

Изобретение относится к способу защищенного суперраспределения пользовательских данных, хранящихся на первом носителе информации. Изобретение дополнительно относится к системе для защищенного суперраспределения пользовательских данных, устройству воспроизведения и/или записи пользовательских данных и носителю информации для хранения пользовательских данных.

Суперраспределение представляет собой подход к распределению программного обеспечения, при котором программное обеспечение является свободно доступным и без ограничений, но защищено от изменений и режимов использования, не санкционированных его производителем. Архитектура суперраспределения, которая, например, известна из работы R. Mori и M. Kawahara "Суперраспределение - концепция и архитектура", The Transaction Of The IEICE, т. E73, № 7, стр. 1133-1146, июль 1990 г. (найденной на сайте <http://www.virtualschool.edu/mon/electronicproperty/morisuperdist.html>), обеспечивает три принципиальные функции:

административные устройства для сбора учетной информации относительно использования программного обеспечения и платы за использование программного обеспечения; процесс учета использования ресурсов, при котором регистрируется и накапливается плата за использование, платежи и распределение платы за использование среди различных продавцов программных средств; и механизм защиты, использующий модули с цифровой защитой, которые защищают систему от помех с помощью ее собственной операции.

- Программное обеспечение суперраспределения распределяется по общедоступным каналам в зашифрованной форме. Оно имеет следующую комбинацию требуемых характеристик:

- Продукты программного обеспечения свободно распределяются без ограничения. Пользователь программного продукта платит за использование такого продукта, а не за его обладание.

Продавец программного продукта может устанавливать продолжительность и условия его использования в перечне оплаты его использования, если таковой вообще имеется.

Программный продукт может исполняться любым пользователем, имеющим надлежащее оборудование, только при условии, что пользователь придерживается условий использования, установленных продавцом, и производит установленную продавцом оплату.

Надлежащая работа системы суперраспределения, включая требование о соблюдении условий, установленных продавцами, обеспечивается электронными устройствами с защитой от несанкционированного доступа, например, интеллектуальными (смарт-)карточками.

Суперраспределение можно использовать не только для распределения программного обеспечения, но также и вообще для распределения пользовательских данных, таких как звуковая и видеоинформация. Суперраспределение содержимого звуковой и видеоинформации может быть привлекательной коммерческой моделью для компаний звукозаписи и кинопроката. Причина заключается в том, что в такой модели потребители берут на себя часть роли агента по продаже, копируя данные, например, свои любимые альбомы, для своих друзей. В соответствии с этим и, например, в зависимости от успеха альбома, стоимость изготовления и распределения физических носителей информации может в значительной степени снижаться. Должно быть ясно, что коммерческая модель, полагающаяся на суперраспределение, жизнеспособна, только если использование копий оплачивается должным образом, что требует принуждения с помощью надежной системы защиты информации. Такая система может быть основана на механизме управления операциями, в котором используется кодирование и, наиболее вероятно, технологии внедрения водяных знаков.

Задачей настоящего изобретения является обеспечить способ защищенного суперраспределения пользовательских данных, который также обеспечивает возможность реализации различных коммерческих моделей.

Эта задача решается посредством способа по п.1 формулы изобретения, содержащего этапы:

а) копирования упомянутых пользовательских данных с упомянутого первого носителя информации на второй носитель информации;

б) сохранения на упомянутом втором носителе информации той информации, которая требуется центром обслуживания для предоставления прав доступа к упомянутой копии упомянутых пользовательских данных; и

с) получения прав доступа к упомянутой копии упомянутых пользовательских данных посредством передачи по меньшей мере упомянутой хранящейся информации в упомянутый центр обслуживания, завершения сделки (транзакции) и приема дополнительной информации доступа, в котором упомянутый центр обслуживания использует упомянутую сохраненную информацию с целью предоставления прав доступа к упомянутой копии упомянутых пользовательских данных для упомянутого второго носителя информации.

Настоящее изобретение основано на идее:

а) управления копиями: копирование содержимого, подлежащего суперраспределению, которое еще не доступно, поскольку сделка (транзакция) с центром обслуживания еще не завершена, в местоположение, отличающееся от второго носителя информации, является бесполезной, поскольку доступ для этого другого местоположения центром обслуживания предоставляться не будет; и

б) управления доступом: после завершения сделки с центром обслуживания, доступ к копии с суперраспределением на втором носителе информации может быть получен только от системы цифрового управления правами (ЦУП).

Дополнительное объяснение для введения в концепцию, аналогичную так называемому суперраспределению с адресацией конкретному устройству (с однонаправленной передачей), состоит в том, что она обеспечивает средство для воспроизведения оригиналов, более привлекательных, чем копии, даже если там нет никакой очевидной разницы, и таким образом, поддерживает розничный сбыт. Например, в случае суперраспределения с адресацией конкретному устройству существует прямая линия связи между владельцем исходного носителя информации и владельцем второго носителя информации, для которого предназначена копия с суперраспределением. Таким образом, суперраспределение с адресацией конкретному устройству (косвенно) прямо эксплуатирует существующую социальную зависимость между людьми и может даже усиливать такие зависимости, поощряя формирование сообщества. Кроме того, суперраспределение с адресацией конкретному устройству может обеспечивать дополнительную защиту, потому что не очень полезно публиковать (зашифрованные) пользовательские данные в Интернете для общей загрузки, поскольку центр обслуживания не будет предоставлять доступ к копии пользовательских данных, которая была получена таким путем.

Решение относительно того, предоставлять или отказывать в доступе к такой копии, полностью зависит от центра обслуживания; технически нет причины, по которой центр обслуживания не мог бы предоставлять доступ, например, из-за недостаточной информации. Наконец, при наличии только оригиналов, которые могут быть пригодны для суперраспределения - которое является способом выполнения оригиналов более привлекательными, чем копии с суперраспределением, например, из-за того, что имеется система поощрений, связанная с суперраспределением, например, через получение доходов от звуковых "миль" - темп роста количества копий с суперраспределением, как ожидается, будет приблизительно равен темпу роста количества проданных оригиналов (предположим, что для каждого проданного оригинала будет сделана приблизительно одна копия с суперраспределением). Снова это является характерной особенностью, поддерживающей розничный сбыт.

Информация, которая требуется центром обслуживания для предоставления прав доступа к копии пользовательских данных, может быть любой информацией, которую центр обслуживания может использовать для идентификации пользовательских данных. Например, информация может состоять из любой информации из следующего перечня или их комбинации:

- уникальный идентификатор пользовательских данных, например, номер МСКЗ (международного стандартного кода записи) музыкальной дорожки;
- уникальный идентификатор коллекции пользовательских данных, например, заголовок альбома;
- ключ расшифровки пользовательских данных, зашифрованных в открытом ключе доступа центра обслуживания;
- уникальный идентификатор носителя информации оригинала;
- уникальный идентификатор носителя информации адресата;
- идентификатор владельца оригинала пользовательских данных;
- кодовые значения, полученные из любого из вышеупомянутых идентификаторов.

Для поддержания реализации коммерческой модели, основанной на защищенном суперраспределении, предпочтительный вариант осуществления настоящего изобретения основан на идее использования уникального идентификатора носителя на первом носителе информации, то есть уникальном ИД диска на записанном заранее диске (ПЗУ) (постоянном запоминающем устройстве). Из этого уникального идентификатора носителя определяется кодовое значение, предпочтительно устройством воспроизведения первого носителя информации, которое сохраняется устройством записи на втором носителе информации вместе с уникальным идентификатором носителя первого носителя информации. Для возможности использования второго носителя информации, то есть копии первого носителя информации, кодовое значение и уникальный идентификатор носителя должны быть переданы в центр обслуживания, например, владельцу содержимого пользовательских данных, хранящихся на первом носителе информации, где эти данные декодируются и/или верифицируются и, в случае положительного результата, требуемые права и информация передаются обратно в устройство записи или устройство воспроизведения второго носителя информации, для обеспечения возможности его использования.

В предпочтительных вариантах осуществления изобретения используются дополнительные идентификаторы, с целью увеличения функциональных возможностей предложенного способа суперраспределения, например, от кого к кому передается копия. В частности, можно использовать идентификатор суперраспределения, который может храниться на первом носителе информации и использоваться для определения кодового значения и верификации кодового значения в центре обслуживания.

В дополнительном варианте осуществления изобретения один или более ключей, которые могут быть частью иерархии ключей, используются для шифрования пользовательских данных, хранящихся в зашифрованной форме на первом носителе информации. Эти ключи необходимо обеспечить из центра обслуживания для обеспечения возможности использования второго носителя информации. Такие ключи

могут быть получены, например, из метки физического диска, например, колебания на оптическом носителе записи.

В дополнительном аспекте изобретения ключ устройства воспроизведения суперраспределения и ключ устройства записи суперраспределения используются для шифрования кодового значения перед его сохранением на втором носителе информации. Тогда расшифровка производится центром обслуживания после того, как зашифрованное кодовое значение передано в центр обслуживания, с целью обеспечения возможности использования второго носителя информации.

Помимо этого, еще в одном дополнительном аспекте изобретения используются идентификатор устройства воспроизведения и идентификатор устройства записи, которые также хранятся на втором носителе информации и передаются в центр обслуживания для расшифровки ключа устройства воспроизведения и ключа устройства записи суперраспределения с целью обеспечения возможности использования второго носителя информации.

В качестве альтернативы, изготовителем устройства воспроизведения и/или устройства записи также может выполняться расшифровка дважды зашифрованного кодового значения, посредством использования идентификаторов устройства записи и/или устройства воспроизведения. Таким образом, изготовители устройств включены в процесс разблокирования второго носителя информации, и это может гарантировать, что используются только соответствующие устройства, что также увеличивает защиту предложенного способа суперраспределения.

В предпочтительном варианте осуществления изобретения предложено возвращать прибыли из центра обслуживания владельцу первого носителя информации в ответ на защищенное суперраспределение пользовательских данных, хранящихся на первом носителе информации. Такое возвращение прибылей является частью коммерческой модели, при которой должно стимулироваться копирование и защищенное распределение пользовательских данных. Прибыли могут быть вознаграждением за первоначальный источник содержимого суперраспределения с "милями музыки", если доступ к этому содержанию кем-то куплен. Другими примерами является бесплатный доступ к "персональному коду доступа", как описано в Европейской заявке на патент 00201663.2, для разблокирования премиальной дорожки на носителе информации оригинала, или премиальные пункты для скидки при будущей покупке. Также можно осуществлять управление таким образом, чтобы такие прибыли возвращались, только если была сделана прямая копия носителя информации оригинала. Этот механизм гарантирует, что остается привлекательным покупать носители информации оригинала, которые дают механизм для защиты для копий с управляемым доступом к содержимому.

В дополнительном предпочтительном варианте осуществления кодовое значение вознаграждения, производимое по меньшей мере из уникального идентификатора носителя первого носителя информации, передается в центр обслуживания для накопления полагающихся прибылей. Центр обслуживания может таким образом определять, имеются ли прибыли и в каком количестве они должны присуждаться владельцу первого носителя информации.

В качестве носителей информации согласно изобретению предпочтительно используются оптические носители записи, в частности, записываемые и/или перезаписываемые компакт-диски (CD) или универсальные цифровые диски (DVD). Однако в объеме изобретения в качестве носителей информации дополнительно можно использовать все другие виды средств для хранения данных. Способ согласно изобретению предпочтительно используется для суперраспределения программного обеспечения, видео и/или звуковой информации, хранящейся на таких носителях информации.

В одном варианте осуществления изобретения второй носитель информации также содержит уникальный идентификатор носителя, который используется для определения кодового значения и который также передается в центр обслуживания для обеспечения возможности использования второго носителя информации. Такой уникальный идентификатор носителя второго носителя информации предпочтительно используется, если важен адресат используемых данных.

Дополнительно изобретение касается системы для защищенного суперраспределения пользовательских данных, содержащей устройство воспроизведения и устройство записи, средство передачи и центр обслуживания по п.14 формулы изобретения. Кроме того, изобретение относится к устройству воспроизведения и/или записи пользовательских данных для использования в такой системе и к носителю информации для хранения пользовательских данных и данных суперраспределения, подлежащих использованию в способе защищенного суперраспределения в соответствии с изобретением. Должно быть понятно, что такая система, устройство и носитель информации согласно изобретению могут быть дополнительно усовершенствованы и могут иметь дополнительные варианты осуществления, которые являются идентичными или подобными этим вариантам осуществления, как описано выше и как установлено в зависимых от п.1 пунктах формулы изобретения.

С точки зрения верхнего уровня, способ и система в соответствии с изобретением действуют следующим образом. Записанный заранее диск содержит информацию, которая зашифрована с ключом актива, который может храниться в устройстве блокировки ключа, типа описанного в Европейской заявке на патент № 00202888.4. Но также можно использовать и ключ, который получен из метки первого физического диска, например, колебания дорожек оптического носителя записи. Этот ключ может быть

частью иерархии ключей и как таковой не используется для непосредственной шифровки самого содержимого, а скорее для промежуточного набора ключей. Для надлежащей работы способа и системы требуется, чтобы информационное наполнение этой метки диска предпочтительно было секретным, то есть доступным только для соответствующих устройств воспроизведения. Информационное наполнение уникально для заголовка диска, но не должно быть уникальным для диска, то есть ключи и зашифрованное содержимое на всех заранее записанных дисках идентичны. Для владельца содержимого это не должно быть проблемой, поскольку все заранее записанные диски являются оригиналами известного изготовления.

В дополнение к первой метке физического диска есть вторая, предпочтительно секретная метка диска на записанном заранее диске (ПЗУ), которая является уникальной для каждого диска. Полезные данные этой второй метки могут использоваться в течение всех стадий процесса суперраспределения, с целью предотвращения неуправляемого суперраспределения. Ключ для звуковоспроизведения, то есть ключ актива, будет (защищенным образом) предоставляться центром обслуживания. На копии обеспечены условия для установления, что содержимое может быть воспроизводимым только на этом конкретном диске, для предотвращения неуправляемого распределения через Интернет. С этой целью записываемый или перезаписываемый диск содержит уникальную метку диска, которая используется для получения ключа (ключей), требуемого для расшифровки содержимого. Для записываемого или перезаписываемого диска эта уникальная метка диска может быть предварительно выдана на диске или записана устройством записи.

Аспектом изобретения является обеспечение гарантии, чтобы было возможно делать копию источника только на один приемник. Также можно обеспечивать возможность копирования с одного источника на множество приемников, то есть через Интернет. Это можно сделать, не используя уникальный дисковый идентификатор для приемника. Однако система премий в этом случае может работать несправедливо. Если один человек контролирует открытие популярного Web-сайта, с которого каждый копирует файлы, он может забрать все премиальные прибыли. Если бы в отличие от этого, диск оригинала был всегда необходим для изготовления копии, то лишь покупатели дисков оригинала получали бы вознаграждение.

После завершения транзакции владелец содержимого, то есть центр обслуживания, обеспечивает ключ (ключи), которые используются устройством записи для того, чтобы сделать копию (и только эту конкретную копию) воспроизводимой. В некоторой точке в транзакции владелец содержимого может определять уникальный идентификатор носителя диска оригинала. Для обеспечения стимула для потребителя, чтобы он делал копии с суперраспределением для друзей, владелец содержимого может решить обеспечивать некоторую прибыль для владельца диска оригинала. Например, можно давать бесплатный доступ к "персональному коду доступа", который можно использовать для разблокирования премиальной дорожки на диске оригинала; все премиальные пункты можно накапливать для скидки при будущей покупке. Если владелец содержимого так желает, копия с суперраспределением сама может быть использована так, чтобы делать другую копию с суперраспределением, либо до бесконечности, либо до заранее определенного предела. В этом случае владелец содержимого может решать возвращать прибыли, связанные с суперраспределением содержимым, любому участнику цепочки, начинающейся с диска оригинала (подобно системе пирамиды). Ясно, что защищенное суперраспределение содержимого допускает бесчисленное количество моделей маркетинга, которые можно выбирать на основании альбома, и можно обеспечивать богатый источник маркетинговой информации.

Ниже изобретение пояснено более подробно со ссылкой на следующие чертежи, на которых:

фиг. 1 изображает блок-схему системы суперраспределения в соответствии с изобретением;

фиг. 2 - блок-схему иерархии ключей, используемой в варианте осуществления изобретения,

фиг. 3А, 3В - компоновку диска оригинала и копии;

фиг. 4 - этапы копирования в соответствии с первым вариантом осуществления изобретения;

фиг. 5 - этапы разблокирования в соответствии с первым вариантом осуществления;

фиг. 6 - этапы накопления прибылей в соответствии с первым вариантом осуществления;

фиг. 7 - этапы копирования в соответствии со вторым вариантом осуществления изобретения;

фиг. 8а, 8б - этапы разблокирования в соответствии со вторым вариантом осуществления и

фиг. 9а, 9б изображают этапы накопления прибылей в соответствии со вторым вариантом осуществления.

На блок-схеме фиг. 1, изображающей вариант осуществления системы суперраспределения в соответствии с изобретением, показано устройство 1 воспроизведения для воспроизведения заранее записанного носителя информации, например, заранее записанного диска (ПЗУ), содержащего пользовательские данные, например, программное обеспечение, видео или звуковые данные. Устройство 2 записи используется для выполнения записи данных, хранящихся на первом носителе информации, воспроизводимых устройством 1 воспроизведения, на втором носителе информации, например, на перезаписываемом или записываемом диске. После того, как пользовательские данные и все необходимые данные суперраспределения переданы из устройства 1 воспроизведения в устройство 2 записи, где эти данные сохраняются на втором носителе информации, этот второй носитель информации разблокируется, то есть он обеспе-

чивается всеми необходимыми правами и информацией для предназначенного использования второго носителя информации посредством передачи требуемых данных суперраспределения в центр 3 обслуживания, где эти данные верифицируют, и если верификация была успешна, данные для обеспечения возможности использования возвращаются в устройство 2 записи. Чтобы верифицировать данные суперраспределения, обеспечиваемые из устройства 2 записи, центр 3 обслуживания может передавать часть данных суперраспределения изготовителю 4 устройства воспроизведения и/или изготовителю 5 устройства записи для расшифровки и/или верификации. Линии связи между устройством воспроизведения и центром обслуживания и между центром обслуживания и изготовителем устройства воспроизведения/устройства записи не являются необходимыми, а факультативными. Линия связи между устройством воспроизведения и центром обслуживания предназначена для возможного накопления прибыли. Другие линии связи используются для "защелкивания" изготовителей, если это желательно. Система и способ для суперраспределения более подробно объясняются ниже.

Блок-схема, изображающая иерархию ключей, используемую в предпочтительном варианте осуществления изобретения, показана на фиг. 2. Сначала считывающее устройство 6 метки диска используется для считывания метки физического диска, обеспечиваемой на диске, для получения первого набора ключей. Из этих ключей в блоке 7 образуется так называемый ключ KL_Key устройства блокировки ключей. Параллельно с этим используется считывающее устройство 8 устройства блокировки ключей для получения зашифрованной версии ключей актива, причем эти ключи актива используются для шифровки пользовательских данных. Функция считывающего устройства 8 устройства блокировки ключей заключается в считывании содержимого устройства блокировки ключей с диска. Само устройство блокировки ключей представляет собой специальную область на диске, где хранятся ключи расшифровки (ключи актива) и права использования содержимого. Содержимое устройства блокировки ключей зашифровано с использованием ключа устройства блокировки ключей, который получают согласно иерархии ключей, показанной на чертеже.

В блоке 9 ключи актива расшифровываются при помощи ключа устройства блокировки ключей, причем этот ключ актива затем используется в блоке 10 для расшифровки зашифрованного содержимого, то есть пользовательских данных, хранящихся на диске. Следует отметить, что показанная на фиг. 2 иерархия ключей является только возможной системой, которая может лежать в основе системы по изобретению. Возможны другие конструктивные решения, которые могут работать одинаково хорошо.

На фиг. 3А и 3В показана компоновка носителя информации оригинала и копии, то есть данных суперраспределения, хранящихся на носителе информации оригинала и копии, оба из которых являются оптическими дисками. Показанный на фиг. 3А диск оригинала содержит следующие данные суперраспределения:

ИД-заголовок: идентификатор данных, который может быть некоторым числом, предназначенным для идентификации заголовка содержимого, не являющегося секретным;

UDI-RO: уникальный идентификатор носителя (диска), в частности, диска ПЗУ, который не является секретным; UDI-RO хранится на диске оригинала (только для чтения) в метке физического диска и идентифицирует конкретный диск (то есть он действует, как своего рода серийный номер). Он не должен копироваться. На копии эквивалентом UDI-RO является UDI-R, который может быть либо предварительно записан на копии (например, изготовителем), либо записан устройством записи, в зависимости от ряда правил устойчивости к нарушениям исходных предпосылок и случайности. Следует отметить, что UDI-R может быть расположен внутри устройства блокировки ключей.

БПК: блок разблокирования ключей (не секретный), который является блоком данных, содержащих ключ, зашифрованный с помощью различных ключей устройства воспроизведения;

МФД (метки МФД): метка (метки) физического диска. Такие метки физического диска могут только считываться соответствующими устройствами, и они предпочтительно секретные. Если используется КБР, МФД также может быть не секретной;

ИД-СР: идентификатор суперраспределения, который может быть некоторым числом, используемым для поддержания функциональных возможностей суперраспределения, являющийся секретным, и который может быть расположен в устройстве блокировки ключей;

КА: ключ актива, который используется для шифровки некоторой части содержимого или пользовательских данных (актива).

Вместо идентификатора носителя UDI-RO показанный на фиг. 3В диск копии содержит идентификатор носителя UDI-R, который является несекретным уникальным идентификатором диска записываемого или перезаписываемого диска. Далее, ключ актива КА в первом примере не хранится на диске копии. Однако, если актив/дорожка разблокируется центром обслуживания, ключ КА будет храниться на диске. Помимо этого, на диске копии хранится отличающийся идентификатор суперраспределения ИД-СР'. Идентификатор ИД-СР' может быть образован устройством записи или также может быть получен посредством некоторой связи с центром обслуживания. В первом случае он должен передаваться в центр обслуживания через защищенный канал аутентификации.

Фиг. 4 изображает этапы копирования пользовательских данных, хранящихся на первом носителе информации, воспроизводимых устройством воспроизведения, на второй носитель информации, причем

запись выполняется в устройстве записи. На первом этапе содержимое первого носителя информации переносится в устройство записи в зашифрованной версии, и оно записывается на втором носителе информации. На втором этапе устройство записи возвращает уникальный идентификатор носителя UDI-R второго носителя информации (диска адресата) так, что копию с суперраспределением можно разблокировать только на этом диске. На этапе 3 устройство воспроизведения возвращает информацию, требуемую для разблокирования копии с суперраспределением. Эта информация содержит кодовое значение, например, хеширование или функцию F, которая включает в себя уникальный идентификатор носителя UDI-RO первого носителя информации, с целью идентифицирования этого конкретного исходного диска, уникальный идентификатор носителя UDI-R второго носителя информации, с целью идентифицирования этого конкретного диска адресата, и идентификатор суперраспределения ИД-СР, с целью обеспечения гарантии, что только соответствующее устройство воспроизведения может вычислить кодовое значение или результат хеширования. Только соответствующее устройство воспроизведения может извлечь ИД-СР. Дополнительно к этому уникальный идентификатор носителя UDI-RO, который позже требуется центром обслуживания для верификации кодового значения (результата хеширования), и идентификатор данных ИД-заголовка, который требуется центром обслуживания для определения идентификатора суперраспределения ИД-СР, передаются в устройство записи и хранятся на втором носителе информации. Факультативно, во втором обмене информацией от устройства воспроизведения к устройству записи также можно обеспечивать UDI-R в незашифрованном виде.

Этапы разблокирования второго носителя информации показаны на фиг. 5. Устройство записи сначала посылает информацию, требуемую для разблокирования копии, в центр обслуживания, причем эта информация включает в себя кодовое значение F, идентификатор носителя оригинала UDI-RO и идентификатор данных ИД-заголовка. Идентификатор носителя копии UDI-R добавляется к этой информации, чтобы дать возможность центру обслуживания верифицировать кодовое значение (результат хеширования). Для передачи данных устанавливается защищенный канал аутентификации ЗКА, с целью идентифицирования исходящего устройства записи, а также для более позднего использования. Такой защищенный канал аутентификации ЗКА является устройством сопряжения, которое можно использовать для защищенной передачи данных.

На следующем этапе центр обслуживания определяет идентификатор суперраспределения ИД-СР и ключ актива КА из идентификатора данных ИД-заголовка, предпочтительно используя базу данных, и верифицирует кодовое значение (результат хеширования). На этом этапе идентификатор носителя оригинала UDI-RO также запоминается в центре обслуживания наряду с присуждаемыми прибылями, если таковые имеются.

Наконец, на последнем этапе центр обслуживания возвращает ключ актива КА, права, купленные устройством записи, и другой идентификатор суперраспределения ИД-СР'. Дополнительно, в сделке также может содержаться некоторый вид передачи денег. Таким образом, защищенный канал аутентификации ЗКА гарантирует, что эту информацию может принимать только соответствующее устройство записи.

Дальше со ссылкой на фиг. 6 поясняются этапы накопления прибылей в первом варианте осуществления. На первом этапе устройство воспроизведения, производящее первоначальные данные, посылает в центр обслуживания информацию, требуемую для накопления прибылей. Эта информация включает в себя другое кодовое значение или хеширование, которое отличается от кодового значения, показанного на фиг. 4 и 5. Хеширование, используемое для накопления прибылей, включает в себя идентификатор носителя оригинала UDI-RO, с целью идентифицирования диска, для которого собраны прибыли, и идентификатор суперраспределения оригинала ИД-СР, с целью гарантирования, что результат хеширования может вычислить только соответствующее устройство воспроизведения. Далее, эта информация, переданная в центр обслуживания, включает в себя UDI-RO, который позже требуется центром обслуживания для верификации результата хеширования, и идентификатор данных ИД-заголовка, который требуется центром обслуживания для определения идентификатора суперраспределения ИД-СР. Снова устанавливается защищенный канал аутентификации ЗКА, с целью идентифицирования исходящего устройства воспроизведения, а также для использования на этапе 3 позже.

На втором этапе центр обслуживания определяет идентификатор суперраспределения ИД-СР из идентификатора данных ИД-заголовка, предпочтительно с использованием базы данных, и верифицирует результат хеширования. Затем определяются прибыли из идентификатора носителя UDI-RO, снова предпочтительно с использованием базы данных. На третьем этапе прибыли или краткий обзор состояния прибылей возвращаются в устройство воспроизведения при помощи защищенного канала аутентификации ЗКА, и это гарантирует, что эту информацию принимает правильное соответствующее устройство воспроизведения. Прибыли могут быть связаны с исходным диском или устройством воспроизведения, в зависимости от коммерческих требований, не только для диска.

В варианте осуществления, показанном на фиг. 4-6 и описанном выше, для установления защищенного канала аутентификации (ЗКА) используется шифрование с использованием асимметричного криптографического ключа и обеспечивается возможность копирования только с диска оригинала. Далее, из-

готовители устройства не заиклены в сделке (транзакции). Однако изобретение не ограничено системой и способом, имеющими такие характеристики. Изобретение также можно использовать, применяя только шифрование с использованием симметричного криптографического ключа и там, где также обеспечена возможность копирования с уже скопированных дисков. Далее, в цикл транзакции могут быть вовлечены изготовители устройства, как это будет показано на фиг. 7-9 и описано в следующем варианте осуществления.

На фиг. 7 показаны этапы процедуры копирования согласно второму варианту осуществления изобретения. На этапе 1 содержимое первого носителя информации переносится в устройство записи в зашифрованной форме. На этапе 2 устройство записи снова возвращает идентификатор носителя UDI-R диска адресата так, чтобы копию с суперраспределением можно было разблокировать только на этом диске. На этапе 3 устройство воспроизведения возвращает информацию, требуемую для разблокирования копии с суперраспределением, причем эта информация включает в себя хеширование (функцию F) идентификатора носителя UDI-RO, с целью идентифицирования конкретного исходного диска, идентификатор носителя UDI-R, с целью идентифицирования конкретного диска адресата, и идентификатор суперраспределения ИД-СР, с целью гарантирования, что только соответствующее устройство воспроизведения может вычислить результат хеширования, и что только обладатель прав может обратиться к хеш-функции (предпочтительно с использованием базы данных). Прежде, чем информация будет передана в устройство записи, результат хеширования факультативно шифруется с использованием ключа устройства воспроизведения суперраспределения КУВСР, который является уникальным для каждого устройства воспроизведения, с целью гарантирования, что изготовители устройства воспроизведения и устройства записи имеют симметричную роль на стадии разблокирования процесса. Дополнительно к этому, идентификатор носителя UDI-RO, который позже требуется центром обслуживания для верификации результата хеширования, и идентификатор данных ИД-заголовка, который требуется центром обслуживания для определения идентификатора суперраспределения ИД-СР, также как идентификатора устройства воспроизведения ИД-устройства воспроизведения, для идентификации исходящего устройства воспроизведения, передаются в устройство записи. Факультативно, UDI-R также можно обеспечивать в незашифрованном виде при втором обмене от устройства воспроизведения к устройству записи.

Этапы разблокирования (обеспечение возможности использования) в этом варианте осуществления показаны на фиг. 8a.

На первом этапе устройство записи посылает информацию, требуемую для разблокирования копии. К этой информации добавляется идентификатор носителя UDI-R, чтобы дать возможность центру обслуживания верифицировать результат хеширования. Перед передачей результата хеширования его зашифровывают с использованием ключа устройства записи суперраспределения КУЗСР, чтобы гарантировать, что информацию посылает конкретное устройство записи. Далее, добавляется идентификатор устройства записи ИД-устройства записи, с целью идентифицирования исходящего устройства записи. На втором этапе центр обслуживания входит в контакт с изготовителями устройства воспроизведения и устройства записи для расшифровки результата хеширования и затем определяет идентификатор суперраспределения ИД-СР и ключ актива КА из идентификатора данных ИД-заголовка, предпочтительно используя базу данных, и верифицирует результаты хеширования. Идентификатор носителя UDI-RO, обеспечиваемый из устройства записи, хранится наряду с присуждаемыми прибылями в центре обслуживания.

На третьем этапе центр обслуживания возвращает ключ актива КА и права, купленные устройством записи. Эта информация сначала зашифровывается с использованием ключа, полученного из идентификатора носителя UDI-R, с целью гарантирования, что изготовитель устройства записи не может использовать эту информацию неправильно. Затем зашифрованная информация дополнительно шифруется изготовителем устройства записи с целью гарантирования, что принимать информацию может только надлежащее устройство записи. Кодирование гарантирует, что информация, возвращенная центром обслуживания, может использоваться только для (обеспечения возможности использования) конкретной копии, а именно, копии, идентифицированной идентификатором UDI-R.

Обмен информацией между центром обслуживания и изготовителем устройства записи или изготовителем устройства воспроизведения для шифрования показан на фиг. 8b.

Этапы накопления прибылей во втором варианте осуществления показаны на фиг. 9a. На этапе 1 устройство воспроизведения посылает в центр обслуживания информацию, требуемую для накопления прибыли. Эта информация содержит хеширование, которое включает в себя идентификатор носителя UDI-RO, с целью идентифицирования диска, для которого собираются прибыли, и идентификатор суперраспределения ИД-СР, с целью гарантирования, что только соответствующее устройство воспроизведения может вычислить результат хеширования, и что только обладатель прав может «обратить» хеш-функцию. Далее информация, переданная в центр обслуживания, содержит идентификатор носителя UDI-RO, который позже требуется центром обслуживания для верификации результата хеширования, и идентификатор данных ИД-заголовка, который требуется центром обслуживания для определения идентификатора суперраспределения ИД-СР. Перед передачей результат хеширования зашифровывается с

помощью ключа устройства воспроизведения суперраспределения для обеспечения гарантии, что эта информация послана соответствующим устройством воспроизведения.

На втором этапе центр обслуживания входит в контакт с изготовителем устройства воспроизведения для расшифровки результата хеширования, и впоследствии определяет идентификатор суперраспределения ИД-СР из идентификатора данных ИД-заголовка, предпочтительно с использованием базы данных, и верифицирует результат хеширования. Дополнительно, прибыли определяются на основании идентификатора носителя UDI-RO, предпочтительно с использованием базы данных.

На третьем этапе прибыли или краткий обзор состояния прибыли возвращаются в устройство воспроизведения. Перед передачей информация сначала зашифровывается с использованием ключа, полученного из идентификатора носителя UDI-RO, с целью гарантирования, что изготовитель устройства воспроизведения не сможет использовать эту информацию неправильно. Второе шифрование этой информации выполняется изготовителем устройства записи, чтобы гарантировать, что информацию может принимать только надлежащее устройство воспроизведения.

Обозначения $E\{KUЗСР\}$ и $E\{КУВСР\}$ указывают на симметричное кодирование. Конечно, можно также использовать асимметричное кодирование или уже присутствующий ЗКА. Поскольку ключ актива КА должен быть секретным, он может быть защищен посредством шифрования его с помощью UDI-R(O) в связи с изготовителем устройства записи. UDI на диске не должен быть секретным. Однако кодирование с помощью UDI-R(O) дает повышенный уровень защиты, поскольку изготовитель устройства записи не знает UDI, используемый во время суперраспределения.

Связь между центром обслуживания и изготовителем устройства записи или изготовителем устройства воспроизведения для шифровки показана на фиг. 9b.

В соответствии с изобретением предложены способ и система для защищенного суперраспределения пользовательских данных. В них могут быть реализованы различные коммерческие модели, в которых содержимое распределяется посредством управляемого домашнего копирования. Копии представляются не воспроизводимыми до тех пор, пока не будет завершена соответствующая сделка (транзакция). Помимо этого, обеспечены новые маркетинговые возможности, обусловленные прямой связью между владельцем содержимого и потребителем. Для потребителей можно предоставлять стимулы для копирования пользовательских данных. Например, копии могут быть более дешевыми, чем оригиналы, и владельцу оригиналов можно обеспечивать прибыли, типа бесплатного доступа к кодам доступа для премиальных дорожек или скидок на будущие покупки ("звуковые мили"). Кроме того, такой способ суперраспределения более удобен, чем загрузка полного альбома из Интернета.

Можно предпринимать меры для сохранения привлекательности оригиналов, например, обеспечивая право оригиналов только на суперраспределение, предотвращая "фабричное" суперраспределение.

Соответствующие изобретению способ и систему можно использовать для накопления маркетинговой информации, например, используя "мили музыки". Устройства, используемые для сделок, могут оставаться анонимными или не анонимными. Кроме того, можно решать, можно ли обеспечивать копирование для суперраспределения только в системе или также и автономно. В итоге, изобретение обеспечивает возможность управления копированием, которое выполняется по всему содержимому с управляемым доступом.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ защищенного суперраспределения пользовательских данных, хранящихся на первом носителе информации, содержащий этапы

а) копирования упомянутых пользовательских данных с упомянутого первого носителя информации на второй носитель информации,

б) сохранения на упомянутом втором носителе информации той информации, которая требуется центром обслуживания для предоставления прав доступа к упомянутой копии упомянутых пользовательских данных, и

с) получения прав доступа к упомянутой копии упомянутых пользовательских данных посредством передачи, по меньшей мере, упомянутой хранящейся информации в упомянутый центр обслуживания, завершения транзакции и приема дополнительной информации доступа,

причем упомянутый центр обслуживания использует упомянутую хранящуюся информацию с целью предоставления прав доступа к упомянутой копии упомянутых пользовательских данных для упомянутого второго носителя информации, отличающийся тем, что каждый из упомянутых первого и второго носителей содержит уникальный идентификатор носителя, и эта упомянутая хранящаяся информация состоит, по меньшей мере, из кодового значения, определяемого, по меньшей мере, из упомянутых уникальных идентификаторов носителей упомянутых первого и второго носителей информации.

2. Способ по п.1, отличающийся тем, что доступ к упомянутым пользовательским данным, хранящимся на упомянутом первом носителе информации, управляется цифровым администрированием прав или системой условного доступа.

3. Способ по п.1, отличающийся тем, что упомянутые уникальные идентификаторы носителей также передаются в упомянутый центр обслуживания.

4. Способ по п.1 или 3, отличающийся тем, что упомянутый первый носитель информации содержит идентификатор суперраспределения, который используется для определения упомянутого кодового значения.

5. Способ по п.1, отличающийся тем, что упомянутое кодовое значение зашифровывается с помощью ключа устройства воспроизведения суперраспределения перед его сохранением на упомянутом втором носителе информации, и это упомянутое зашифрованное кодовое значение дополнительно зашифровывается ключом устройства записи суперраспределения перед его передачей в упомянутый центр обслуживания.

6. Способ по п.5, отличающийся тем, что упомянутый идентификатор устройства воспроизведения, соответствующий упомянутому ключу устройства воспроизведения суперраспределения, хранится на упомянутом втором носителе информации, и этот упомянутый идентификатор устройства воспроизведения и идентификатор устройства записи, соответствующий упомянутому ключу устройства записи суперраспределения, передаются в упомянутый центр обслуживания.

7. Способ по п.6, отличающийся тем, что расшифровка упомянутого зашифрованного кодового значения выполняется соответствующими изготовителями устройства воспроизведения и/или устройства записи.

8. Способ по п.1 или 2, отличающийся тем, что упомянутый центр обслуживания вознаграждает владельца упомянутого первого носителя информации в ответ на заверченный процесс защищенного суперраспределения упомянутых пользовательских данных, хранящихся на упомянутом первом носителе информации.

9. Способ по п.8, отличающийся тем, что кодовое значение вознаграждения, образованное, по меньшей мере, из упомянутого уникального идентификатора упомянутого первого носителя информации, передается в упомянутый центр обслуживания для накопления присуждаемых прибылей.

10. Способ по п.1 или 2, отличающийся тем, что в качестве носителей информации используются оптические диски, в частности, записываемые и/или перезаписываемые компакт-диски (CD) или универсальные цифровые диски (DVD).

11. Способ по п.1 или 2, отличающийся тем, что упомянутые пользовательские данные представляют собой звуковые данные, видеoinформацию или программное обеспечение.

12. Способ по п.1, отличающийся тем, что упомянутый центр обслуживания использует упомянутую хранящуюся информацию с целью предоставления прав доступа к упомянутой копии упомянутых пользовательских данных только для упомянутого второго носителя информации.

13. Система для защищенного суперраспределения пользовательских данных, хранящихся на первом носителе информации, содержащая

а) устройство воспроизведения и устройство записи для копирования упомянутых пользовательских данных с упомянутого первого носителя информации на второй носитель информации, каждый из упомянутых первого и второго носителей содержит уникальный идентификатор носителя, и сохранения данных суперраспределения на упомянутом втором носителе информации,

б) средство передачи для передачи хранящихся данных суперраспределения в центр обслуживания,

и

в) центр обслуживания для предоставления прав доступа к упомянутой копии упомянутых пользовательских данных на упомянутом втором носителе информации,

в которой упомянутое устройство воспроизведения обеспечено для определения кодового значения, по меньшей мере, упомянутых уникальных идентификаторов носителей упомянутых первого и второго носителей информации, и упомянутое устройство записи обеспечено для сохранения, по меньшей мере, упомянутого кодового значения и упомянутого уникального идентификатора упомянутого первого носителя информации на упомянутом втором носителе информации.

14. Устройство для воспроизведения и/или записи пользовательских данных для использования в системе по п.13.

15. Носитель информации для сохранения пользовательских данных и данных суперраспределения, подлежащих использованию в способе защищенного суперраспределения по п.1, где данные суперраспределения содержат

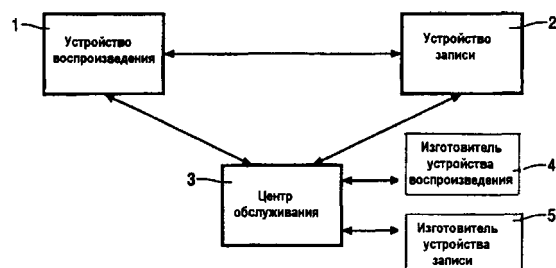
а) уникальный идентификатор носителя, идентифицирующий носитель информации,

б) идентификатор данных, идентифицирующий пользовательские данные, хранящиеся на носителе информации,

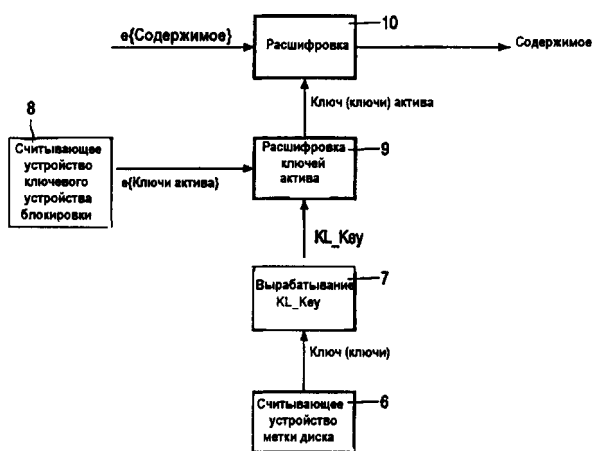
в) идентификатор суперраспределения, используемый для обеспечения функциональных возможностей суперраспределения,

г) один или более ключей для шифрования пользовательских данных и/или данных суперраспределения и

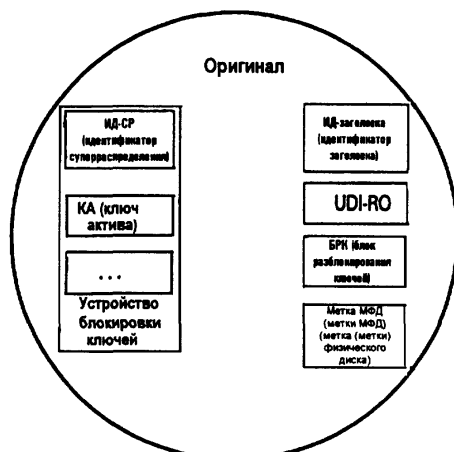
е) кодовое значение, определяемое, по меньшей мере, из упомянутого уникального идентификатора носителей упомянутого носителя информации и уникального идентификатора носителя второго носителя информации.



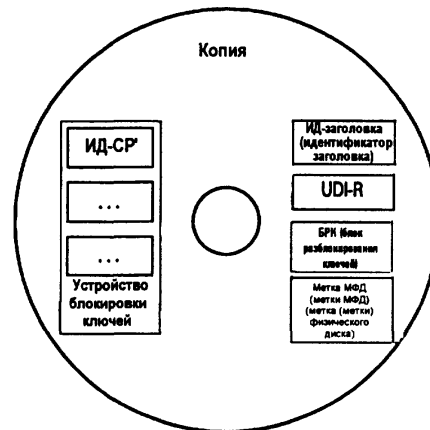
Фиг. 1



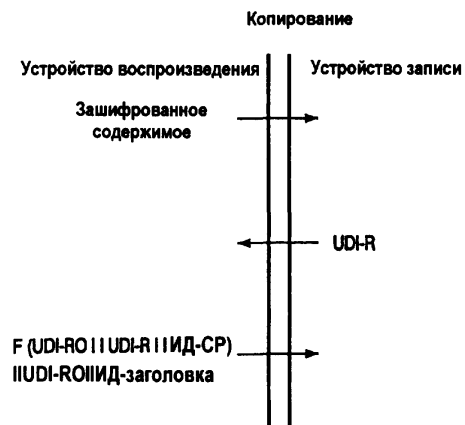
Фиг. 2



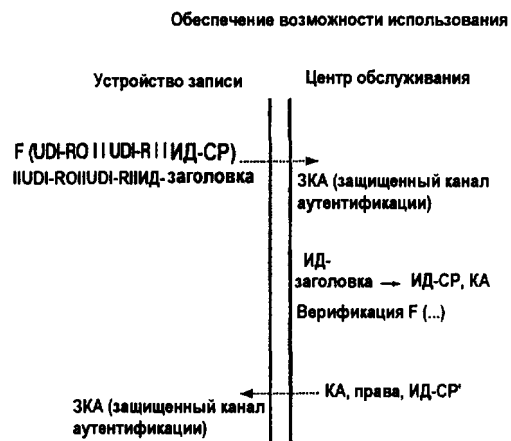
Фиг. 3А



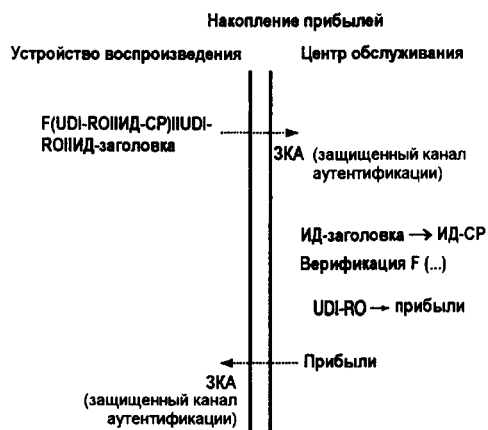
Фиг. 3В



Фиг. 4



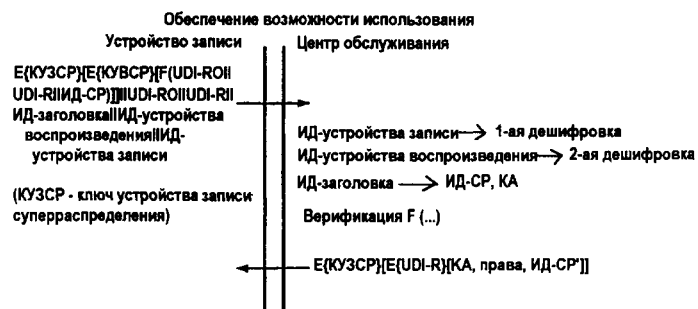
Фиг. 5



Фиг. 6



Фиг. 7



Фиг. 8А

