с помощью средства 210 обработки запроса). В некоторых вариантах осуществления информация о конфигурации, относящейся к системам подготовки ключей, может передаваться на устройство связи. Информация об устройстве связи может передаваться к локальному репозиторию 285 пользователей, базе 295 данных инвентаризации устройств и/или т.п. На этапе B630 устройство связи может присоединяться (например, с помощью средства 210 обработки запроса). Например, устройство связи может передавать запрос аутентификации сервера на средство 210 обработки запроса и принимать положительный ответ разрешения.

Затем на этапе B640 может подтверждаться пригодность устройства связи (например, с помощью средства 210 обработки запроса). Например, средство 210 обработки запроса и/или средство 205 обработки запроса управления могут проверять существующие политики 115, основываясь на информации об устройстве, для определения, было или нет устройство связи классифицировано в соответствующей группе, может или нет устройство 110 подготовки ключей иметь возможность управления устройством связи, их комбинацию и/или т.п.

Затем на этапе B650 средство 210 обработки запроса может обеспечивать информацию аутентификации устройства на устройство связи. Информация аутентификации может включать в себя конфигурации (например, регистрационные данные, коды доступа и/или т.п.) для получения доступа к устройству 110 подготовки ключей. Затем на этапе B660 средство 210 обработки запроса и/или средство 205 обработки запроса управления могут определять правила подготовки для устройства связи. После этапа B660 на этапе B670 соответствующий идентификатор, устройство угрозы добавлено к регистрации подготовки. Впоследствии устройство связи может запрашивать ключи шифрования, генерировать ключи шифрования, принимать одобренные ключи шифрования и/или т.п. описанным образом. Такой процесс гарантирует, что устройства связи, использующие услуги, обеспечиваемые с помощью устройства 110 подготовки ключей, могут соответствовать действующим стандартам устройства 110 подготовки ключей.

Фиг. 7 показывает пример процесса 700 управления и распространения ключей согласно различным вариантам осуществления. Что касается фиг. 1-7, процесс 700 управления и распространения ключей может воплощаться с устройствами связи, зарегистрированными, обнаруженными и/или присоединенными с помощью устройства 110 подготовки ключей.

Сначала на этапе B710 средство 205 обработки запроса управления может определять команду управления ключами. Команда управления ключами может быть конкретной командой для события управления ключами (например, "заданием"). Событие управления ключами может быть событием, запускающим набор алгоритмов для создания ключей шифрования, основываясь на политиках 115, и распространения (например, принудительной отправки ключей шифрования по меньшей мере в одно из устройств связи (например, в сотовое устройство 250a, сетевое устройство 250b, ..., устройство N 250n, устройство-источник 150a, устройство-адресат 150b, устройство A 350a, устройство B 350b, устройство 400 связи, их комбинацию и/или т.п.).

В некоторых вариантах осуществления событие управления ключами может основываться на времени. Например, средство 205 обработки запроса управления может конфигурироваться для повторного создания ключей, по меньшей мере, для некоторых (иногда всех) устройств связи, связанных с предприятием (или с другим предприятием) периодически (например, каждый день, каждую неделю, каждый месяц и/или т.п.). В различных вариантах осуществления событие управления ключами может происходить автоматически через вызов API. Вызов API может выдаваться из любых компонент, внутренних и/или внешних, к устройству 110 подготовки ключей в пределах того же самого или отличающегося предприятия.

Событие управления ключами может также определяться пользователем. Например, пользовательский интерфейс 220 управления может принимать вводимую пользователем информацию от назначенного пользователя для немедленной генерации ключей шифрования по меньшей мере для одного устройст-

ва связи. В таких примерах такие определяемые пользователем события управления ключами могут инициироваться в ответ на внезапное событие, которое включает в себя кибератаки, нарушение правил безопасности, изменение в политике 115 и/или т.п. Пользовательский интерфейс 220 управления может также изменять политики 115, сохраненные в пределах базы 280 данных политик, в ответ на эти события управления ключами. Создаваемые новые ключи шифрования должны соответствовать измененному набору политик 115.

Команда управления ключами может включать в себя обеспечение ключа шифрования в некоторые или во все устройства связи в пределах того же самого или отличающегося предприятия, повторную передачу того же самого или отличающегося ключа шифрования в некоторые или во все устройства связи в пределах того же самого или отличающегося предприятия, их комбинации и/или т.п. В различных вариантах осуществления средство 205 обработки запроса управления может определять множество команд управления ключами, каждая из которых может соответствовать операции связи и/или устройству связи, связанному с предприятием. В дополнительных вариантах осуществления средство 205 обработки запроса управления может определять команды управления ключами для устройств связи, связанных с отличающимся предприятием, когда это разрешено моделью объединения. Команды управления (например, ключи шифрования) могут передаваться через интерфейсы 260 объединения ключей, связанные с каждым предприятием.

Затем на этапе B720 средство 205 обработки запроса управления может создавать очередь команд управления ключами. Задание, созданное в ответ на событие управления ключами, может включать в себя множество команд управления ключами, каждая из которых может соответствовать устройству связи и/или операции связи. Соответственно когда команды управления ключами генерируют новые ключи шифрования и распространяют их к двум или большему количеству устройств связи, команды управления ключами могут быть поставлены в очередь (например, сохранены в пределах базы 275 данных операций) для выполнения, учитывая объем команд управления ключами. Также составная команда может соответствовать командам управления ключами для множества источников ключей для выдачи ключей шифрования к множеству принимающих ключи шифрования устройств связи. Составная команда может связываться с множеством команд управления ключами и может сохраняться в целом в базе 275 данных операций, ожидая распространения. Таким образом, даже если сервер (например, средство 205 обработки запроса управления) отключается прежде, чем все команды управления ключами будут выполнены/распространены, процесс может возобновляться, как только этот сервер включится.

На этапе B730 команда управления ключами, связанная с неактивными устройствами связи (например, с устройствами связи, которые могут быть выключены и/или вне сети), может сохраняться в базе 275 данных операций для будущего распространения (например, когда неактивные устройства связи будут включены) с помощью средства 205 обработки запроса управления. С другой стороны, для активных элементов (например, устройств связи, которые могут быть включены и/или в сети) команда управления ключами может выполняться на этапе B740 с помощью средства 205 обработки запроса управления.

Например, на этапе B750 средство 205 обработки запроса управления может запрашивать ключи шифрования из источников 170 ключей, основываясь на командах управления ключами. Например, команды управления ключами могут определять один или большее количество источников 170 ключей для выдачи ключей шифрования на устройства связи. Соответственно некоторые устройства связи могут принимать ключи шифрования из первого источника ключа, в то время как другие устройства связи могут принимать ключи шифрования из второго отличающегося источника ключа. Затем на этапе B760 средство 205 обработки запроса управления может распространять ключи шифрования к устройствам связи. В некоторых вариантах осуществления средство 205 обработки запроса управления может выполнять анализ ключа шифрования описанным образом, основываясь на атрибутах 160 ключей и на наборе политик 115. После одобрения средство 205 обработки запроса управления может направлять ключи шифрования к соответствующим устройствам связи через средство 210 обработки запроса.

Затем на этапе B770 средство 205 обработки запроса управления может принимать из устройств связи ответ на распространение. Например, средство 205 обработки запроса управления может определять на этапе B780, основываясь на ответах из устройств связи, было или нет такое распространение успешным. Когда средство 205 обработки запроса управления определяет, что распространение было успешным по отношению к заданному устройству связи (например, что устройство связи приняло распространяемый ему ключ шифрования), на этапе B795 положительная обратная связь может обеспечиваться на средство 205 обработки запроса управления.

С другой стороны, когда средство 205 обработки запроса управления определяет, что распространение было неудачным (например, что устройство связи не приняло распространяемый ему ключ шифрования) для заданного устройства связи, на этапе B790 отрицательный ответ этого устройства связи может обеспечиваться к средству 205 обработки запроса управления. Средство 205 обработки запроса управления может затем определять на этапе B798, следует или нет пытаться выполнить команду управления ключами снова в более позднее время для этого устройства связи, основываясь на существующих ранее алгоритмах или вводимой пользователем информации.

Когда средство 205 обработки запроса управления определяет, что выполнение команд управления

ключами (например, распространение шифрования) не должно снова предприниматься (B798: "нет"), процесс заканчивается. С другой стороны, когда средство 205 обработки запроса управления определяет, что команды управления ключами, которые успешно не распространены, должны будут снова выполняться (B798: "да"), команды управления ключами могут сохраняться на этапе B730 (например, в базе 275 данных операций) для будущего распространения.

В некоторых вариантах осуществления, когда распространение команд управления ключами является неудачным, средство 205 обработки запроса управления может определять, что следует повторить распространение неудачных команд управления ключами (B780: "повтор"). Например, на этапе B740 средство 205 обработки запроса управления может снова выполнять команды управления ключами для активных элементов.

Фиг. 8 - последовательность операций процесса, показывающая пример процесса 800 объединения ключей шифрования согласно различным вариантам осуществления. Что касается фиг. 1-8, устройства 110 подготовки ключей (например, и в том же самом локальном предприятии, и во внешнем предприятии) могут взаимно подтверждать подлинность и распространять ключи шифрования, основываясь на политиках 115, воплощаемых для устройств 110 подготовки ключей или для каждого предприятия, для объединения ключей шифрования одного предприятия с другим предприятием. Кроме того, процесс 800 объединения ключей шифрования может также включать в себя прием ключей шифрования из внешнего устройства подготовки ключей в результате политики объединения внешнего устройства подготовки ключей.

Сначала на этапе B810 локальное устройство подготовки ключей (например, устройство A 310a подготовки ключей) может обеспечивать информацию аутентификации к внешнему устройству подготовки ключей (например, к устройству B 310b подготовки ключей). Информация аутентификации может быть любой подходящей подсказкой и/или запросом аутентификации для объединения. Затем на этапе B820 локальное устройство подготовки ключей может принимать ответ аутентификации из внешнего устройства подготовки ключей, соглашаясь на инициирование модели объединения. Этапы B810 и B820 могут представлять обычное установление связи для обмена сертификатами безопасности, причем объединенное доверие установлено между этими двумя предприятиями.

Затем на этапе B830 локальное устройство подготовки ключей может обеспечивать информацию о политике доверия к внешнему устройству подготовки ключей. На этапе B840 локальное устройство подготовки ключей может принимать информацию о политике доверия из внешнего устройства подготовки ключей. Информация о политике доверия может включать в себя любые конфигурации, установки, степень доверия, взаимно согласованные политики, их комбинацию и/или т.п.

Затем на этапе B850 локальное устройство подготовки ключей и внешнее устройство подготовки ключей могут управлять и распространять информацию ключа (например, ключ шифрования, связанные с ним атрибуты 160 ключа, их комбинацию и/или т.п.) описанным образом.

В конкретных вариантах осуществления внешнее устройство подготовки ключей передает запрос 175 на локальное устройство подготовки ключей для генерации ключей шифрования для операции связи между устройством связи, связанным с внешним устройством подготовки ключей, и устройством связи, связанным с локальным устройством подготовки ключей. Ключ шифрования может генерироваться с помощью локального устройства подготовки ключей и анализироваться с помощью локального средства обработки политик. Ключ шифрования может передаваться на внешнее устройство подготовки ключей для анализа с помощью внешнего средства обработки политик в некоторых вариантах осуществления, но не в других.

В некоторых вариантах осуществления вместо запроса 175 внешнее устройство подготовки ключей может передавать генерируемый ключ шифрования (который может быть проанализирован или может не быть проанализирован с помощью средства обработки политик внешнего устройства подготовки ключей в зависимости от заданной информации политики доверия). Локальное устройство подготовки ключей может анализировать или может не анализировать ключ шифрования и связанные с ним атрибуты 160 ключа с помощью политик 115, основываясь на информации политики доверия, определенной между предприятиями.

Фиг. 9 - последовательность операций процесса, показывающая пример процесса 900 управления и распространения ключей шифрования согласно различным вариантам осуществления. В различных вариантах осуществления процесс 900 управления и распространения ключей шифрования может внедрять элементы подготовки ключей, которые включают в себя управление ключами, распространение ключей и объединение ключей.

Сначала на этапе B910 может описываться набор политик 115, причем каждая политика 115 может относиться к одному или большему количеству атрибутов 160 ключа. Политики 115 могут описываться с помощью предназначенного для этого персонала и сохраняться в базе 280 данных политик для будущего поиска и обновления. Затем на этапе B920 средство 205 обработки запроса управления может принимать ключ шифрования и по меньшей мере один атрибут ключа, связанный с ключом шифрования, из источника 170 ключей описанным образом.

Затем на этапе B930 средство 205 обработки запроса управления может определять пригодность

принятого ключа шифрования, основываясь, по меньшей мере частично, по меньшей мере на одном атрибуте ключа и на наборе политик 115, которые относятся к одному по меньшей мере из одного атрибута ключа. Например, средство 205 обработки запроса управления может проверять значение, соответствующее атрибуту 160 ключа, для определения, находится или нет значение в пределах пригодного диапазона, как описывается с помощью политик 115 описанным образом.

Затем на этапе B940 средство 205 обработки запроса управления может определять, является или нет ключ шифрования пригодным. Если ключ шифрования является пригодным (B940: "да"), то на этапе B950 средство 205 обработки запроса управления может распространять ключ шифрования к устройствам связи, запрашивающим ключ для операции связи между ними. С другой стороны, когда ключ шифрования недопустим (B940: "нет"), средство 205 обработки запроса управления может передавать сообщение "запрещено" к источнику 170 ключей на этапе B960. Опционально на этапе B970 средство 205 обработки запроса управления может передавать подсказку к источнику ключа для облегчения генерации ключей. Средство 205 обработки запроса управления может затем находиться в состоянии ожидания до приема второго ключа шифрования (и связанных с ним атрибутов 160 ключа) на этапе B920.

Система подготовки ключей (например, устройство 110 подготовки ключей, средство 205 обработки запроса управления, устройство A 310a подготовки ключей, устройство B 310b подготовки ключей и/или т.п.), описанная в данной работе, может воплощаться в любых подходящих вычислительных устройствах, имеющих процессор и запоминающее устройство. Процессор может включать в себя любое подходящее устройство обработки данных, такое как универсальный процессор (например, микропроцессор), но альтернативно процессор может быть любым обычным процессором, контроллером, микроконтроллером или конечным автоматом. Процессор может также воплощаться как комбинация вычислительных устройств, например как комбинация DSP и микропроцессора, множества микропроцессоров, по меньшей мере одного микропроцессора вместе с ядром DSP или любой другой такой конфигурации. Память может функционально соединяться с процессором и может включать в себя любое подходящее устройство для сохранения программного обеспечения и данных для контроля и использования процессором для выполнения операций и функций, описанных в данной работе, включающее в себя оперативную память ОП, постоянное запоминающее устройство ПЗУ, гибкие диски, жесткие диски, аппаратные ключи или другие подключенные к RSB устройства памяти или т.п., но не ограниченное ими.

Устройство 110 подготовки ключей, средство 205 обработки запроса управления, устройство A 310a подготовки ключей и/или устройство B 310b подготовки ключей могут воплощаться на подходящих операционных системах (OS), таких как OS Linux, Windows, Mac OS и т.п., но которые не ограничены ими. Дополнительно устройство 110 подготовки ключей, средство 205 обработки запроса управления, устройство A 310a подготовки ключей и/или устройство B 310b подготовки ключей могут воплощаться в небольшом конструктиве, например как встроенные системы.

Варианты осуществления, которые описаны относительно фиг. 1-9, относятся к ключам шифрования. Специалисты должны признать, что в других вариантах осуществления системы и способы, направленные на устройство 110 подготовки ключей, вовлекающие управление, распространение и объединение, могут воплощаться подобным образом для других важных объектов, таких как информация идентификатора пользователя, сертификаты, биометрические данные, данные генератора случайных чисел, определенные данные генератора случайных чисел, неопределенные данные генератора случайных чисел, информация проверки пользователя, компоненты политики, другие компоненты, связанные с компонентой обеспечения безопасности организации и/или т.п., но которые не ограничены ими.

Различные варианты осуществления, описанные выше со ссылкой на фиг. 1-9, включают в себя выполнение различных процессов или задач. В различных вариантах осуществления такие процессы или задачи могут выполняться через выполнение считывания машинного кода со считываемых компьютером носителей данных. Например, в различных вариантах осуществления один или большее количество считываемых компьютером носителей данных хранят одну или большее количество компьютерных программ, которые, когда выполняются с помощью процессора, побуждают процессор выполнять процессы или задачи, которые описаны по отношению к процессору в вышеупомянутых вариантах осуществления. Кроме того, в различных вариантах осуществления один или большее количество считываемых компьютером носителей данных хранят одну или большее количество компьютерных программ, которые, когда выполняются с помощью устройства, побуждают компьютер выполнять процессы или задачи, которые описаны по отношению к устройствам, упомянутых в приведенных выше вариантах осуществления. В различных вариантах осуществления один или большее количество считываемых компьютером носителей данных хранят одну или большее количество компьютерных программ, которые, когда выполняются с помощью базы данных, побуждают базу данных выполнять процессы или задачи, которые описаны по отношению к базе данных в вышеупомянутых вариантах осуществления.

Таким образом, варианты осуществления включают в себя программные продукты, содержащие считываемые компьютером или машинно-считываемые носители для переноса или содержания выполняемых компьютером или машинно-выполняемых команд или структур данных, сохраненных на них. Такие считываемые компьютером носители данных могут быть любым доступным носителем, к которому можно получать доступ, например с помощью универсального или специального компьютера или

другой машины с процессором. Посредством примера такие считываемые компьютером носители данных могут содержать полупроводниковую память, флэш-память, жесткие диски, оптические диски, такие как компакт-диски (CD) или цифровые универсальные диски (DVD), магнитное запоминающее устройство, оперативную память (ОП), постоянное запоминающее устройство (ПЗУ) и/или т.п. Комбинации этих типов памяти также находятся в пределах объема считываемых компьютером носителей данных. Выполняемый компьютером код программы может содержать, например, команды и данные, которые побуждают компьютер или обрабатывающую машину выполнять определенные функции, вычисления, действия или т.п.

Варианты осуществления, раскрытые в данной работе, должны рассматриваться во всех отношениях в качестве иллюстративных, а не ограничительных. Настоящее раскрытие никоим образом не ограничено вариантами осуществления, описанными выше. Различные модификации и изменения могут быть сделаны к вариантам осуществления, не отступая от объема и формы раскрытия. Предполагается, что различные модификации и изменения, которые находятся в пределах значения и диапазона эквивалентности формулы изобретения, должны находиться в пределах объема данного раскрытия.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ управления информационным объектом безопасности, содержащий этапы, на которых

задают и сохраняют множество политик, связанных, по меньшей мере отчасти, с информационным объектом безопасности, в базе данных, соединенной со средством обработки политик;

принимают с помощью средства обработки политик информационный объект безопасности для его распространения по меньшей мере в одно устройство связи и по меньшей мере один атрибут объекта, связанный с информационным объектом безопасности;

определяют с помощью средства обработки политик основывающуюся на соображениях криптографии пригодность информационного объекта безопасности, чтобы определить, является ли информационный объект безопасности достаточно безопасным, основываясь, по меньшей мере отчасти, на этом по меньшей мере одном атрибуте объекта и по меньшей мере одной из упомянутого множества политик, соответствующей этому по меньшей мере одному атрибуту объекта; и

распространяют тот информационный объект безопасности, который был принят, в упомянутое по меньшей мере одно устройство связи, связанное со средством обработки политик, в качестве реакции на определение того, что информационный объект безопасности является пригодным, причем это по меньшей мере одно устройство связи устанавливает связь, основываясь, по меньшей мере отчасти, на информационном объекте безопасности.

2. Способ по п.1, в котором информационный объект безопасности является ключом шифрования.

3. Способ по п.1, в котором упомянутый по меньшей мере один атрибут объекта содержит характеристики по меньшей мере одного из информационного объекта безопасности, первого устройства, генерирующего информационный объект безопасности, второго устройства, передающего информационный объект безопасности, третьего устройства, принимающего информационный объект безопасности, первого пользователя, связанного с первым устройством, второго пользователя, связанного со вторым устройством, и третьего пользователя, связанного с третьим устройством.

4. Способ по п.1, в котором упомянутый по меньшей мере один атрибут объекта содержит по меньшей мере одно из размера информационного объекта безопасности, времени, когда информационный объект безопасности генерируется, георасположения, где информационный объект безопасности генерируется, классификации информационного объекта безопасности, роли, связанной с источником ключа, роли, связанной с устройством-источником, и роли, связанной с устройством-адресатом.

5. Способ по п.4, в котором упомянутое множество политик содержит подтверждение пригодности информационного объекта безопасности, когда размер информационного объекта безопасности находится в пределах заранее определенного диапазона размеров.

6. Способ по п.4, в котором упомянутое множество политик содержит подтверждение пригодности информационного объекта безопасности, когда информационный объект безопасности генерируется в пределах заранее определенного интервала времени.

7. Способ по п.4, в котором упомянутое множество политик содержит подтверждение пригодности информационного объекта безопасности, когда георасположение, где информационный объект безопасности генерируется, находится в пределах заранее определенной области.

8. Способ по п.4, в котором упомянутое множество политик содержит подтверждение пригодности информационного объекта безопасности, когда классификация информационного объекта безопасности связана с заранее определенной группой классификаций информационного объекта безопасности.

9. Способ по п.4, в котором упомянутое множество политик содержит подтверждение пригодности информационного объекта безопасности, когда роль, связанная с источником ключа, устройством-источником или устройством-адресатом, связана с заранее определенной группой ролей.

10. Способ по п.1, дополнительно содержащий этапы, на которых

передают в источник ключа указатель отклонения;

передают в источник ключа подсказку, сообщающую о несоответствии информационного объекта безопасности,

причем информационный объект безопасности принимается из источника ключа.

11. Способ по п.1, в котором прием средством обработки политик информационного объекта безопасности содержит этапы, на которых

принимают с помощью средства обработки политик запрос сгенерировать информационный объект безопасности;

генерируют с помощью средства обработки политик информационный объект безопасности.

12. Способ управления информационным объектом безопасности, содержащий этапы, на которых

задают и сохраняют первое множество политик, связанных, по меньшей мере отчасти, с информационным объектом безопасности, в первой базе данных первого устройства подготовки ключей, причем первая база данных связана с первым предприятием;

принимают с помощью первого устройства подготовки ключей, связанного с первым предприятием, информационный объект безопасности для его распространения по меньшей мере в одно устройство связи и по меньшей мере один атрибут объекта, связанный с информационным объектом безопасности, из второго устройства подготовки ключей, связанного со вторым предприятием;

определяют с помощью первого устройства подготовки ключей основывающуюся на соображениях криптографии пригодность информационного объекта безопасности, чтобы определить, является ли информационный объект безопасности достаточно безопасным, основываясь, по меньшей мере отчасти, на этом по меньшей мере одном атрибуте объекта и по меньшей мере одной из первого множества политик, соответствующей этому по меньшей мере одному атрибуту объекта; и

распространяют тот информационный объект безопасности, который был принят, в первое устройство связи, связанное с первым предприятием.

13. Способ по п.12, дополнительно содержащий этап, на котором задают и сохраняют второе множество политик во второй базе данных второго устройства подготовки ключей, причем, по меньшей мере, первая часть первого множества политик и вторая часть второго множества политик являются одинаковыми.

14. Способ по п.12, дополнительно содержащий этапы, на которых

передают из первого устройства подготовки ключей во второе устройство подготовки ключей информационный объект безопасности; и

распространяют информационный объект безопасности во второе устройство связи, связанное со вторым предприятием, причем первое устройство связи и второе устройство связи могут устанавливать связь, основываясь на информационном объекте безопасности.

15. Способ по п.13, дополнительно содержащий этапы, на которых

передают из первого устройства подготовки ключей во второе устройство подготовки ключей информационный объект безопасности;

определяют с помощью второго устройства подготовки ключей пригодность информационного объекта безопасности, основываясь, по меньшей мере отчасти, на упомянутом по меньшей мере одном атрибуте объекта и по меньшей мере одной из второго множества политик, соответствующей этому по меньшей мере одному атрибуту объекта; и

распространяют информационный объект безопасности во второе устройство связи, связанное со вторым предприятием, причем первое устройство связи и второе устройство связи могут устанавливать связь, основываясь на информационном объекте безопасности.

16. Способ по п.12, в котором прием информационного объекта безопасности и по меньшей мере одного атрибута объекта, связанного с информационным объектом безопасности, из второго устройства подготовки ключей содержит этапы, на которых

принимают с помощью первого устройства подготовки ключей из второго устройства подготовки ключей запрос сгенерировать информационный объект безопасности;

генерируют с помощью источника ключа, связанного с первым предприятием, информационный объект безопасности в ответ на данный запрос.

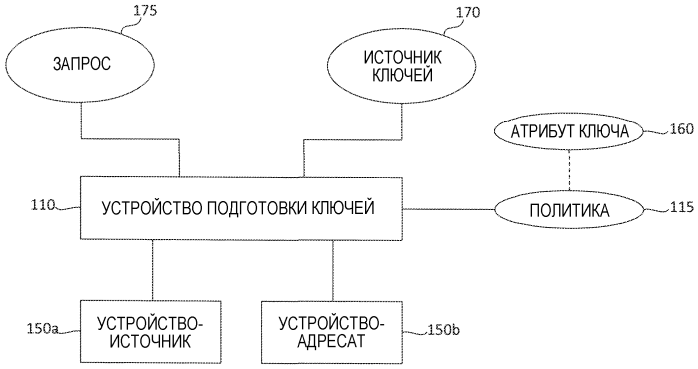
17. Машиночитаемый носитель, содержащий машиноисполняемые команды, которыми при их исполнении выполняется способ управления информационным объектом безопасности по п.1.

18. Машиночитаемый носитель по п.17, при этом информационный объект безопасности является ключом шифрования.

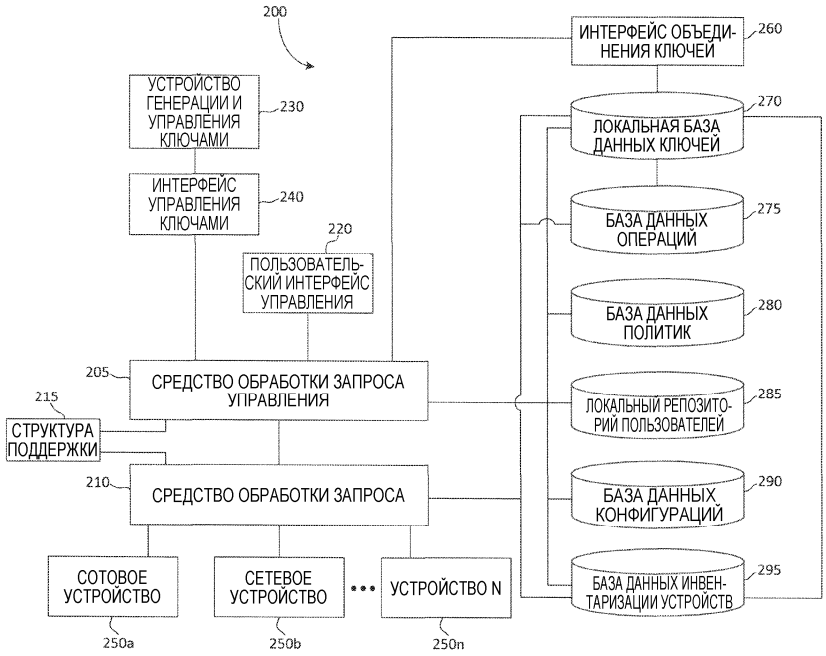
19. Машиночитаемый носитель по п.17, при этом упомянутый по меньшей мере один атрибут объекта содержит по меньшей мере одно из размера информационного объекта безопасности, времени, когда информационный объект безопасности генерируется, георасположения, где информационный объект безопасности генерируется, классификации информационного объекта безопасности, роли, связанной с источником ключа, роли, связанной с устройством-источником, и роли, связанной с устройством-адресатом.

20. Машиночитаемый носитель по п.17, при этом упомянутое множество политик содержит подтверждение пригодности информационного объекта безопасности, когда выполняется по меньшей мере

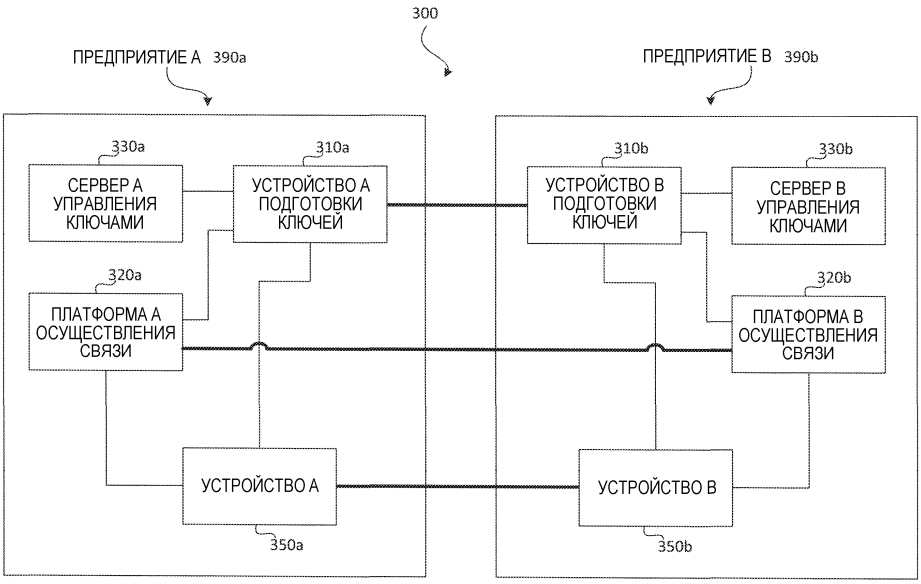
одно из следующих условий: размер информационного объекта безопасности находится в пределах заранее определенного диапазона размеров, время, когда информационный объект безопасности генерируется, находится в пределах заранее определенного интервала времени, георасположение, где информационный объект безопасности генерируется, находится в пределах заранее определенной области, классификацию информационного объекта безопасности включает в себя заранее определенная группа классификаций информационного объекта безопасности и роль, связанная с источником ключа, устройством-источником или устройством-адресатом, связана с заранее определенной группой ролей.



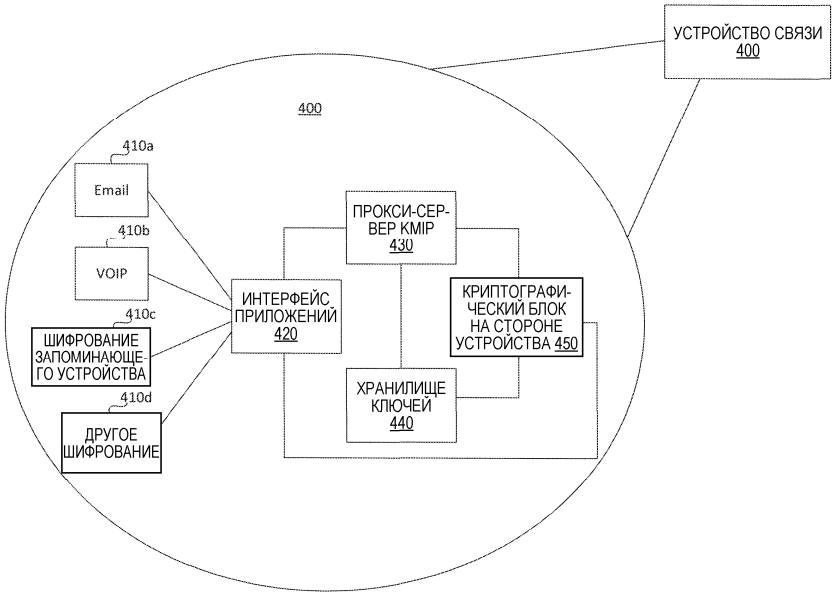
Фиг. 1



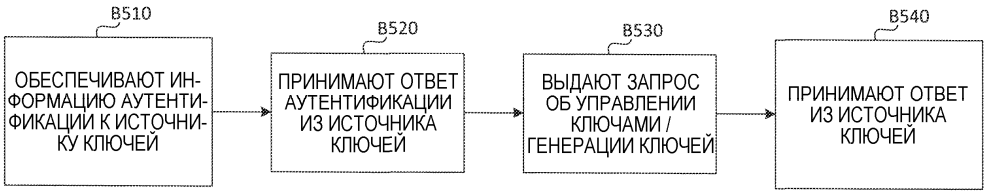
Фиг. 2



Фиг. 3



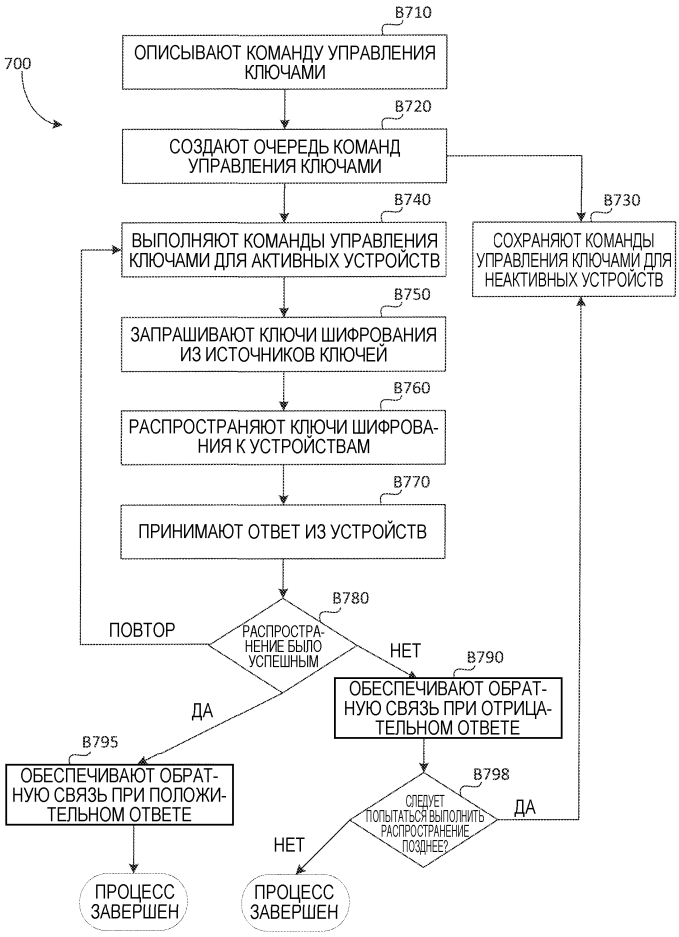
Фиг. 4



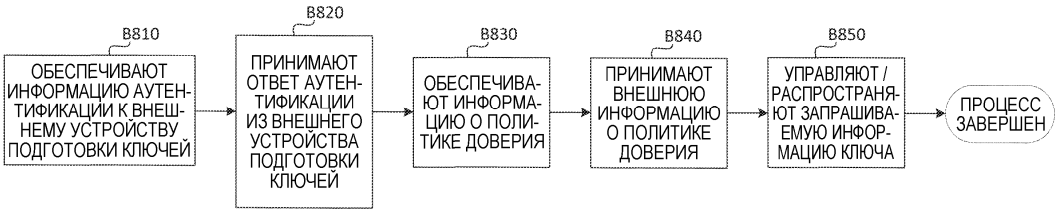
Фиг. 5


B610
УСТРОЙСТВО ОБНАРУЖЕНО
B620
УСТРОЙСТВО СВЯЗИ ЗАРЕГИСТРИРОВАНО
B630
УСТРОЙСТВО ПОДКЛЮЧЕНО
B640
ПОДТВЕРЖДАЮТ ПРИГОДНОСТЬ УСТРОЙСТВА
B650
ОБЕСПЕЧИВАЮТ ИНФОРМАЦИЮ АУТЕНТИФИКАЦИИ УСТРОЙСТВА
B660
ОПИСЫВАЮТ ПРАВИЛА ПОДГОТОВКИ ДЛЯ УСТРОЙСТВА
B670
ДОБАВЛЯЮТ УСТРОЙСТВО К РЕГИСТРАЦИИ ПОДГОТОВКИ
ПРОЦЕСС ЗАВЕРШЕН

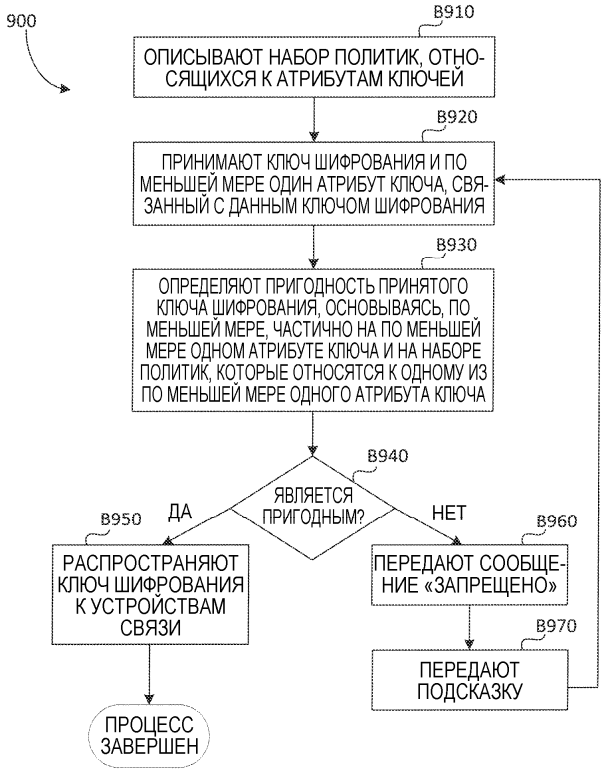
Фиг. 6


700
B710
ОПИСЫВАЮТ КОМАНДУ УПРАВЛЕНИЯ КЛЮЧАМИ
B720
СОЗДАЮТ ОЧЕРЕДЬ КОМАНД УПРАВЛЕНИЯ КЛЮЧАМИ
B730
СОХРАНЯЮТ КОМАНДЫ УПРАВЛЕНИЯ КЛЮЧАМИ ДЛЯ НЕАКТИВНЫХ УСТРОЙСТВ
B740
ВЫПОЛНЯЮТ КОМАНДЫ УПРАВЛЕНИЯ КЛЮЧАМИ ДЛЯ АКТИВНЫХ УСТРОЙСТВ
B750
ЗАПРАШИВАЮТ КЛЮЧИ ШИФРОВАНИЯ ИЗ ИСТОЧНИКОВ КЛЮЧЕЙ
B760
РАСПРОСТРАНЯЮТ КЛЮЧИ ШИФРОВАНИЯ К УСТРОЙСТВАМ
B770
ПРИНИМАЮТ ОТВЕТ ИЗ УСТРОЙСТВ
B780
РАСПРОСТРАНЕНИЕ БЫЛО УСПЕШНЫМ
ПОВТОР
НЕТ
ДА
B790
ОБЕСПЕЧИВАЮТ ОБРАТНУЮ СВЯЗЬ ПРИ ОТРИЦАТЕЛЬНОМ ОТВЕТЕ
B795
ОБЕСПЕЧИВАЮТ ОБРАТНУЮ СВЯЗЬ ПРИ ПОЛОЖИТЕЛЬНОМ ОТВЕТЕ
B798
СЛЕДУЕТ ПОПЫТАТЬСЯ ВЫПОЛНИТЬ РАСПРОСТРАНЕНИЕ ПОЗДНЕЕ?
ДА
НЕТ
ПРОЦЕСС ЗАВЕРШЕН
ПРОЦЕСС ЗАВЕРШЕН

Фиг. 7


B810
ОБЕСПЕЧИВАЮТ ИНФОРМАЦИЮ АУТЕНТИФИКАЦИИ К ВНЕШНЕМУ УСТРОЙСТВУ ПОДГОТОВКИ КЛЮЧЕЙ
B820
ПРИНИМАЮТ ОТВЕТ АУТЕНТИФИКАЦИИ ИЗ ВНЕШНЕГО УСТРОЙСТВА ПОДГОТОВКИ КЛЮЧЕЙ
B830
ОБЕСПЕЧИВАЮТ ИНФОРМАЦИЮ О ПОЛИТИКЕ ДОВЕРИЯ
B840
ПРИНИМАЮТ ВНЕШНЮЮ ИНФОРМАЦИЮ О ПОЛИТИКЕ ДОВЕРИЯ
B850
УПРАВЛЯЮТ / РАСПРОСТРАНЯЮТ ЗАПРАШИВАЕМУЮ ИНФОРМАЦИЮ КЛЮЧА
ПРОЦЕСС ЗАВЕРШЕН

Фиг. 8


900
B910
ОПИСЫВАЮТ НАБОР ПОЛИТИК, ОТНОСЯЩИХСЯ К АТРИБУТАМ КЛЮЧЕЙ
B920
ПРИНИМАЮТ КЛЮЧ ШИФРОВАНИЯ И ПО МЕНЬШЕЙ МЕРЕ ОДИН АТРИБУТ КЛЮЧА, СВЯЗАННЫЙ С ДАННЫМ КЛЮЧОМ ШИФРОВАНИЯ
B930
ОПРЕДЕЛЯЮТ ПРИГОДНОСТЬ ПРИНЯТОГО КЛЮЧА ШИФРОВАНИЯ, ОСНОВЫВАЯСЬ, ПО МЕНЬШЕЙ МЕРЕ, ЧАСТИЧНО НА ПО МЕНЬШЕЙ МЕРЕ ОДНОМ АТРИБУТЕ КЛЮЧА И НА НАБОРЕ ПОЛИТИК, КОТОРЫЕ ОТНОСЯТСЯ К ОДНОМУ ИЗ ПО МЕНЬШЕЙ МЕРЕ ОДНОГО АТРИБУТА КЛЮЧА
B940
ЯВЛЯЕТСЯ ПРИГОДНЫМ?
ДА
НЕТ
B950
РАСПРОСТРАНЯЮТ КЛЮЧ ШИФРОВАНИЯ К УСТРОЙСТВАМ СВЯЗИ
B960
ПЕРЕДАЮТ СООБЩЕНИЕ «ЗАПРЕЩЕНО»
B970
ПЕРЕДАЮТ ПОДСКАЗКУ
ПРОЦЕСС ЗАВЕРШЕН

Фиг. 9