РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **107 608** (13) **U1**

(51) МПК
G06F 12/14 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ К ПАТЕНТУ

(21)(22) Заявка: **2010153819/08, 27.12.2010**

(24) Дата начала отсчета срока действия патента:
27.12.2010

Приоритет(ы):
(22) Дата подачи заявки: **27.12.2010**

(45) Опубликовано: **20.08.2011**

Адрес для переписки:
**111123, Москва, Свободный пр-кт, 4,
Руководителю ФГУП "18 ЦНИИ" МО РФ**

(72) Автор(ы):
**Вдовин Евгений Викторович (RU),
Лакеев Владимир Анатольевич (RU),
Хотячук Валентин Константинович (RU),
Гончаров Владимир Сергеевич (RU),
Шкирин Владимир Григорьевич (RU),
Бакунин Игорь Борисович (RU)**

(73) Патентообладатель(и):
Федеральное государственное унитарное предприятие "18 Центральный научно-исследовательский институт" Министерсва обороны Российской Федерации (RU)

(54) АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО С ЗАЩИТОЙ ИНФОРМАЦИИ ОТ УТЕЧЕК ПО КАНАЛУ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК

Формула полезной модели

Автоматизированное рабочее место (АРМ) с защитой информации от утечек по каналу ПЭМИН, состоящее из системного блока персональной электронно-вычислительной машины (СБ ПЭВМ), монитора, принтера, клавиатуры, манипулятора типа мышь (МТМ), сетевого фильтра (СФ), блока электрических розеток (БЭР), USB-ключа, микроконтроллера (МК), коммутатора, генератора широкополосного электромагнитного поля (ГШЭП), широкополосного детектора электромагнитного поля (ШДЭП), выход которого соединен с первым портом узла МК, который вторым портом соединен с первым портом коммутатора, который вторым и третьим портами соединен соответственно с USB-ключом и первым портом узла СБ ПЭВМ, который со второго по пятый портами соединен соответственно с портом узла МТМ, с портом клавиатуры, с портом принтера и с портом монитора, который входом электропитания соединен с первым выходом узла СФ, который вторым выходом, третьим выходом и входом соединен соответственно со входом электропитания принтера, со входом электропитания узла СБ ПЭВМ и первым выходом узла БЭР, который входом соединен с питающей электрической сетью (ПЭС) 220В, и выполненное с возможностью установки на СБ ПЭВМ программного обеспечения (ПО) в виде операционной системы (ОС), обеспечивающей формирование интерфейса пользователя АРМ для управления функциями АРМ, программно-аппаратных средств доверенной загрузки ОС, функционирования узла МК по программе, обеспечивающей обработку сигналов, поступающих с узла ШДЭП, и формирование сигналов управления доступом к интерфейсу пользователя узла СБ ПЭВМ, отличающееся тем, что в его состав

RU 107608 U1
RU 107608 U1

дополнительно введен датчик тока (ДТ), который входом, первым и вторым выходами соединен соответственно со вторым выходом узла БЭР, входом узла ГШЭП и третьим портом узла МК, при этом узел ДТ выполнен с возможностью измерения тока, протекающего в цепи электропитания узла ГШЭП, узел МК выполнен с возможностью функционирования по программе, обеспечивающей многоканальный прием и комплексную обработку сигналов, одновременно поступающих от датчика тока и широкополосного детектора электромагнитного поля, распознавания (идентификации) активности узла ГШЭП по уровню мощности, потребляемой этим узлом от узла ПЭС, и наличию в локальной зоне, где размещено АРМ, электромагнитного поля, создаваемого упомянутым узлом ГШЭП, управления доступом к функциям АРМ путем эмуляции подключения или отключения аппаратных средств доверенной загрузки, используемых в составе СБ ПЭВМ, соответственно при выполнении упомянутой идентификации наличия или отсутствия активности широкополосного детектора электромагнитного поля.

RU 107608 U1

Полезная модель относится к электросвязи, а точнее к устройствам защиты компьютерных систем от несанкционированной деятельности и может быть использована в информационных системах и комплексах, преимущественно, оборудованных автоматизированным рабочим местом (АРМ), для защиты информации от несанкционированного доступа, который может быть организован на основе перехвата и анализа побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых АРМ, особенно в случаях деактивации технических средств, используемых в составе АРМ, для маскировки или подавления упомянутых ПЭМИН.

Для обработки и хранения различных видов информации широко применяются средства вычислительной техники, организованные в виде автоматизированных рабочих мест (АРМ) [Л1].

Как отмечают многие эксперты, содержащаяся и циркулирующая в АРМ информация часто становится объектом пристального внимания и «охоты» со стороны посторонних физических и юридических лиц (конкурентов злоумышленников и т.п.), которые используют различные методы и технологи для осуществления несанкционированного доступа (НСД) к системным и информационным ресурсам АРМ.

Как известно [Л2, Л3], защита АРМ от несанкционированного доступа к находящейся в нем информации (НСДИ), то есть, к информации, которая находится в памяти компьютера АРМ, на съемных и несъемных носителях информации, а также отображается на экране монитора, излучается в радиоэфир, распространяется по проводным и кабельным системам, является весьма сложной задачей. Сложность этой задачи вытекает из наличия разноплановых угроз НСДИ и вероятных утечек информации по различным каналам, которые могут быть использованы злоумышленниками для реализации своих неблаговидных планов, связанных с «добычей» информации, циркулирующей в АРМ.

Как отмечают многие эксперты, наиболее опасным каналом утечки информации из АРМ является технический канал [Л4], формируемый побочными излучениями и наводками - ПЭМИН [Л5], которые образуются при функционировании технических средств, входящих в состав АРМ.

Исследования показали, что известные из техники решения в области защиты АРМ от утечек информации по техническому каналу типа ПЭМИН, имеют низкую эффективность. Это обусловлено влиянием на уровень защиты данного канала факторов объективного и субъективного характера. Основным объективным фактором является эффективность функционирования технических средств защиты информации (ТСЗИ), обеспечивающих маскировку и/или подавление ПЭМИН, возникающих при эксплуатации АРМ. К субъективным факторам можно отнести поведение и действия легитимного персонала, который в процессе эксплуатации АРМ должен выполнять установленные регламенты и инструкции по поддержке упомянутых ТСЗИ в исправном и активном состоянии при выполнении работ с использованием технических средств АРМ. Однако, на практике, при эксплуатации АРМ, регламенты использования упомянутых ТСЗИ, могут нарушаться. Персонал, выполняющий работы на АРМ, может игнорировать (преднамеренно или по халатности) установленные правила и не активировать (не обслуживать) технические средства маскировки/подавления канала типа ПЭМИН. При этом, состояние исправности и/или активности ТСЗИ активной защиты канала типа ПЭМИН не препятствует выполнению работ на АРМ. Поэтому, продолжая работу на АРМ при деактивированных ТСЗИ, персонал создает условия для утечки информации по

техническому каналу типа ПЭМИН.

По оценкам экспертов [Л5-Л7], излучение элементов компьютера и других технических средств АРМ, является достаточно информативным каналом утечки информации. Принимая и декодируя эти излучения, посторонние физические лица и/или злоумышленники могут получить сведения обо всей информации, обрабатываемой в компьютере АРМ. Современные достижения в области технологий производства радиоприемных устройств многоканального приема сигналов (как с различных направлений, так и на различных частотах), с последующей их корреляционной обработкой, позволяют обеспечить достаточную дальность перехвата информации. Процесс перехвата информации, циркулирующей в АРМ, например, путем приема паразитного излучения композитного сигнала монитора вполне реален. Более того, используются способы заставить компьютер передавать нужную информацию и не ждать, пока пользователь сам обратится к конфиденциальным документам. Это решается следующим образом: компьютер, входящий в состав АРМ, «заражается» специальной программой-закладкой типа «троянский конь» любым из известных способов по технологии вирусов: через компакт-диск с презентацией, интересной программой или игрушкой, диск с драйверами, а также через любой из каналов связи, к которому подключен АРМ (локальной сети, Интернет и др.). Далее, Spy-программа ищет необходимую информацию на диске ПЭВМ, и путем обращения к различным устройствам компьютера, инициирует в эфире побочные электромагнитные излучения и наводки. Например, Spy-программа может встраивать сообщение в композитный сигнал монитора, при этом пользователь, играя в любимую игру типа «Солитер», даже не подозревает, что в изображение игральных карт могут быть вставлены конфиденциальные текстовые сообщения или изображения. С помощью специального приемного устройства может обеспечиваться перехват паразитного излучения монитора и выделение требуемого полезного сигнала.

Проведенные экспериментальные исследования подтвердили такую возможность добывания конфиденциальной информации. В этом состоит один из вариантов технологии скрытой передачи данных по каналу побочных электромагнитных излучений с помощью программных средств. Предложенная учеными Кембриджа, подобная технология по своей сути есть разновидность компьютерной стеганографии, т.е. метода скрытной передачи полезного сообщения в безобидных видео, аудио, графических и текстовых файлах. Особенностью технологии является использование для передачи данных канала ПЭМИН, что значительно затрудняет обнаружение самого факта несанкционированной передачи по сравнению с традиционной компьютерной стеганографией. Так, если для предотвращения несанкционированной передачи данных по локальной сети или сети Интернет существуют аппаратные и программные средства (FireWall, Proxy server и т.п.), то средств для обнаружения скрытой передачи данных по ПЭМИН - отсутствуют, а обнаружить такое излучение в общем широкополосном спектре (более 1000 МГц) паразитных излучений ПЭВМ, без знания параметров полезного сигнала, весьма проблематично.

Основная опасность технологии передачи конфиденциальной информации с использованием ПЭМИН заключается в скрытности работы программы-вируса. Такая программа, в отличие от большинства вирусов, не «портит» данные, не нарушает работу ПЭВМ, не производит несанкционированную рассылку данных по сети, а значит, долгое время не обнаруживается пользователем и администратором

сети. Поэтому, если вирусы, использующие Интернет для передачи данных, проявляют себя практически мгновенно, и на них быстро находится «противоядие» в виде антивирусных программ, то вирусы, использующие ПЭМИН для передачи данных, могут работать годами, не обнаруживая себя, управляя излучением практически любого элемента компьютера.

Исследования показали, что формировать ПЭМИН могут большинство элементов компьютера, клавиатура, манипулятор типа мышь, принтер и другие технические устройства, содержащиеся в составе АРМ. При этом, сигналы, излучаемые этими устройствами, могут быть перехвачены без существенных затрат, так как информация в этих устройствах передается последовательным кодом, все параметры которого стандартизированы и хорошо известны.

Известно, что для предотвращения утечек информации из АРМ, наиболее широко используются широкополосные генераторы электромагнитного поля (ШГЭП), способные создавать в локальной (ближней) зоне, где размещены технические средства, входящие в состав АРМ, электромагнитное поле со спектром, перекрывающим ПЭМИН и вызывающих их маскировку и/или подавление. Это затрудняет ведение технической разведки, направленной на перехват и анализ ПЭМИН, создаваемых АРМ.

При использовании изделий типа ШГЭП предполагается, что прежде чем активировать АРМ, то есть включить системный блок ПЭВМ, монитор, и другие технические средства, входящие в состав автоматизированного рабочего места, пользователь в первую очередь должен проверить исправность ТСЗИ типа ШГЭП, например, осмотреть качество заземления, наличие антенно-фидерной систем, далее - включить электропитание этого устройства и, при необходимости, установить заданный режим работы.

Однако, как показали исследования, в известных технических решениях, используемых для защиты АРМ от утечек информации по каналу ПЭМИН, отсутствует эффективный контроль как технического состояния, так и активности упомянутых ТСЗИ. В результате, АРМ может использоваться по назначению без ограничения доступа к его функциям при деактивированных ТСЗИ. Как показано выше, деактивация ТСЗИ может быть вызвана как неисправностью технических средств, так случайным или преднамеренным их выключением персоналом, эксплуатирующим АРМ.

Исследования показали, что низкая эффективность известных технических решений, которые используются для защиты информации от утечек по техническому каналу типа ПЭМИН, образующемуся при эксплуатации АРМ, обусловлена действием факторов, устранение которых затрудняется наличием противоречия: чтобы эксплуатировать АРМ-персонал надо допустить на рабочее место, при этом этот же персонал может тем или иным способом деактивировать ТСЗИ и создать условия утечки информации по каналу типа ПЭМИН. С другой стороны, чтобы предотвратить утечку информации по каналу типа ПЭМИН - надо запретить доступ персонала к АРМ.

В связи с этим, поиск технических решений, направленных на повышение уровня зашиты информации, содержащейся и циркулирующей в автоматизированном рабочем месте, от несанкционированного доступа к ней методом перехвата и анализа побочных электромагнитных излучений и наводок, возникающих в процессе эксплуатации автоматизированного рабочего места, особенно в результате деактивации ТСЗИ, используемых для маскировки/подавления канала типа ПЭМИН,

является актуальной задачей.

Из техники [Л8] известно автоматизированное рабочее место (АРМ), состоящее из монитора, принтера, клавиатуры, манипулятора типа мышь (МТМ), USB ключа, системного блока персональной электронно-вычислительной машины (СБ ПЭВМ), генератора электромагнитного поля (ГЭМП), сетевого фильтра (СФ) и блока электрических розеток (БЭР), который входом, первым выходом и вторым выходом соединен, соответственно, с питающей электрической сетью 220 В (ПЭС), со входом электропитания узла ГЭМП и со входом узла СФ, который первым, вторым и третьим выходами соединен, соответственно, со входом электропитания монитора, со входом электропитания принтера и со входом электропитания узла СБ ПЭВМ, который первым, вторым, третьим, четвертым и пятым портами соединен, соответственно, с монитором, с принтером, с клавиатурой, с узлом МТМ и с USB ключом, и выполненное с возможностью установки и функционирования на узле СБ ПЭВМ программного обеспечения в виде операционной системы (ОС), обеспечивающей управление функциями программно-аппаратных средств АРМ, формирование интерфейса пользователя с предоставлением ему возможностей ввода и/или вывода информации с помощью клавиатуры, узла МТМ, принтера и монитора, программного обеспечения для обработки информации, программного обеспечения для защиты информации от вирусов, программного обеспечения для шифрования данных и программного обеспечения для выполнения доверенной загрузки ОС с использованием аппаратного средства типа USB-ключа, по которому обеспечивается возможность аутентификации пользователя, контроль загрузки ОС и контроль доступа к программным, информационным и аппаратным ресурсам АРМ в процессе функционирования СБ ПЭВМ, кроме того, узел ГЭМП выполнен с возможностью формирования в локальной зоне, в которой размещены аппаратные узлы АРМ, электромагнитного поля (ЭМП) в широком спектре радиочастот.

Работа АРМ (комплекса) осуществляется типовым образом. Так, на компьютере АРМ (узле СБ ПЭВМ) инсталлируется системное программное обеспечение, например, типа Windows2000/XP/Vista, устанавливаются также драйверы, необходимые для работы аппаратных средств, в том числе, клавиатуры, узла МТМ, принтера и монитора. Затем, в соответствии с видом обрабатываемой на комплексе информации, устанавливается (инсталлируется) прикладное программное обеспечение, например, для подготовки и обработки текстовой информации (создания документов, презентаций и т.п.) в ОС может инсталлироваться пакет офисных программ, например, Microsoft Office. Для защиты от НСД к ресурсам СБ ПЭВМ используется средств доверенной загрузки операционной системы, функционирующей на СБ ПЭВМ. При этом, аппаратной частью этих средств является USB-ключ. Как известно из [Л9], доверенная загрузка компьютера препятствуем несанкционированному запуску системного блока ПЭВМ, а также предотвращает загрузку операционной системы и получение возможности доступа к информации, содержащейся в АРМ. В область действия средств доверенной загрузки входят этапы работы компьютера от запуска микропрограммы BIOS до начала загрузки операционной системы. Доверенная загрузка включает в себя: аутентификацию, контроль устройства, с которого BIOS начинает загрузку операционной системы, контроль целостности и достоверности загрузочного сектора устройства и системных файлов запускаемой операционной системы, шифрование/дешифрование загрузочного сектора и системных файлов операционной системы.

При эксплуатации данного комплекса предусмотрена возможность использования генератора электромагнитного поля ГЭМП, который может излучать ЭМП со спектром, распределенным в широкой полосе. Это позволяет искусственно «зашумлять» радиоэфир, в том числе, ту полосу частот, где сосредоточены ПЭМИН, создаваемые работой узлов комплекса. В активном состоянии ГЭМП подавляет или маскирует ПЭМИН, которые образуются при работе комплекса, что существенно затрудняет работу злоумышленников по организации НСД к АРМ путем перехвата и последующего анализа информационных компонент, содержащихся в побочных электромагнитных излучениях технических средств АРМ.

Недостатком данного комплекса является его низкий уровень защиты информации от несанкционированного доступа, который может быть организован путем перехвата и анализа ПЭМИН, излучаемых аппаратными узлами комплекса в процессе его эксплуатации. Это обусловлено уязвимостью системы защиты комплекса к возможным нарушениям правил эксплуатации комплекса и нерегламентированным действиям персонала (НДП), выполняющего эксплуатацию АРМ. Так, по вине легитимных пользователей АРМ, функционирование узла ГЭМП может быть нарушено (по случайности или преднамеренно). Также узел ГЭМП может выйти из строя, а этот факт персоналом может быть проигнорирован или, просто не замечен (по халатности). Во всех указанных случаях возможность беспрепятственной работы персонала на АРМ - сохраняется. То есть, по субъективным причинам, могут быть созданы условия, при которых подавление/маскировка ПЭМИН, создаваемых комплексом, отсутствует (не выполняется), следовательно, возможна утечка информации по техническому каналу - за счет побочных электромагнитных излучений, которые, во время отсутствия в эфире искусственно созданного с помощью ГЭМП широкополосного электромагнитного излучения, используемого для маскировки/подавления ПЭМИН, могут быть перехвачены злоумышленниками для организации несанкционированного доступа к информационным ресурсам АРМ путем перехвата и анализа ПЭМИН.

Анализ информационной защищенности АРМ показал, что эффективность его защиты от НСДИ по техническому каналу типа ПЭМИН может быть существенно повышена путем нейтрализации влияния субъективного фактора, то есть, устранения возможности легитимному персоналу продолжать эксплуатировать АРМ в случаях деактивации технических средств защиты информации (при выключенном узле типа ГЭМП).

Установлено, что задачу повышения надежности защиты АРМ от НСД по каналу типа ПЭМИН можно свести к созданию таких условий использования АРМ, при которых небрежность в обслуживании технических средств защиты информации и/или иные действия персонала, эксплуатирующего АРМ, повлекшие деактивацию ТСЗИ, вызвали ограничение доступа к функциям АРМ.

Например, допустим, что существует функциональная зависимость между доступом к интерфейсу пользователя системного блока ПЭВМ, входящего в состав АРМ, и активностью ТСЗИ, обеспечивающих маскировку/подавление ПЭМИН, создаваемых АРМ.

Тогда, контролируя активность упомянутого узла типа ГЭМП, например, по наличию создаваемого им ЭМП, с одной стороны, и использованию контроля загрузки операционной системы на упомянутом СБ ПЭВМ, с другой стороны, можно реализовать прямую и обратную связь (ПОС), позволяющую

автоматизировать управление доступом к функциям АРМ в зависимости от активности ТСЗИ.

Прямая и обратная связь между управлением доступом к ресурсам ОС, функционирующей на СБ ПЭВМ, и активностью ТСЗИ, обеспечивающих защиту от утечек информации по техническому каналу типа ПЭМИН, в рассмотренном выше комплексе, где в качестве ТСЗИ используется узел ГЭМП, - отсутствует, что существенно снижает эффективность защиты автоматизированного рабочего места от НСДИ за счет побочных излучений и наводок, возникающих при эксплуатации АРМ.

Из-за отсутствия упомянутой ПОС эксплуатация данного АРМ может быть продолжена, даже при выключенных (вышедших из строя) технических средствах подавления/маскировки ПЭМИН, что и создает угрозу НСДИ.

По мнению авторов, наиболее близким по технической сущности к заявленному объекту (прототипом) является, известное из техники [Л10], автоматизированное рабочее место (АРМ), состоящее из системного блока персональной электронно-вычислительной машины (СБ ПЭВМ), монитора, принтера, клавиатуры, манипулятора типа мышь (МТМ), USB ключа, сетевого фильтра (СФ), микроконтроллера (МК), коммутатора, генератора широкополосного электромагнитного поля (ГЭМП), широкополосного детектора электромагнитного поля (ДП), выход которого соединен с первым портом узла МК, который вторым портом соединен с первым портом коммутатора, который вторым и третьим портами соединен, соответственно, с USB ключом и первым портом узла СБ ПЭВМ, который со второго по пятый портами соединен, соответственно, с портом узла МТМ, с портом клавиатуры, с портом принтера, с портом монитора, который входом электропитания соединен с первым выходом узла СФ, который вторым выходом, третьим выходом и входом соединен, соответственно, со входом электропитания принтера, со входом электропитания узла СБ ПЭВМ и первым выходом блока электрических розеток (БЭР), который входом и вторым выходом соединен, соответственно, с питающей электрической сетью (ПЭС) 220 В и входом электропитания узла ГЭМП, и выполненное с возможностью установки на СБ ПЭВМ программного обеспечения (ПО) в виде операционной системы (ОС), обеспечивающей управление функциями АРМ, формирование интерфейса пользователя АРМ, принтера, монитора и программного обеспечения доверенной загрузки ОС с использованием USB-ключа, и выполнения узла микроконтроллера с возможностью функционирования по программе, обеспечивающей возможность анализа и обработки сигналов, поступающих с узла ДП, и формирования управляющих сигналов, обеспечивающих блокировку доступа к интерфейсу пользователя СБ ПЭВМ и ресурсам АРМ.

Функциональная схема данного автоматизированного рабочего места (далее - комплекс), приведена на фиг.1.

Комплекс (фиг.1), состоит из системного блока персональной электронно-вычислительной машины (СБ ПЭВМ) 1, сетевого фильтра (СФ) 2, монитора 3, блока электрических розеток (БЭР) 4, принтера 6, генератора широкополосного электромагнитного поля (ГЭМП) 7, клавиатуры 8, манипулятора типа мышь (МТМ) 10, коммутатора 11, микроконтроллера (МК) 12, широкополосного детектора электромагнитного поля (ДП) 13, USB ключа 14. При этом, узел БЭР 4 своими входом, первым выходом и вторым выходом соединен, соответственно, с питающей силовой электросетью 220 В (ПЭС) 5, с узлом ГЭМП 7 и с узлом СФ 2, который

первым, вторым и третьим выходами соединен, соответственно, со входом электропитания принтера 6, со входом электропитания монитора 3 и со входом электропитания узла СБ ПЭВМ 1, который первым, вторым, третьим, четвертым и пятым портами, соединен, соответственно, с портом монитора 3, с портом принтера 6, с портом клавиатуры 8, с портом узла МТМ 10 и с первым портом коммутатора 11, который вторым и третьим портами соединен, соответственно, с USB-ключом 14 и с последовательно соединенными узлами МК 12 и ДП 13.

Комплекс (фиг.1) функционирует следующим образом.

В исходном состоянии комплекс выключен. Для обеспечения возможности использования комплекса по назначению на узле СБ ПЭВМ 1 инсталлируется пакет программного обеспечения (ПО). При этом на СБ ПЭВМ 1 осуществляется установка операционной системы (ОС), обеспечивающей управление функциями программно-аппаратных средств комплекса, формирование интерфейса пользователя с предоставлением ему возможностей ввода и/или вывода информации с помощью клавиатуры 8, узла МТМ 10, монитора 3 и принтера 6, установки программного обеспечения, ориентированного для обработки информации, необходимой пользователю, установки программного обеспечения для защиты ОС и пользовательской информации от вирусов, установки программного обеспечения для шифрования данных и программного обеспечения для выполнения доверенной загрузки ОС с использованием USB-ключа 14. Также инсталлируются драйверы для работы аппаратных узлов комплекса (монитора 3, принтера 6 и др.) под управлением ОС, установленной на СБ ПЭВМ 1. После установки ПО, необходимого для функционирования комплекса, к нему может быть допущен персонал для использования комплекса по назначению.

Персоналу, допущенному для выполнения работ на комплексе, выдается идентификационный USB-ключ 14. Работа на комплексе начинается с того, что пользователем АРМ активируется (включается) узел ГЭМП 7, который в локальной зоне размещения аппаратных узлов комплекса формирует электромагнитное поле (ЭМП) 9, спектр которого перекрывает спектр излучений, которые образуются в процессе функционирования программно-аппаратных узлов комплекса.

ЭМП 9, созданное ГЭМП 7, принимается узлом ДП 13 и выполняет его широкополосную демодуляцию. При этом, ДП 13 настроен таким образом, что при наличии на его входе интенсивного ЭМП 9, на выходе ДП 13 формируется сигнал высокого уровня, который подается на узел МК 12. При получении сигнала высокого уровня от ДП 13 узлом МК 12 осуществляется включения коммутатора 11. При включении коммутатора 11 осуществляется коммутация USB-ключа 14 к узлу СБ ПЭВМ 1.

После этого, пользователь включает СБ ПЭВМ 1. Происходит загрузка ОС, в процессе которой обеспечивается доверенная загрузка с аутентификацией пользователя по USB-ключу 14. Отсутствие USB-ключа 14 блокирует доступ к ОС.

Если по какой либо причине узел ГЭМП 7 будет деактивирован, то на вход узла ДП 13 перестанет поступать ЭМП 9. Это приведет к тому, что на выходе ДП 13 установится низкий уровень сигнала. При подаче низкого уровня сигнала на МК 12, на его выходе формируется сигнал выключения коммутатора 11. Это приведет к эмуляции отключения USB-ключа 14 от узла СБ ПЭВМ 1. В результате этого доступ к ОС, к программным, информационным и аппаратным ресурсам комплекса будет заблокирован.

После включения узла ГЭМП 7, работа улов ДП 13, МК 12, и коммутатора 11

осуществляется в порядке, описанном выше, в результате чего доступ к ОС комплекса - возобновляется.

Данный комплекс частично устраняет недостатки предыдущего АРМ. Это достигается за счет того, что в нем установлена ПОС - связь между доступом к операционной системе (ОС), установленной на СБ ПЭВМ 1 и наличием ЭМП 9, создаваемого при работе ГЭМП 7, который и обеспечивает необходимый уровень блокировки/маскировки ПЭМИН, формируемых в процессе работы технических средств АРМ.

При реализации обратной связи между функциями АРМ и активностью ГЭМП 7 уровень защищенности информации от утечек по каналу ПЭМИН существенно повышается. Это достигается за счет того, что возможность выполнения работ персоналом на АРМ, определяемая их доступом к интерфейсу СБ ПЭВМ 1, становится зависимой от наличия ЭМП 9 и рабочего состояния ГЭМП 7, обеспечивающего подавление и/или маскировку ПЭМИН, создаваемых АРМ. Если ГЭМП 7 функционирует в штатном режиме и ЭМП 9 - есть, то доступ к ресурсам АРМ (СБ ПЭВМ 1) - открыт, а если ЭМП 7 - отсутствует, из-за того что ГЭМП 7 по той или иной причине не функционирует, то доступ к ОС СБ ПЭВМ 1 - блокируется. При этом, персонал не может продолжить эксплуатацию АРМ при деактивированном узле ГЭМП 7. То есть, последствия не регламентированных действий легитимного персонала, приведших к деактивации узла ГЭМП 7, частично устраняются.

Таким образом, в случаях деактивации (отключения, выхода из строя и т.п.) ГЭМП 7, обеспечивается ограничение доступа к ресурсам ОС и функциям АРМ до тех пор, пока ГЭМП 7 будет снова включен и в локальной зоне размещения АРМ будет сформировано ЭМП 9 для подавления/маскировки ПЭМИН. Это способствует повышению уровня защиты информации от утечек по техническому каналу типа ПЭМИН, которые образуются при эксплуатации АРМ.

Недостатком данного комплекса-прототипа является низкий уровень защиты информации от утечек по техническому каналу типа ПЭМИН. Это обусловлено следующими факторами.

В АРМ-прототипе узел ДП 13 выполнен с возможностью приема и широкополосной демодуляции ЭМП 9, формируемого и излучаемого узлом ГЭМП 7. Это означает, что узел ДП 13 может детектировать радиосигналы, которые распределены по диапазону частот в широкой полосе. Такое свойство обеспечивает прием всех сигналов, которые поступают из радиоэфира на вход ДП 13. Из [Л11-Л13] известно, что радиодиапазон насыщен сигналами от множества источников, в том числе, от средств радиосвязи, вещательных радиостанций, излучений от промышленных объектов, автотранспорта и бытовых приборов и др. Сигналы, созданные всеми этими объектами, также могут поступать на вход ДП 13 и вызывать его ложное срабатывание при отсутствии активности узла ГЭМП 7. То есть, если узел ГЭМП 7 будет по тем или иным причинам деактивирован, например, выйдет из строя или не отключен персоналом, эксплуатирующим АРМ, то поступающие на вход узла ДП 13 радиосигналы от посторонних (относительно узла ГЭМП 7) источников излучения могут быть восприняты в качестве ЭМП 9, в то время, когда они таковыми не являются. Это приводит к опасной, с точки зрения утечки информации с АРМ, ситуации, которую условно можно назвать «пропуск тревог».

Установлено, что эти «пропуски тревог» обусловлены тем, что в данном

техническом решении, для идентификации активности ТСЗИ (ГЭМП 7), предназначенного для подавления/маскировки ПЭМИН, используется признак с низкой информативностью, что не обеспечивает получение достоверных данных, необходимых для реализации надежного контроля активности ГЭМП 7.

При функционировании АРМ образуются побочные электромагнитные излучения, спектр которых распределен в широком диапазоне радиочастот, поэтому для их маскировки узел ГЭМП 7 выполнен с возможностью формирования шумового радиосигнала со спектром, перекрывающим спектр в котором могут быть созданы ПЭМИН. Для приема и обработки сигналов, формируемых ГЭМП 7, то есть реагирования на ЭМП 9, радиоприемник узла ДП 13 тоже выполнен широкополосным. Это приводит к тому, что в широкополосный тракт узла ДП 13 будут попадать излучения от множества посторонних источников радиоизлучений (ИРИ), которыми интенсивно насыщен эфир. То есть, узлом ДП 13 будут приниматься радиосигналы от бытовых радио и телевизионных передатчиков, передатчики от систем радиорелейной и сотовой связи и др. В результате этого, сигналы от упомянутых посторонних ИРИ будут восприниматься как ЭМП 9, создаваемое ГЭМП 7, в то время как сам ГЭМП 7 может быть выключен или выведенным из строя по тем или иным причинам, в том числе по вине персонала, эксплуатирующего АРМ.

В данном комплексе (прототипе), в случаях деактивации узла ГЭМП 7, узлом ДП 13 могут приниматься сигналы посторонних ИРИ, на основе которых будет ложно идентифицироваться наличие активности ГЭМП 7, поэтому возможность использования АРМ по назначению при деактивированном узле ГЭМП 7, то есть без маскировки/подавления ПЭМИН, создаваемых АРМ, - сохраняется, что существенно снижает эффективность защиты информации от утечек по техническому каналу типа ПЭМИН.

Исследования показали, что низкая надежность идентификации активности узла ГЭМП 7, в данном техническом решении обусловлена использованием для принятия соответствующего решения (что узел ГЭМП 7 - активен) признаков с низкой информативностью. По сути, узел ДП 13 не обладает свойствами, позволяющими надежно идентифицировать сигналы создаваемые узлом ГЭМП 7. Поэтому, формируемая в техническом решении прототипа обратная связи между функциями АРМ и активностью ГЭМП 7 - является слабой и не устойчивой, что существенно снижает надежность защиты информации, содержащейся в АРМ, от ее утечек по техническому каналу типа ПЭМИН.

Следует заметить, что усилить упомянутую ПОС только лишь с использованием признаков и свойств АРМ-прототипа не представляется возможным, так как надежная идентификация ЭМП 9, создаваемого узла ГЭМП 7 - не обеспечивается. Это обусловлено тем, что ЭМП 9 и сигнал от посторонних ИРИ - находятся в одной полосе радиочастот, а мощность узла ГЭМП 7 - ограничена соответствующими стандартами и распределена («размазана») по широкому диапазону, поэтому, в полосе приема узла ДП 13 могут присутствовать сосредоточенные помехи от посторонних ИРИ с уровнем мощности, превышающим интенсивность сигналов ЭМП 9. То есть, ни по частоте, ни по мощности надежная идентификация сигналов, создаваемых узлом ГЭМП 7 - не может быть реализована с использованием признаков и свойств, присущих комплексу-прототипу.

Упомянутая ПОС, то есть, связь между активностью ГЭМП 7 и доступом к ресурсам АРМ в комплексе-прототипе имеет низкую надежность из-за действия

субъективных факторов (нерегламентированных действий легитимного персонала) и объективных факторов (эфирных ЭМП). В данном комплексе, при выходе из строя ТСЗИ (ГЭМП 7), а также при нерегламентированных действиях персонала, повлекших деактивацию узла ГЭМП 7, АРМ может функционировать без наличия ЭМП 9 из-за наличия в эфире достаточного количества посторонних ИРИ, излучения которых могут приводить к образованию ситуаций типа «пропуски тревог», при которых деактивация узла ГЭМП 7 не вызывает блокировки функций АРМ и функционирование (эксплуатация) которого может продолжаться без подавления/маскировки канала ПЭМИН, по которому возможна утечка информации, циркулирующей на АРМ.

Для повышения уровня защиты информации, содержащейся и циркулирующей в автоматизированном рабочем месте (АРМ), от несанкционированного доступа (НСД) к ней методом перехвата и анализа побочных электромагнитных излучений и наводок, возникающих в процессе эксплуатации автоматизированного рабочего места, авторами предложено значительно усилить упомянутую ПОС между функциями доступа к АРМ и активностью технических средств активной защиты типа ГЭМП 7. Это позволит устранить ситуации типа «ложных пропусков» и обеспечить гарантированное функционирования АРМ с постоянно действующим техническим средством активной защиты информации, содержащейся и циркулирующей в АРМ, от ее утечек по техническому каналу типа ПЭМИН.

Целью полезной модели является расширение функциональных возможностей автоматизированного рабочего места (АРМ) по контролю активности технических средств защиты информации от утечек по техническому каналу типа ПЭМИН, которые образуются при функционировании упомянутого АРМ.

Поставленная цель достигается за счет того, что в известное автоматизированное рабочее место (АРМ), состоящее из системного блока персональной электронно-вычислительной машины (СБ ПЭВМ), монитора, принтера, клавиатуры, манипулятора типа мышь (МТМ), сетевого фильтра (СФ), блока электрических розеток (БЭР), USB ключа, микроконтроллера (МК), коммутатора, генератора широкополосного электромагнитного поля (ГЭМП), широкополосного детектора электромагнитного поля (ДП), который выполнен с возможностью приема и широкополосной демодуляции радиосигналов и выход которого соединен с первым портом узла МК, который вторым портом соединен с первым портом коммутатора, который вторым и третьим портами соединен, соответственно, с USB ключом и первым портом узла СБ ПЭВМ, который со второго по пятый портами соединен, соответственно, с портом узла МТМ, с портом клавиатуры, с портом принтера и с портом монитора, который входом электропитания соединен с первым выходом узла СФ, который вторым выходом, третьим выходом и входом соединен, соответственно, со входом электропитания принтера, со входом электропитания узла СБ ПЭВМ и первым выходом блока электрических розеток (БЭР), который входом соединен с питающей электрической сетью (ПЭС) 220 В, и выполненное с возможностью установки на СБ ПЭВМ программного обеспечения (ПО) в виде операционной системы (ОС), обеспечивающей формирование интерфейса пользователя АРМ для управления функциями АРМ, программно-аппаратных средств доверенной загрузки ОС на узле СБ ПЭВМ, функционирования узла микроконтроллера по программе, обеспечивающей возможность обработки сигналов, поступающих с узла ДП и формирования сигналов блокировки доступа к интерфейсу пользователя узла СБ ПЭВМ, дополнительно введен датчик тока (ДТ),

который входом, первым и вторым выходами соединен, соответственно, со вторым выходом узла БЭР, входом узла ГЭМП и третьим портом узла МК, при этом, узел ДТ выполнен с возможностью измерения тока, протекающего в цепи электропитания узла ГЭМП, узел МК выполнен с возможностью функционирования по программе, обеспечивающей многоканальный приема и комплексную обработку сигналов, одновременно поступающих от узлов ДТ и ДП, с распознаванием (идентификацией) активности узла ГЭМП по уровню потребляемой им мощности и наличию излучаемого им электромагнитного поля, синтез устойчивой к воздействию внешних факторов обратной связи в виде функциональной зависимости между режимами работы программно-аппаратных средств доверенной загрузки операционной системы узла СБ ПЭВМ и активностью узла ГЭМП, формирование сигналов управления доступом к функциям АРМ, путем эмуляции подключения или отключения USB-ключа от узла СБ ПЭВМ, с использованием результатов упомянутой идентификации наличия или отсутствия активности узла ГЭМП.

В предлагаемом техническом решении обеспечивается следующее сочетание отличительных признаков и свойств.

Это - введение в состав АРМ датчик тока (ДТ), который входом, первым и вторым выходами соединен, соответственно, со вторым выходом узла БЭР, входом узла ГЭМП и третьим портом узла МК. При этом, узел ДТ выполнен с возможностью измерения тока, протекающего в цепи электропитания узла ГЭМП, что позволяет диагностировать работоспособность изделия. Введение этих признаков и использования новых свойств обеспечивает существенное повышение надежности контроля активности (режимов работы) узла ГЭМП.

Это - функционирование узла МК по программе, обеспечивающей возможность многоканального приема и комплексной обработки сигналов, одновременно поступающих от узлов ДТ и ДП, с распознаванием (идентификацией) активности узла ГЭМП по уровню потребляемой им мощности и наличию излучаемого им электромагнитного поля.

Это - синтез устойчивой к воздействию внешних факторов обратной связи в виде функциональной зависимости между режимами работы программно-аппаратных средств доверенной загрузки операционной системы узла СБ ПЭВМ и активностью узла ГЭМП.

Это - формирование сигналов управления доступом к функциям АРМ, путем эмуляции подключения или отключения USB-ключа от узла СБ ПЭВМ, с использованием результатов упомянутой идентификации наличия или отсутствия активности узла ГЭМП.

Использование новых признаков и свойств позволяет полностью устранить ситуации, соответствующие «пропуску тревог», так как идентификация активности узла ГЭМП осуществляется с использованием двух надежных признаков (факторов): наличию ЭМП, создаваемого узлом ГЭМП, и уровню тока, потребляемого этим узлом. Двухфакторная идентификация активности узла ГЭМП позволяет организовать устойчивую к воздействию различных факторов обратную связь между активностью технического средства защиты информации от утечек по ПЭМИН и доступом к системным и информационным ресурсам АРМ.

Наличие указанных признаков позволяет реализовать новые свойства, которые существенным образом влияют на достижение поставленной цели.

Наличие и использование всех, указанных выше признаков и свойств позволяет существенным образом усилить упомянутую обратную связь между доступом к

функциям АРМ и активностью ТС АЗ (узел ГЭМП), что обеспечивает возможность эксплуатации АРМ только лишь в режиме с маскированным и/или подавленным техническим каналом (ПЭМИН) утечки информации.

Сочетание отличительных признаков и свойств, предлагаемого автоматизированного рабочего места с защитой информации от утечек по каналу ПЭМИН, из техники неизвестно, поэтому оно соответствует критерию новизны. При этом, для достижения максимального эффекта по расширению функциональных возможностей автоматизированного рабочего места (АРМ) по контролю активности технических средств защиты информации от утечек по техническому каналу типа ПЭМИН, которые образуются при функционировании упомянутого АРМ, необходимо использовать всю совокупность отличительных признаков и свойств, указанных выше.

На фиг.2 приведена функциональная схема автоматизированного рабочего места с защитой информации от утечек по каналу ПЭМИН (далее - комплекс).

Комплекс (фиг.2), состоит из системного блока персональной электронно-вычислительной машины (СБ ПЭВМ) 1, сетевого фильтра (СФ) 2, монитора 3, блока электрических розеток (БЭР) 4, принтера 6, клавиатуры 7, генератора широкополосного электромагнитного поля (ГЭМП) 8, датчика тока (ДТ) 9, манипулятора типа мышь (МТМ) 10, USB ключа 12, широкополосного детектора электромагнитного поля (ДП) 13, коммутатора 14 и микроконтроллера (МК) 15. При этом, узел БЭР 4 своими входом, первым выходом и вторым выходом соединен, соответственно, с питающей силовой электросетью 220 В (ПЭС) 5, с первым портом узла ДТ 9 и с узлом СФ 2, который первым, вторым и третьим выходами соединен, соответственно, со входом электропитания монитора 3, со входом электропитания принтера 6, и со входом электропитания узла СБ ПЭВМ 1, который своими пятью портами, соединен, соответственно, с портом монитора 3, с портом принтера 6, с портом клавиатуры 7, с портом узла МТМ 10 и с первым портом коммутатора 14, который вторым и третьим портами соединен, соответственно, с USB-ключом 12 и с первым портом узла МК 15, который вторым и третьим портами соединен, соответственно, с выходом узла ДП 13 и вторым портом узла ДТ 9, который третьим портом соединен с узлом ГЭМП 8, который выполнен с возможностью формирования широкополосного электромагнитного поля (ЭМП 11). Кроме того, узел ДП 13, выполнен с возможностью приема и широкополосной демодуляции радиосигналов, узел ДТ 9 выполнен с возможностью измерения величины тока, потребляемого узлом ГЭМП 8 от узла БЭР 4, узел СБ ПЭВМ 1 выполнен с возможностью установки и функционирования на нем программного обеспечения (ПО) в виде операционной системы (ОС), обеспечивающей формирование интерфейса пользователя АРМ для управления функциями АРМ, программно-аппаратных средств доверенной загрузки операционной системы. При этом, узел МК 15 функционирует по программе, обеспечивающей возможность одновременного приема и комплексной обработки сигналов, поступающих от узла ДТ 9 и данных, поступающих от узла ДП 13 с распознаванием (идентификацией) активности узла ГЭМП 8 по одновременному наличию излучаемого им ЭМП 11 и уровню потребляемого им тока, синтеза устойчивой к воздействию внешних факторов обратной связи в виде функциональной зависимости между процедурой доверенной загрузки операционной системы узла СБ ПЭВМ 1 и активностью узла ГЭМП 8 для контроля и управления доступом к функциям АРМ с использованием результатов упомянутой идентификации наличия или отсутствия активности узла

ГЭМП 8 путем эмуляции, соответственно, подключения или отключения USB-ключа 12 к узлу СБ ПЭВМ 1.

Комплекс (фиг.2) функционирует следующим образом. В исходном состоянии комплекс выключен. Для обеспечения возможности использования комплекса по назначению на узле СБ ПЭВМ 1 инсталлируется пакет программного обеспечения (ПО). При этом на СБ ПЭВМ 1 осуществляется установка операционной системы (ОС), обеспечивающей управление функциями программно-аппаратных средств комплекса, формирование интерфейса пользователя с предоставлением ему возможностей ввода и/или вывода информации с помощью клавиатуры 7, узла МТМ 10, монитора 3 и принтера 6, установки программного обеспечения, ориентированного для обработки информации, необходимой пользователю, установки программного обеспечения для защиты ОС и пользовательской информации от вирусов, установки программного обеспечения для шифрования данных и программного обеспечения для выполнения доверенной загрузки ОС с использованием USB-ключа 12. Также инсталлируются драйверы для работы аппаратных узлов комплекса (монитора 3, принтера 6 и др.) под управлением ОС, установленной на СБ ПЭВМ 1. После установки ПО, необходимого для функционирования комплекса, к нему может быть допущен персонал для использования комплекса по назначению.

Работа на комплексе начинается с того, что активируется (включается) узел ГЭМП 8, который в локальной зоне размещения аппаратных узлов комплекса формирует ЭМП 11 для маскировки/подавления ПЭМИН, которые образуются в процессе функционирования программно-аппаратных узлов комплекса.

ЭМП 11 принимается узлом ДП 13, который выполняет его широкополосную демодуляцию. ДП 13 настроен таким образом, что при наличии на его входе интенсивного ЭМП 11, на выходе ДП 13 формируется сигнал высокого уровня, который подается на первый порт узла МК 15.

При включении узла ГЭМП 8 в цепи его электропитания протекает ток, который фиксируется узлом ДТ 9. Так как ДТ 9 выполнен с возможностью измерения величины тока, потребляемого узлом ГЭМП 8 от узла БЭР 4, то данные, полученные от узла ДТ 9 постоянно подаются на узел МК 15. В простейшем случае, логика работы узла ДТ 9 может быть основана на контроле уровня тока, потребляемого узлом ГЭМП 8. Например, путем формирования на выходе узла ДТ 9 логической единицы (высокого уровня напряжения), при превышении тока, потребляемого узлом ГЭМП 8, заданного порогового значения и формирования на выходе узла ДТ 9 логического нуля (низкого уровня напряжения), при уровне тока, потребляемого узлом ГЭМП 8, ниже установленного порога. Сигнал с узла ДТ 9 подается на второй порт узла МК 15. При одновременном получении высоких уровней сигналов от узлов ДП 13 и ДТ 9, узлом МК 15 осуществляется включения коммутатора 14. При включении коммутатора 14 выполняется коммутация USB-ключа 12 к порту узла СБ ПЭВМ 1.

Когда сигналы, поступающие с узлов ДП 13 и ДТ 9, имеют уровень, соответствующий логической единице, то доступ к функциям комплекса - открыт. Персонал, допущенный к АРМ, может использовать комплекс по назначению. Доверенная загрузка ОС на СБ ПЭВМ 1 с аутентификацией пользователя по USB-ключу 12 - обеспечивается.

Если по какой либо причине узел ГЭМП 8 будет деактивирован, то на вход узла ДП 13 перестанет поступать ЭМП 11 и ток, потребляемый узлом ГЭМП 8,

существенно снизится или прекратится совсем. В результате этого, на выходе узлов ДП 13 и ДТ 9 появятся сигналы, соответствующие логическому нулю. При наличии в локальной зоне размещения комплекса интенсивных радиоизлучений от посторонних ИРИ, они могут детектироваться узлом ДП 13 и приводить к формированию на его выходе уровня, соответствующего логической единице. Для нейтрализации влияния внешних факторов, узел МК 15 вырабатывает сигналы, соответствующие эмуляции подключения USB-ключа 12 к порту узла СБ ПЭВМ 1, только при одновременном наличии сигналов логической единицы на выходах узлов ДП 13 и ДТ9.

После активации узла ГЭМП 8, комплекс возвращается в рабочее состояние и доступ к системным и информационным ресурсам комплекса - возобновляется.

Таким образом, узлом МК 15 обеспечивается одновременный прием и комплексная обработка сигналов, поступающих от узла ДТ 9 и данных, поступающих от узла ДП 13. Это позволяет надежно распознавать (идентифицировать) активность узла ГЭМП 8 по одновременному наличию излучаемого им ЭМП 11 и уровню потребляемого им тока. Это также обеспечивает формирование устойчивой функциональной зависимости между процедурой доверенной загрузки операционной системы узла СБ ПЭВМ 1 и активностью узла ГЭМП 8. Наличие устойчивой к воздействию внешних факторов обратной связи между доступом к функциям комплекса и активностью узла ГЭМП 8 обеспечивает надежный контроль и управление доступом к функциям комплекса с использованием результатов упомянутой идентификации наличия или отсутствия активности узла ГЭМП 8 путем эмуляции подключения или отключения USB- ключа 12 к порту узла СБ ПЭВМ1.

Техническим результатом, достигаемым при реализации данной полезной модели, является повышение надежности идентификации активности узла ГЭМП 8, что достигается за счет увеличения количества и информативности используемых признаков, снижение вероятности утечки информации по техническому каналу типа ПЭМИН, что достигается за счет сокращения времени эксплуатации комплекса в не защищенном режиме - при деактивированном (выключенном) узле ГЭМП 8 и повышение устойчивости к воздействию внешних факторов обратной связи между доступом к функциям комплекса и активностью узла ГЭМП 8, что достигается за счет непосредственного контроля (измерения) его рабочих электрических параметров.

При реализации комплекса, его алгоритм функционирования может быть представлен в следующем виде:

- Начало;
- Запуск операционной системы на СБ ПЭВМ 1;
- Проверка-1: сигнал логической единицы с выхода узла ДП 13 - есть? Если нет, то возврат, если - Да, то переход к проверке - 2;
- Проверка-2: сигнал логической единицы с выхода узла ДТ 9 - есть? Если нет, то возврат, если - Да, то продолжение;
- Запуск пользовательской программной среды, выполнение работ на АРМ;
- Проверка-3: сигнал логической единицы с выхода узла ДП 13 - есть? Если нет, то блокировка доступа к интерфейсу пользователя, запрос авторизации пользователя. Если - Да, то переход к проверке - 4;
- Проверка-4: сигнал логической единицы с выхода узла ДТ 9 - есть? Если нет, то блокировка доступа к интерфейсу пользователя, запрос авторизации пользователя.

Если - Да, то продолжение;

- Завершение работы: выключение СБ ПЭВМ 1, отключение USB-ключа 12, выключение ГЭМП 8;

- Конец.

Узлы СБ ПЭВМ 1, СФ 2, монитора 3, БЭР 4, принтера 6, клавиатуры 7, ГЭМП 8, МТМ 10, USB-ключа 12, широкополосного детектора электромагнитного поля 13, коммутатора 14 и МК 15, могут быть аналогичными соответствующим признакам и свойствам АРМ-прототипа и не требуют доработки при их реализации.

Узел ДТ 9 может быть может быть реализован на датчиках тока открытого типа фирмы Honeywell, которые построены на базе интегрированных линейных датчиков Холла типа 91SS12-2 и SS94A1 [Л14], обладающих повышенной температурной стабильностью и линейностью характеристики. Эти датчики имеют аналоговый выход, напряжение на котором прямо пропорционально величине тока, протекающего через контролируемый проводник. При этом, дополнительная регулировка чувствительности производится путем увеличения числа витков проводника с током вокруг кольца магнитопровода датчика. Альтернативным вариантом реализации узла ДТ 9 является использование компенсационных датчиков тока, например, модели CSNE151, CSNE381 [Л14], которые позволяют бесконтактным способом измерять постоянный, переменный и импульсный токи в широком диапазоне их значений (до ±1200 А). Эти датчики преобразуют токовый выход в напряжение, имеют регулировку чувствительности, которая также осуществляется путем увеличения числа витков проводника вокруг кольца магнитопровода датчика или установкой перемычек, задающих число витков внутренней компенсационной катушки датчика.

При реализации узлов данного комплекса могут быть также использованы технологические, конструктивные и программно-аппаратные решения, известные из [Л15-Л21].

Как показано, предлагаемое техническое решение позволяет успешно решить поставленную задачу по повышению уровня защиты информации, содержащейся и циркулирующей в автоматизированном рабочем месте, от несанкционированного доступа к ней методом перехвата и анализа побочных электромагнитных излучений и наводок, возникающих в процессе эксплуатации упомянутого автоматизированного рабочего места. При этом эффективное решение упомянутой задачи обеспечивается на основе расширения функциональных возможностей автоматизированного рабочего места (АРМ) по контролю активности технических средств защиты информации от утечек по техническому каналу типа ПЭМИН, которые образуются при функционировании упомянутого АРМ, а также использованию достигаемого технического результата. Следует отметить, что благодаря использованию данного технического решения риски утечек информации, обусловленные нерегламентированными действиями персонала, при которых работа комплекса может осуществляться при деактивированных средствах активной защиты комплекса (узла ГЭМП 8), полностью устраняются. То есть, при деактивации узла ГЭПМ 8 - доступ к функциям АРМ - блокируется.

Приведенные средства, с помощью которых возможно осуществление полезной модели, позволяют обеспечить ее промышленную применимость.

Основные узлы комплекса экспериментально проверены и могут быть положены в основу создания образцов комплексов, обеспечивающих эффективную защиту информации от несанкционированного доступа со стороны ПФЛ, который может

быть организован на основе перехвата и анализа ПЭМИН, излучаемых в процессе эксплуатации комплекса.

Разработанное авторами техническое решение и получаемый с помощью его технических результат, предоставляет возможность значительного повышения уровня защиты информации, содержащейся и циркулирующей в автоматизированном рабочем месте, от несанкционированного доступа по техническому каналу типа ПЭМИН, возникающему при эксплуатации комплекса, маскировка и/или подавление которого может нарушаться при деактивации технических средств активной защиты типа широкополосного генератора электромагнитного поля, в том числе, в результате нарушения правил эксплуатации комплекса и/или иных нерегламентированных действий персонала, эксплуатирующего данный комплекс, а также случайных воздействий внешней среды, например, действия эфирных электромагнитных полей.

Автоматизированное рабочее место с защитой информации от утечек по каналу ПЭМИН будет востребовано широким кругом потребителей, использующих вычислительную технику для обработки конфиденциальной информации, нуждающейся в защите от утечек, которые могут быть вызваны деактивацией технических средств маскировки и/или подавления канала типа ПЭМИН, который возникает в процессе эксплуатации АРМ.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Автоматизированное рабочее место,http://ru.wikipedia.org/wiki/

2. ГОСТ Р 51275-99 Защита информации.http://www.centre-expert.ru/index.php/infosec/

3. Угрозы информационной безопасности, http://www.bre.ru/security/

4. Технический канал утечки информации. Терминология в области защиты информации, http://www.centre-expert.ru/index.php/infosec/

5. Исследования побочных электромагнитных излучений технических средств, http://www.pemi.ru/

6. Защита компьютерной информации от утечки по ПЭМИН, http: //www.support17.com/component/content/39.html?task=view

7. Скрытая утечка информации. Компьютерная стеганография и ПЭМИН - вирус, http://www.cio-world.ru/bsolutions/e-safety/28763/page2.html

8. Автоматизированное рабочее место обмена закрытой документальной информацией, полезная модель №80040, дата публикации: 20.01.2009 г.

9. Доверенная загрузка,http://ru.wikipedia.org/wiki/

10. ФГУП «18 ЦНИИ» МО РФ, Патент на полезную модель «Автоматизированное рабочее место с защитой от несанкционированного доступа», зарегистрирован за №96435 от 27.07.2010 г., авторы: Галах В.П., Лакеев В.А., Егоров В.И., Хотячук В.К., Шкирин В.Г.

11. Электромагнитное излучение,http://ru.wikipedia.org/wiki/%D0%

12. Источники электромагнитных помех, http://www.obzor-electro.ru/publ/ehl_magnitnaja_sovmestimost/istochniki_ehlektromagnitnykh_pomekh/9-1-0-53

13. Электромагнитные помехи и их классификация, http: //www.vxi.su/praktikum/elektromagnitnye-pomehi/

14. Датчики тока на эффекте Холла,http://news.cxem.net/articles/circuit_268.php

15. Полезная модель «Накопитель с контролем местоположения». Патент на полезную модель №90233 от 27.12.2009 г. авторы: Баталов А.В., Хотячук В.К., Хотячук К.М., Тимошкин В.С.

16. ФГУП «18 ЦНИИ» МО РФ, программа для ЭВМ «Менеджер сенсора»,

Свидетельство о государственной регистрации в ФИПС РФ №2009610444 от 19.01.2009 г., авторы: Хотячук В.К., Хотячук К.М. и др.

17. ФГУП «18 ЦНИИ» МО РФ, Программа для ЭВМ «Контроллер приемопередатчика». Свидетельство о государственной регистрации в ФИПС РФ №2009610445 от 19.01.2009 г., авторы: Бакунин И.Б., Хотячук В.К., Хотячук К.М., Гончаров В.С.

18. ФГУП «18 ЦНИИ» МО РФ, Программа для ЭВМ «Монитор коммуникационного оборудования». Свидетельство о государственной регистрации в ФИПС РФ №2009611020 от 16.02.2009 г., авторы: Васин М.С., Шелестов М.Е., Хотячук В.К.

19. ФГУП «18 ЦНИИ» МО РФ, Полезная модель «Защищенный накопитель», Патент на полезную модель №87276 от 29.05.2009 г. авторы: Хотячук В.К., Хотячук К.М., Тимошкин В.С., Покормяк Л.В.

20. ФГУП «18 ЦНИИ» МО РФ, Полезная модель «Накопитель с защитой от несанкционированного доступа к памяти», Патент на полезную модель №84594 от 10.07.2009 г., авторы: Вдовин Е.И, Хотячук К.М., Хотячук В.К.

21. ФГУП «18 ЦНИИ» МО РФ, Полезная модель «Скрытый регистратор доступа на объект», Патент на полезную модель №86026 от 20.08.2009 г. авторы: Бугаенко О.В., Хотячук В.К., Хотячук К.М., Тимошкин В.С.

(57) Реферат

Полезная модель относится к электросвязи, а точнее к устройствам защиты компьютерных систем от несанкционированной деятельности и может быть использована в информационных системах и комплексах, преимущественно, оборудованных автоматизированным рабочим местом (АРМ), для повышения уровня защиты информации от несанкционированного доступа по техническому каналу, создаваемому за счет побочных электромагнитных излучений и наводок, которые возникают при функционировании технических средств, входящих в состав АРМ.

Сущность полезной модели заключается в том, что в известное автоматизированное рабочее место (АРМ), состоящее из системного блока персональной электронно-вычислительной машины (СБ ПЭВМ), монитора, принтера, клавиатуры, манипулятора типа мышь (МТМ), сетевого фильтра (СФ), блока электрических розеток (БЭР), USB-ключа, микроконтроллера (МК), коммутатора, генератора широкополосного электромагнитного поля (ГШЭП), широкополосного детектора электромагнитного поля (ШДЭП), выход которого соединен с первым портом узла МК, который вторым портом соединен с первым портом коммутатора, который вторым и третьим портами соединен, соответственно, с USB-ключом и первым портом узла СБ ПЭВМ, который со второго по пятый портами соединен, соответственно, с портом узла МТМ, с портом клавиатуры, с портом принтера и с портом монитора, который входом электропитания соединен с первым выходом узла СФ, который вторым выходом, третьим выходом и входом соединен, соответственно, со входом электропитания принтера, со входом электропитания узла СБ ПЭВМ и первым выходом блока электрических розеток (БЭР), который входом соединен с питающей электрической сетью (ПЭС) 220 В, выполненное с возможностью установки на СБ ПЭВМ программного обеспечения (ПО) в виде операционной системы (ОС), обеспечивающей формирование интерфейса пользователя АРМ для управления

функциями АРМ, программно-аппаратных средств доверенной загрузки ОС, функционирования узла микроконтроллера по программе, обеспечивающей обработку сигналов, поступающих с узла ШДЭП, и формирование сигналов управления доступом к интерфейсу пользователя узла СБ ПЭВМ, дополнительно введен датчик тока (ДТ), который входом, первым и вторым выходами соединен, соответственно, со вторым выходом узла БЭР, входом узла ГШЭП и третьим портом узла МК, при этом, узел ДТ выполнен с возможностью измерения тока, протекающего в цепи электропитания узла ГШЭП, узел МК выполнен с возможностью функционирования по программе, обеспечивающей многоканальный приема и комплексную обработку сигналов, одновременно поступающих от датчика тока и широкополосного детектора электромагнитного поля, с распознаванием (идентификацией) активности узла ГШЭП по уровню мощности, потребляемой упомянутым узлом ГШЭП от питающей электросети, и наличию в локальной зоне, где размещено АРМ, электромагнитного поля, созданного упомянутым узлом ГШЭП, управления доступом к функциям АРМ путем эмуляции подключения или отключения аппаратных средств доверенной загрузки, используемых в составе СБ ПЭВМ, соответственно, при наличии или отсутствии фактов упомянутой идентификации активности широкополосного детектора электромагнитного поля.

Введенные существенные признаки обеспечили возможность существенного повышения уровня защиты информации, содержащейся и циркулирующей в АРМ, от несанкционированного доступа по техническому каналу типа ПЭМИН, что достигнуто за счет повышения надежности контроля активности ТСЗИ, используемых для маскировки и/или подавление ПЭМИН, возникающих при эксплуатации АРМ, и ограничения доступа к функциям АРМ, при деактивации упомянутых ТСЗИ.

РЕФЕРАТ

Автоматизированное рабочее место

с защитой информации от утечек по каналу ПЭМИН

Полезная модель относится к электросвязи, а точнее к устройствам защиты компьютерных систем от несанкционированной деятельности и может быть использована в информационных системах и комплексах, преимущественно, оборудованных автоматизированным рабочим местом (АРМ), для повышения уровня защиты информации от несанкционированного доступа по техническому каналу, создаваемому за счет побочных электромагнитных излучений и наводок, которые возникают при функционировании технических средств, входящих в состав АРМ.

Сущность полезной модели заключается в том, что в известное автоматизированное рабочее место (АРМ), состоящее из системного блока персональной электронно-вычислительной машины (СБ ПЭВМ), монитора, принтера, клавиатуры, манипулятора типа мышь (МТМ), сетевого фильтра (СФ), блока электрических розеток (БЭР), USB- ключа, микроконтроллера (МК), коммутатора, генератора широкополосного электромагнитного поля (ГШЭП), широкополосного детектора электромагнитного поля (ШДЭП), выход которого соединен с первым портом узла МК, который вторым портом соединен с первым портом коммутатора, который вторым и третьим портами соединен, соответственно, с USB- ключом и первым портом узла СБ ПЭВМ, который со второго по пятый портами соединен, соответственно, с портом узла МТМ, с портом клавиатуры, с портом принтера и с портом монитора, который входом электропитания соединен с первым выходом узла СФ, который вторым выходом, третьим выходом и входом соединен, соответственно, со входом электропитания принтера, со входом электропитания узла СБ ПЭВМ и первым выходом блока электрических розеток (БЭР), который входом соединен с питающей электрической сетью (ПЭС) 220 В, выполненное с возможностью установки на СБ ПЭВМ программного обеспечения (ПО) в виде операционной системы (ОС),

обеспечивающей формирование интерфейса пользователя АРМ для управления функциями АРМ, программно-аппаратных средств доверенной загрузки ОС, функционирования узла микроконтроллера по программе, обеспечивающей обработку сигналов, поступающих с узла ШДЭП, и формирование сигналов управления доступом к интерфейсу пользователя узла СБ ПЭВМ, **дополнительно введен** датчик тока (ДТ), который входом, первым и вторым выходами соединен, соответственно, со вторым выходом узла БЭР, входом узла ГШЭП и третьим портом узла МК, при этом, узел ДТ выполнен с возможностью измерения тока, протекающего в цепи электропитания узла ГШЭП, узел МК выполнен с возможностью функционирования по программе, обеспечивающей многоканальный приема и комплексную обработку сигналов, одновременно поступающих от датчика тока и широкополосного детектора электромагнитного поля, с распознаванием (идентификацией) активности узла ГШЭП по уровню мощности, потребляемой упомянутым узлом ГШЭП от питающей электросети, и наличию в локальной зоне, где размещено АРМ, электромагнитного поля, созданного упомянутым узлом ГШЭП, управления доступом к функциям АРМ путем эмуляции подключения или отключения аппаратных средств доверенной загрузки, используемых в составе СБ ПЭВМ, соответственно, при наличии или отсутствии фактов упомянутой идентификации активности широкополосного детектора электромагнитного поля.

Введенные существенные признаки обеспечили возможность существенного повышения уровня защиты информации, содержащейся и циркулирующей в АРМ, от несанкционированного доступа по техническому каналу типа ПЭМИН, что достигнуто за счет повышения надежности контроля активности ТСЗИ, используемых для маскировки и/или подавление ПЭМИН, возникающих при эксплуатации АРМ, и ограничения доступа к функциям АРМ, при деактивации упомянутых ТСЗИ.

RU 107 608 U1

2010153819

МКИ G06F 21/00

АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО С ЗАЩИТОЙ ИНФОРМАЦИИ ОТ УТЕЧЕК ПО КАНАЛУ ПЭМИН

Полезная модель относится к электросвязи, а точнее к устройствам защиты компьютерных систем от несанкционированной деятельности и может быть использована в информационных системах и комплексах, преимущественно, оборудованных автоматизированным рабочим местом (АРМ), для защиты информации от несанкционированного доступа, который может быть организован на основе перехвата и анализа побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых АРМ, особенно в случаях деактивации технических средств, используемых в составе АРМ, для маскировки или подавления упомянутых ПЭМИН.

Для обработки и хранения различных видов информации широко применяются средства вычислительной техники, организованные в виде автоматизированных рабочих мест (АРМ) [Л1].

Как отмечают многие эксперты, содержащаяся и циркулирующая в АРМ информация часто становится объектом пристального внимания и «охоты» со стороны посторонних физических и юридических лиц (конкурентов злоумышленников и т.п.), которые используют различные методы и технологи для осуществления несанкционированного доступа (НСД) к системным и информационным ресурсам АРМ.

Как известно [Л2, Л3], защита АРМ от несанкционированного доступа к находящейся в нем информации (НСДИ), то есть, к информации, которая находится в памяти компьютера АРМ, на съемных и несъемных носителях информации, а также отображается на экране монитора, излучается в радиоэфир, распространяется по проводным и кабельным системам, является весьма сложной задачей. Сложность этой задачи вытекает из наличия

разноплановых угроз НСДИ и вероятных утечек информации по различным каналам, которые могут быть использованы злоумышленниками для реализации своих неблаговидных планов, связанных с «добычей» информации, циркулирующей в АРМ.

Как отмечают многие эксперты, наиболее опасным каналом утечки информации из АРМ является технический канал [Л4], формируемый побочными излучениями и наводками - ПЭМИН [Л5], которые образуются при функционировании технических средств, входящих в состав АРМ.

Исследования показали, что известные из техники решения в области защиты АРМ от утечек информации по техническому каналу типа ПЭМИН, имеют низкую эффективность. Это обусловлено влиянием на уровень защиты данного канала факторов объективного и субъективного характера. Основным объективным фактором является эффективность функционирования технических средств защиты информации (ТСЗИ), обеспечивающих маскировку и/или подавление ПЭМИН, возникающих при эксплуатации АРМ. К субъективным факторам можно отнести поведение и действия легитимного персонала, который в процессе эксплуатации АРМ должен выполнять установленные регламенты и инструкции по поддержке упомянутых ТСЗИ в исправном и активном состоянии при выполнении работ с использованием технических средств АРМ. Однако, на практике, при эксплуатации АРМ, регламенты использования упомянутых ТСЗИ, могут нарушаться. Персонал, выполняющий работы на АРМ, может игнорировать (преднамеренно или по халатности) установленные правила и не активировать (не обслуживать) технические средства маскировки/ подавления канала типа ПЭМИН. При этом, состояние исправности и/или активности ТСЗИ активной защиты канала типа ПЭМИН не препятствует выполнению работ на АРМ. Поэтому, продолжая работу на АРМ при деактивированных ТСЗИ, персонал создает условия для утечки информации по техническому каналу типа ПЭМИН.

По оценкам экспертов [Л5-Л7], излучение элементов компьютера и других технических средств АРМ, является достаточно информативным каналом утечки информации. Принимая и декодируя эти излучения, посторонние физические лица и/или злоумышленники могут получить сведения обо всей информации, обрабатываемой в компьютере АРМ. Современные достижения в области технологий производства радиоприемных устройств многоканального приема сигналов (как с различных направлений, так и на различных частотах), с последующей их корреляционной обработкой, позволяют обеспечить достаточную дальность перехвата информации. Процесс перехвата информации, циркулирующей в АРМ, например, путем приема паразитного излучения композитного сигнала монитора вполне реален. Более того, используются способы заставить компьютер передавать нужную информацию и не ждать, пока пользователь сам обратится к конфиденциальным документам. Это решается следующим образом: компьютер, входящий в состав АРМ, «заражается» специальной программой-закладкой типа «троянский конь» любым из известных способов по технологии вирусов: через компакт-диск с презентацией, интересной программой или игрушкой, диск с драйверами, а также через любой из каналов связи, к которому подключен АРМ (локальной сети, Интернет и др.). Далее, Spy-программа ищет необходимую информацию на диске ПЭВМ, и путем обращения к различным устройствам компьютера, инициирует в эфире побочные электромагнитные излучения и наводки. Например, Spy-программа может встраивать сообщение в композитный сигнал монитора, при этом пользователь, играя в любимую игру типа «Солитер», даже не подозревает, что в изображение игральных карт могут быть вставлены конфиденциальные текстовые сообщения или изображения. С помощью специального приемного устройства может обеспечиваться перехват паразитного излучения монитора и выделение требуемого полезного сигнала.

Проведенные экспериментальные исследования подтвердили такую возможность добывания конфиденциальной информации. В этом состоит один из вариантов технологии скрытой передачи данных по каналу побочных электромагнитных излучений с помощью программных средств. Предложенная учеными Кембриджа, подобная технология по своей сути есть разновидность компьютерной стеганографии, т.е. метода скрытной передачи полезного сообщения в безобидных видео, аудио, графических и текстовых файлах. Особенностью технологии является использование для передачи данных канала ПЭМИН, что значительно затрудняет обнаружение самого факта несанкционированной передачи по сравнению с традиционной компьютерной стеганографией. Так, если для предотвращения несанкционированной передачи данных по локальной сети или сети Интернет существуют аппаратные и программные средства (FireWall, Proxy server и т.п.), то средств для обнаружения скрытой передачи данных по ПЭМИН - отсутствуют, а обнаружить такое излучение в общем широкополосном спектре (более 1000 МГц) паразитных излучений ПЭВМ, без знания параметров полезного сигнала, весьма проблематично.

Основная опасность технологии передачи конфиденциальной информации с использованием ПЭМИН заключается в скрытности работы программы-вируса. Такая программа, в отличие от большинства вирусов, не «портит» данные, не нарушает работу ПЭВМ, не производит несанкционированную рассылку данных по сети, а значит, долгое время не обнаруживается пользователем и администратором сети. Поэтому, если вирусы, использующие Интернет для передачи данных, проявляют себя практически мгновенно, и на них быстро находится «противоядие» в виде антивирусных программ, то вирусы, использующие ПЭМИН для передачи данных, могут работать годами, не обнаруживая себя, управляя излучением практически любого элемента компьютера.

Исследования показали, что формировать ПЭМИН могут большинство элементов компьютера, клавиатура, манипулятор типа мышь, принтер и

другие технические устройства, содержащиеся в составе АРМ. При этом, сигналы, излучаемые этими устройствами, могут быть перехвачены без существенных затрат, так как информация в этих устройствах передается последовательным кодом, все параметры которого стандартизированы и хорошо известны.

Известно, что для предотвращения утечек информации из АРМ, наиболее широко используются широкополосные генераторы электромагнитного поля (ШГЭП), способные создавать в локальной (ближней) зоне, где размещены технические средства, входящие в состав АРМ, электромагнитное поле со спектром, перекрывающим ПЭМИН и вызывающих их маскировку и/или подавление. Это затрудняет ведение технической разведки, направленной на перехват и анализ ПЭМИН, создаваемых АРМ.

При использовании изделий типа ШГЭП предполагается, что прежде чем активировать АРМ, то есть включить системный блок ПЭВМ, монитор, и другие технические средства, входящие в состав автоматизированного рабочего места, пользователь в первую очередь должен проверить исправность ТСЗИ типа ШГЭП, например, осмотреть качество заземления, наличие антенно-фидерной систем, далее- включить электропитание этого устройства и, при необходимости, установить заданный режим работы.

Однако, как показали исследования, в известных технических решениях, используемых для защиты АРМ от утечек информации по каналу ПЭМИН, отсутствует эффективный контроль как технического состояния, так и активности упомянутых ТСЗИ. В результате, АРМ может использоваться по назначению без ограничения доступа к его функциям при деактивированных ТСЗИ. Как показано выше, деактивация ТСЗИ может быть вызвана как неисправностью технических средств, так случайным или преднамеренным их выключением персоналом, эксплуатирующим АРМ.

Исследования показали, что низкая эффективность известных технических решений, которые используются для защиты информации от утечек по техническому каналу типа ПЭМИН, образующемуся при

эксплуатации АРМ, обусловлена действием факторов, устранение которых затрудняется наличием противоречия: чтобы эксплуатировать АРМ-персонал надо допустить на рабочее место, при этом этот же персонал может тем или иным способом деактивировать ТСЗИ и создать условия утечки информации по каналу типа ПЭМИН. С другой стороны, чтобы предотвратить утечку информации по каналу типа ПЭМИН- надо запретить доступ персонала к АРМ.

В связи с этим, поиск технических решений, направленных на повышение уровня защиты информации, содержащейся и циркулирующей в автоматизированном рабочем месте, от несанкционированного доступа к ней методом перехвата и анализа побочных электромагнитных излучений и наводок, возникающих в процессе эксплуатации автоматизированного рабочего места, особенно в результате деактивации ТСЗИ, используемых для маскировки/ подавления канала типа ПЭМИН, является **актуальной задачей.**

Из техники [Л8] известно автоматизированное рабочее место (АРМ), состоящее из монитора, принтера, клавиатуры, манипулятора типа мышь (МТМ), USB ключа, системного блока персональной электронно-вычислительной машины (СБ ПЭВМ), генератора электромагнитного поля (ГЭМП), сетевого фильтра (СФ) и блока электрических розеток (БЭР), который входом, первым выходом и вторым выходом соединен, соответственно, с питающей электрической сетью 220 В (ПЭС), со входом электропитания узла ГЭМП и со входом узла СФ, который первым, вторым и третьим выходами соединен, соответственно, со входом электропитания монитора, со входом электропитания принтера и со входом электропитания узла СБ ПЭВМ, который первым, вторым, третьим, четвертым и пятым портами соединен, соответственно, с монитором, с принтером, с клавиатурой, с узлом МТМ и с USB ключом, и выполненное с возможностью установки и функционирования на узле СБ ПЭВМ программного обеспечения в виде операционной системы (ОС),

обеспечивающей управление функциями программно-аппаратных средств АРМ, формирование интерфейса пользователя с предоставлением ему возможностей ввода и/или вывода информации с помощью клавиатуры, узла МТМ, принтера и монитора, программного обеспечения для обработки информации, программного обеспечения для защиты информации от вирусов, программного обеспечения для шифрования данных и программного обеспечения для выполнения доверенной загрузки ОС с использованием аппаратного средства типа USB-ключа, по которому обеспечивается возможность аутентификации пользователя, контроль загрузки ОС и контроль доступа к программным, информационным и аппаратным ресурсам АРМ в процессе функционирования СБ ПЭВМ, кроме того, узел ГЭМП выполнен с возможностью формирования в локальной зоне, в которой размещены аппаратные узлы АРМ, электромагнитного поля (ЭМП) в широком спектре радиочастот.

Работа АРМ (комплекса) осуществляется типовым образом. Так, на компьютере АРМ (узле СБ ПЭВМ) инсталлируется системное программное обеспечение, например, типа Windows 2000/XP/Vista, устанавливаются также драйверы, необходимые для работы аппаратных средств, в том числе, клавиатуры, узла МТМ, принтера и монитора. Затем, в соответствии с видом обрабатываемой на комплексе информации, устанавливается (инсталлируется) прикладное программное обеспечение, например, для подготовки и обработки текстовой информации (создания документов, презентаций и т.п.) в ОС может инсталлироваться пакет офисных программ, например, Microsoft Office. Для защиты от НСД к ресурсам СБ ПЭВМ используется средств доверенной загрузки операционной системы, функционирующей на СБ ПЭВМ. При этом, аппаратной частью этих средств является USB-ключ. Как известно из [Л9], доверенная загрузка компьютера препятствуем несанкционированному запуску системного блока ПЭВМ, а также предотвращает загрузку операционной системы и получение возможности доступа к информации, содержащейся в АРМ. В область

действия средств доверенной загрузки входят этапы работы компьютера от запуска микропрограммы BIOS до начала загрузки операционной системы. Доверенная загрузка включает в себя: аутентификацию, контроль устройства, с которого BIOS начинает загрузку операционной системы, контроль целостности и достоверности загрузочного сектора устройства и системных файлов запускаемой операционной системы, шифрование/ дешифрование загрузочного сектора и системных файлов операционной системы.

При эксплуатации данного комплекса предусмотрена возможность использования генератора электромагнитного поля ГЭМП, который может излучать ЭМП со спектром, распределенным в широкой полосе. Это позволяет искусственно «зашумлять» радиоэфир, в том числе, ту полосу частот, где сосредоточены ПЭМИН, создаваемые работой узлов комплекса. В активном состоянии ГЭМП подавляет или маскирует ПЭМИН, которые образуются при работе комплекса, что существенно затрудняет работу злоумышленников по организации НСД к АРМ путем перехвата и последующего анализа информационных компонент, содержащихся в побочных электромагнитных излучениях технических средств АРМ.

Недостатком данного комплекса является его низкий уровень защиты информации от несанкционированного доступа, который может быть организован путем перехвата и анализа ПЭМИН, излучаемых аппаратными узлами комплекса в процессе его эксплуатации. Это обусловлено уязвимостью системы защиты комплекса к возможным нарушениям правил эксплуатации комплекса и нерегламентированным действиям персонала (НДП), выполняющего эксплуатацию АРМ. Так, по вине легитимных пользователей АРМ, функционирование узла ГЭМП может быть нарушено (по случайности или преднамеренно). Также узел ГЭМП может выйти из строя, а этот факт персоналом может быть проигнорирован или, просто не замечен (по халатности). Во всех указанных случаях возможность беспрепятственной работы персонала на АРМ - сохраняется. То есть, по субъективным причинам, могут быть созданы условия, при которых

подавление/ маскировка ПЭМИН, создаваемых комплексом, отсутствует (не выполняется), следовательно, возможна утечка информации по техническому каналу - за счет побочных электромагнитных излучений, которые, во время отсутствия в эфире искусственно созданного с помощью ГЭМП широкополосного электромагнитного излучения, используемого для маскировки/ подавления ПЭМИН, могут быть перехвачены злоумышленниками для организации несанкционированного доступа к информационным ресурсам АРМ путем перехвата и анализа ПЭМИН.

Анализ информационной защищенности АРМ показал, что эффективность его защиты от НСДИ по техническому каналу типа ПЭМИН может быть существенно повышена путем нейтрализации влияния субъективного фактора, то есть, устранения возможности легитимному персоналу продолжать эксплуатировать АРМ в случаях деактивации технических средств защиты информации (при выключенном узле типа ГЭМП).

Установлено, что задачу повышения надежности защиты АРМ от НСД по каналу типа ПЭМИН можно свести к созданию таких условий использования АРМ, при которых небрежность в обслуживании технических средств защиты информации и/или иные действия персонала, эксплуатирующего АРМ, повлекшие деактивацию ТСЗИ, вызвали ограничение доступа к функциям АРМ.

Например, допустим, что существует функциональная зависимость между доступом к интерфейсу пользователя системного блока ПЭВМ, входящего в состав АРМ, и активностью ТСЗИ, обеспечивающих маскировку/ подавление ПЭМИН, создаваемых АРМ.

Тогда, контролируя активность упомянутого узла типа ГЭМП, например, по наличию создаваемого им ЭМП, с одной стороны, и использованию контроля загрузки операционной системы на упомянутом СБ ПЭВМ, с другой стороны, можно реализовать прямую и обратную связь (ПОС),

позволяющую автоматизировать управление доступом к функциям АРМ в зависимости от активности ТСЗИ.

Прямая и обратная связь между управлением доступом к ресурсам ОС, функционирующей на СБ ПЭВМ, и активностью ТСЗИ, обеспечивающих защиту от утечек информации по техническому каналу типа ПЭМИН, в рассмотренном выше комплексе, где в качестве ТСЗИ используется узел ГЭМП, - отсутствует, что существенно снижает эффективность защиты автоматизированного рабочего места от НСДИ за счет побочных излучений и наводок, возникающих при эксплуатации АРМ.

Из-за отсутствия упомянутой ПОС эксплуатация данного АРМ может быть продолжена, даже при выключенных (вышедших из строя) технических средствах подавления/ маскировки ПЭМИН, что и создает угрозу НСДИ.

По мнению авторов, наиболее близким по технической сущности к заявленному объекту (**прототипом**) является, известное из техники [Л10], автоматизированное рабочее место (АРМ), состоящее из системного блока персональной электронно-вычислительной машины (СБ ПЭВМ), монитора, принтера, клавиатуры, манипулятора типа мышь (МТМ), USB ключа, сетевого фильтра (СФ), микроконтроллера (МК), коммутатора, генератора широкополосного электромагнитного поля (ГЭМП), широкополосного детектора электромагнитного поля (ДП), выход которого соединен с первым портом узла МК, который вторым портом соединен с первым портом коммутатора, который вторым и третьим портами соединен, соответственно, с USB ключом и первым портом узла СБ ПЭВМ, который со второго по пятый портами соединен, соответственно, с портом узла МТМ, с портом клавиатуры, с портом принтера, с портом монитора, который входом электропитания соединен с первым выходом узла СФ, который вторым выходом, третьим выходом и входом соединен, соответственно, со входом электропитания принтера, со входом электропитания узла СБ ПЭВМ и первым выходом блока электрических розеток (БЭР), который входом и

вторым выходом соединен, соответственно, с питающей электрической сетью (ПЭС) 220 В и входом электропитания узла ГЭМП, и выполненное с возможностью установки на СБ ПЭВМ программного обеспечения (ПО) в виде операционной системы (ОС), обеспечивающей управление функциями АРМ, формирование интерфейса пользователя АРМ, принтера, монитора и программного обеспечения доверенной загрузки ОС с использованием USB-ключа, и выполнения узла микроконтроллера с возможностью функционирования по программе, обеспечивающей возможность анализа и обработки сигналов, поступающих с узла ДП, и формирования управляющих сигналов, обеспечивающих блокировку доступа к интерфейсу пользователя СБ ПЭВМ и ресурсам АРМ.

Функциональная схема данного автоматизированного рабочего места (далее- комплекс), приведена на фиг.1.

Комплекс (фиг.1), состоит из системного блока персональной электронно-вычислительной машины (СБ ПЭВМ) 1, сетевого фильтра (СФ) 2, монитора 3, блока электрических розеток (БЭР) 4, принтера 6, генератора широкополосного электромагнитного поля (ГЭМП) 7, клавиатуры 8, манипулятора типа мышь (МТМ) 10, коммутатора 11, микроконтроллера (МК) 12, широкополосного детектора электромагнитного поля (ДП) 13, USB ключа 14. При этом, узел БЭР 4 своими входом, первым выходом и вторым выходом соединен, соответственно, с питающей силовой электросетью 220 В (ПЭС) 5, с узлом ГЭМП 7 и с узлом СФ 2, который первым, вторым и третьим выходами соединен, соответственно, со входом электропитания принтера 6, со входом электропитания монитора 3 и со входом электропитания узла СБ ПЭВМ 1, который первым, вторым, третьим, четвертым и пятым портами, соединен, соответственно, с портом монитора 3, с портом принтера 6, с портом клавиатуры 8, с портом узла МТМ 10 и с первым портом коммутатора 11, который вторым и третьим портами соединен, соответственно, с USB-ключом 14 и с последовательно соединенными узлами МК 12 и ДП 13.

Комплекс (фиг.1) функционирует следующим образом.

В исходном состоянии комплекс выключен. Для обеспечения возможности использования комплекса по назначению на узле СБ ПЭВМ 1 инсталлируется пакет программного обеспечения (ПО). При этом на СБ ПЭВМ 1 осуществляется установка операционной системы (ОС), обеспечивающей управление функциями программно-аппаратных средств комплекса, формирование интерфейса пользователя с предоставлением ему возможностей ввода и/или вывода информации с помощью клавиатуры 8, узла МТМ 10, монитора 3 и принтера 6, установки программного обеспечения, ориентированного для обработки информации, необходимой пользователю, установки программного обеспечения для защиты ОС и пользовательской информации от вирусов, установки программного обеспечения для шифрования данных и программного обеспечения для выполнения доверенной загрузки ОС с использованием USB-ключа 14. Также инсталлируются драйверы для работы аппаратных узлов комплекса (монитора 3, принтера 6 и др.) под управлением ОС, установленной на СБ ПЭВМ 1. После установки ПО, необходимого для функционирования комплекса, к нему может быть допущен персонал для использования комплекса по назначению.

Персоналу, допущенному для выполнения работ на комплексе, выдается идентификационный USB –ключ 14. Работа на комплексе начинается с того, что пользователем АРМ активируется (включается) узел ГЭМП 7, который в локальной зоне размещения аппаратных узлов комплекса формирует электромагнитное поле (ЭМП) 9, спектр которого перекрывает спектр излучений, которые образуются в процессе функционирования программно-аппаратных узлов комплекса.

ЭМП 9, созданное ГЭМП 7, принимается узлом ДП 13 и выполняет его широкополосную демодуляцию. При этом, ДП 13 настроен таким образом, что при наличии на его входе интенсивного ЭМП 9, на выходе ДП 13 формируется сигнал высокого уровня, который подается на узел МК 12. При

получении сигнала высокого уровня от ДП 13 узлом МК 12 осуществляется включения коммутатора 11. При включении коммутатора 11 осуществляется коммутация USB -ключа 14 к узлу СБ ПЭВМ 1.

После этого, пользователь включает СБ ПЭВМ 1. Происходит загрузка ОС, в процессе которой обеспечивается доверенная загрузка с аутентификацией пользователя по USB -ключу 14. Отсутствие USB -ключа 14 блокирует доступ к ОС.

Если по какой либо причине узел ГЭМП 7 будет деактивирован, то на вход узла ДП 13 перестанет поступать ЭМП 9. Это приведет к тому, что на выходе ДП 13 установится низкий уровень сигнала. При подаче низкого уровня сигнала на МК 12, на его выходе формируется сигнал выключения коммутатора 11. Это приведет к эмуляции отключения USB -ключа 14 от узла СБ ПЭВМ 1. В результате этого доступ к ОС, к программным, информационным и аппаратным ресурсам комплекса будет заблокирован.

После включения узла ГЭМП 7, работа улов ДП 13, МК 12, и коммутатора 11 осуществляется в порядке, описанном выше, в результате чего доступ к ОС комплекса– возобновляется.

Данный комплекс частично устраняет недостатки предыдущего АРМ. Это достигается за счет того, что в нем установлена ПОС - связь между доступом к операционной системе (ОС), установленной на СБ ПЭВМ 1 и наличием ЭМП 9, создаваемого при работе ГЭМП 7, который и обеспечивает необходимый уровень блокировки/ маскировки ПЭМИН, формируемых в процессе работы технических средств АРМ.

При реализации обратной связи между функциями АРМ и активностью ГЭМП 7 уровень защищенности информации от утечек по каналу ПЭМИН существенно повышается. Это достигается за счет того, что возможность выполнения работ персоналом на АРМ, определяемая их доступом к интерфейсу СБ ПЭВМ 1, становится зависимой от наличия ЭМП 9 и рабочего состояния ГЭМП 7, обеспечивающего подавление и/или маскировку ПЭМИН, создаваемых АРМ. Если ГЭМП 7 функционирует в

штатном режиме и ЭМП 9 – есть, то доступ к ресурсам АРМ (СБ ПЭВМ 1)– открыт, а если ЭМП 7 – отсутствует, из-за того что ГЭМП 7 по той или иной причине не функционирует, то доступ к ОС СБ ПЭВМ 1- блокируется. При этом, персонал не может продолжить эксплуатацию АРМ при деактивированном узле ГЭМП 7. То есть, последствия не регламентированных действий легитимного персонала, приведших к деактивации узла ГЭМП 7, частично устраняются.

Таким образом, в случаях деактивации (отключения, выхода из строя и т.п.) ГЭМП 7, обеспечивается ограничение доступа к ресурсам ОС и функциям АРМ до тех пор, пока ГЭМП 7 будет снова включен и в локальной зоне размещения АРМ будет сформировано ЭМП 9 для подавления/ маскировки ПЭМИН. Это способствует повышению уровня защиты информации от утечек по техническому каналу типа ПЭМИН, которые образуются при эксплуатации АРМ.

Недостатком данного комплекса-прототипа является низкий уровень защиты информации от утечек по техническому каналу типа ПЭМИН. Это обусловлено следующими факторами.

В АРМ- прототипе узел ДП 13 выполнен с возможностью приема и широкополосной демодуляции ЭМП 9, формируемого и излучаемого узлом ГЭМП 7. Это означает, что узел ДП 13 может детектировать радиосигналы, которые распределены по диапазону частот в широкой полосе. Такое свойство обеспечивает прием всех сигналов, которые поступают из радиоэфира на вход ДП 13. Из [Л11- Л13] известно, что радиодиапазон насыщен сигналами от множества источников, в том числе, от средств радиосвязи, вещательных радиостанций, излучений от промышленных объектов, автотранспорта и бытовых приборов и др. Сигналы, созданные всеми этими объектами, также могут поступать на вход ДП 13 и вызывать его ложное срабатывание при отсутствии активности узла ГЭМП 7. То есть, если узел ГЭМП 7 будет по тем или иным причинам деактивирован, например, выйдет из строя или не отключен персоналом, эксплуатирующим

АРМ, то поступающие на вход узла ДП 13 радиосигналы от посторонних (относительно узла ГЭМП 7) источников излучения могут быть восприняты в качестве ЭМП 9, в то время, когда они таковыми не являются. Это приводит к опасной, с точки зрения утечки информации с АРМ, ситуации, которую условно можно назвать «пропуск тревог».

Установлено, что эти «пропуски тревог» обусловлены тем, что в данном техническом решении, для идентификации активности ТСЗИ (ГЭМП 7), предназначенного для подавления/ маскировки ПЭМИН, используется признак с низкой информативностью, что не обеспечивает получение достоверных данных, необходимых для реализации надежного контроля активности ГЭМП 7.

При функционировании АРМ образуются побочные электромагнитные излучения, спектр которых распределен в широком диапазоне радиочастот, поэтому для их маскировки узел ГЭМП 7 выполнен с возможностью формирования шумового радиосигнала со спектром, перекрывающим спектр в котором могут быть созданы ПЭМИН. Для приема и обработки сигналов, формируемых ГЭМП 7, то есть реагирования на ЭМП 9, радиоприемник узла ДП 13 тоже выполнен широкополосным. Это приводит к тому, что в широкополосный тракт узла ДП 13 будут попадать излучения от множества посторонних источников радиоизлучений (ИРИ), которыми интенсивно насыщен эфир. То есть, узлом ДП 13 будут приниматься радиосигналы от бытовых радио и телевизионных передатчиков, передатчики от систем радиорелейной и сотовой связи и др. В результате этого, сигналы от упомянутых посторонних ИРИ будут восприниматься как ЭМП 9, создаваемое ГЭМП 7, в то время как сам ГЭМП 7 может быть выключен или выведенным из строя по тем или иным причинам, в том числе по вине персонала, эксплуатирующего АРМ.

В данном комплексе (прототипе), в случаях деактивации узла ГЭМП 7, узлом ДП 13 могут приниматься сигналы посторонних ИРИ, на основе которых будет ложно идентифицироваться наличие активности ГЭМП 7,

поэтому возможность использования АРМ по назначению при деактивированном узле ГЭМП 7, то есть без маскировки/ подавления ПЭМИН, создаваемых АРМ, - сохраняется, что существенно снижает эффективность защиты информации от утечек по техническому каналу типа ПЭМИН.

Исследования показали, что низкая надежность идентификации активности узла ГЭМП 7, в данном техническом решении обусловлена использованием для принятия соответствующего решения (что узел ГЭМП 7 - активен) признаков с низкой информативностью. По сути, узел ДП 13 не обладает свойствами, позволяющими надежно идентифицировать сигналы создаваемые узлом ГЭМП 7. Поэтому, формируемая в техническом решении прототипа обратная связи между функциями АРМ и активностью ГЭМП 7 – является слабой и не устойчивой, что существенно снижает надежность защиты информации, содержащейся в АРМ, от ее утечек по техническому каналу типа ПЭМИН.

Следует заметить, что усилить упомянутую ПОС только лишь с использованием признаков и свойств АРМ- прототипа не представляется возможным, так как надежная идентификация ЭМП 9, создаваемого узла ГЭМП 7 – не обеспечивается. Это обусловлено тем, что ЭМП 9 и сигнал от посторонних ИРИ - находятся в одной полосе радиочастот, а мощность узла ГЭМП 7 - ограничена соответствующими стандартами и распределена («размазана») по широкому диапазону, поэтому, в полосе приема узла ДП 13 могут присутствовать сосредоточенные помехи от посторонних ИРИ с уровнем мощности, превышающим интенсивность сигналов ЭМП 9. То есть, ни по частоте, ни по мощности надежная идентификация сигналов, создаваемых узлом ГЭМП 7 - не может быть реализована с использованием признаков и свойств, присущих комплексу - прототипу.

Упомянутая ПОС, то есть, связь между активностью ГЭМП 7 и доступом к ресурсам АРМ в комплексе- прототипе имеет низкую надежность из-за действия субъективных факторов (нерегламентированных действий

легитимного персонала) и объективных факторов (эфирных ЭМП). В данном комплексе, при выходе из строя ТСЗИ (ГЭМП 7), а также при нерегламентированных действиях персонала, повлекших деактивацию узла ГЭМП 7, АРМ может функционировать без наличия ЭМП 9 из-за наличия в эфире достаточного количества посторонних ИРИ, излучения которых могут приводить к образованию ситуаций типа «пропуски тревог», при которых деактивация узла ГЭМП 7 не вызывает блокировки функций АРМ и функционирование (эксплуатация) которого может продолжаться без подавления/ маскировки канала ПЭМИН, по которому возможна утечка информации, циркулирующей на АРМ.

Для повышения уровня защиты информации, содержащейся и циркулирующей в автоматизированном рабочем месте (АРМ), от несанкционированного доступа (НСД) к ней методом перехвата и анализа побочных электромагнитных излучений и наводок, возникающих в процессе эксплуатации автоматизированного рабочего места, авторами предложено значительно усилить упомянутую ПОС между функциями доступа к АРМ и активностью технических средств активной защиты типа ГЭМП 7. Это позволит устранить ситуации типа «ложных пропусков» и обеспечить гарантированное функционирования АРМ с постоянно действующим техническим средством активной защиты информации, содержащейся и циркулирующей в АРМ, от ее утечек по техническому каналу типа ПЭМИН.

Целью полезной модели является расширение функциональных возможностей автоматизированного рабочего места (АРМ) по контролю активности технических средств защиты информации от утечек по техническому каналу типа ПЭМИН, которые образуются при функционировании упомянутого АРМ.

Поставленная цель достигается за счет того, что в известное автоматизированное рабочее место (АРМ), состоящее из системного блока персональной электронно-вычислительной машины (СБ ПЭВМ), монитора, принтера, клавиатуры, манипулятора типа мышь (МТМ), сетевого фильтра (СФ), блока электрических розеток (БЭР), USB ключа, микроконтроллера (МК), коммутатора, генератора широкополосного электромагнитного поля (ГЭМП), широкополосного детектора электромагнитного поля (ДП), который выполнен с возможностью приема и широкополосной демодуляции радиосигналов и выход которого соединен с первым портом узла МК, который вторым портом соединен с первым портом коммутатора, который вторым и третьим портами соединен, соответственно, с USB ключом и первым портом узла СБ ПЭВМ, который со второго по пятый портами соединен, соответственно, с портом узла МТМ, с портом клавиатуры, с портом принтера и с портом монитора, который входом электропитания соединен с первым выходом узла СФ, который вторым выходом, третьим выходом и входом соединен, соответственно, со входом электропитания принтера, со входом электропитания узла СБ ПЭВМ и первым выходом блока электрических розеток (БЭР), который входом соединен с питающей электрической сетью (ПЭС) 220 В, и выполненное с возможностью установки на СБ ПЭВМ программного обеспечения (ПО) в виде операционной системы (ОС), обеспечивающей формирование интерфейса пользователя АРМ для управления функциями АРМ, программно-аппаратных средств доверенной загрузки ОС на узле СБ ПЭВМ, функционирования узла микроконтроллера по программе, обеспечивающей возможность обработки сигналов, поступающих с узла ДП и формирования сигналов блокировки доступа к интерфейсу пользователя узла СБ ПЭВМ, **дополнительно введен** датчик тока (ДТ), который входом, первым и вторым выходами соединен, соответственно, со вторым выходом узла БЭР, входом узла ГЭМП и третьим портом узла МК, при этом, узел ДТ выполнен с возможностью измерения тока, протекающего в цепи электропитания узла

ГЭМП, узел МК выполнен с возможностью функционирования по программе, обеспечивающей многоканальный приема и комплексную обработку сигналов, одновременно поступающих от узлов ДТ и ДП, с распознаванием (идентификацией) активности узла ГЭМП по уровню потребляемой им мощности и наличию излучаемого им электромагнитного поля, синтез устойчивой к воздействию внешних факторов обратной связи в виде функциональной зависимости между режимами работы программно-аппаратных средств доверенной загрузки операционной системы узла СБ ПЭВМ и активностью узла ГЭМП, формирование сигналов управления доступом к функциям АРМ, путем эмуляции подключения или отключения USB- ключа от узла СБ ПЭВМ, с использованием результатов упомянутой идентификации наличия или отсутствия активности узла ГЭМП.

В предлагаемом техническом решении обеспечивается следующее сочетание отличительных признаков и свойств.

Это- введение в состав АРМ датчик тока (ДТ), который входом, первым и вторым выходами соединен, соответственно, со вторым выходом узла БЭР, входом узла ГЭМП и третьим портом узла МК. При этом, узел ДТ выполнен с возможностью измерения тока, протекающего в цепи электропитания узла ГЭМП, что позволяет диагностировать работоспособность изделия. Введение этих признаков и использования новых свойств обеспечивает существенное повышение надежности контроля активности (режимов работы) узла ГЭМП.

Это- функционирование узла МК по программе, обеспечивающей возможность многоканального приема и комплексной обработки сигналов, одновременно поступающих от узлов ДТ и ДП, с распознаванием (идентификацией) активности узла ГЭМП по уровню потребляемой им мощности и наличию излучаемого им электромагнитного поля.

Это- синтез устойчивой к воздействию внешних факторов обратной связи в виде функциональной зависимости между режимами работы программно-

аппаратных средств доверенной загрузки операционной системы узла СБ ПЭВМ и активностью узла ГЭМП.

Это- формирование сигналов управления доступом к функциям АРМ, путем эмуляции подключения или отключения USB- ключа от узла СБ ПЭВМ, с использованием результатов упомянутой идентификации наличия или отсутствия активности узла ГЭМП.

Использование новых признаков и свойств позволяет полностью устранить ситуации, соответствующие «пропуску тревог», так как идентификация активности узла ГЭМП осуществляется с использованием двух надежных признаков (факторов): наличию ЭМП, создаваемого узлом ГЭМП, и уровню тока, потребляемого этим узлом. Двухфакторная идентификация активности узла ГЭМП позволяет организовать устойчивую к воздействию различных факторов обратную связь между активностью технического средства защиты информации от утечек по ПЭМИН и доступом к системным и информационным ресурсам АРМ.

Наличие указанных признаков позволяет реализовать новые свойства, которые существенным образом влияют на достижение поставленной цели.

Наличие и использование всех, указанных выше признаков и свойств позволяет существенным образом усилить упомянутую обратную связь между доступом к функциям АРМ и активностью ТС АЗ (узел ГЭМП), что обеспечивает возможность эксплуатации АРМ только лишь в режиме с маскированным и/или подавленным техническим каналом (ПЭМИН) утечки информации.

Сочетание отличительных признаков и свойств, предлагаемого автоматизированного рабочего места с защитой информации от утечек по каналу ПЭМИН, из техники неизвестно, поэтому оно соответствует критерию **новизны.** При этом, для достижения максимального эффекта по расширению функциональных возможностей автоматизированного рабочего места (АРМ) по контролю активности технических средств защиты

информации от утечек по техническому каналу типа ПЭМИН, которые образуются при функционировании упомянутого АРМ, необходимо использовать всю совокупность отличительных признаков и свойств, указанных выше.

На фиг.2 приведена функциональная схема автоматизированного рабочего места с защитой информации от утечек по каналу ПЭМИН (далее-комплекс).

Комплекс (фиг.2), состоит из системного блока персональной электронно-вычислительной машины (СБ ПЭВМ) 1, сетевого фильтра (СФ) 2, монитора 3, блока электрических розеток (БЭР) 4, принтера 6, клавиатуры 7, генератора широкополосного электромагнитного поля (ГЭМП) 8, датчика тока (ДТ) 9, манипулятора типа мышь (МТМ) 10, USB ключа 12, широкополосного детектора электромагнитного поля (ДП) 13, коммутатора 14 и микроконтроллера (МК) 15. При этом, узел БЭР 4 своими входом, первым выходом и вторым выходом соединен, соответственно, с питающей силовой электросетью 220 В (ПЭС) 5, с первым портом узла ДТ 9 и с узлом СФ 2, который первым, вторым и третьим выходами соединен, соответственно, со входом электропитания монитора 3, со входом электропитания принтера 6, и со входом электропитания узла СБ ПЭВМ 1, который своими пятью портами, соединен, соответственно, с портом монитора 3, с портом принтера 6, с портом клавиатуры 7, с портом узла МТМ 10 и с первым портом коммутатора 14, который вторым и третьим портами соединен, соответственно, с USB-ключом 12 и с первым портом узла МК 15, который вторым и третьим портами соединен, соответственно, с выходом узла ДП 13 и вторым портом узла ДТ 9, который третьим портом соединен с узлом ГЭМП 8, который выполнен с возможностью формирования широкополосного электромагнитного поля (ЭМП 11). Кроме того, узел ДП 13, выполнен с возможностью приема и широкополосной демодуляции радиосигналов, узел ДТ 9 выполнен с возможностью измерения

величины тока, потребляемого узлом ГЭМП 8 от узла БЭР 4, узел СБ ПЭВМ 1 выполнен с возможностью установки и функционирования на нем программного обеспечения (ПО) в виде операционной системы (ОС), обеспечивающей формирование интерфейса пользователя АРМ для управления функциями АРМ, программно-аппаратных средств доверенной загрузки операционной системы. При этом, узел МК 15 функционирует по программе, обеспечивающей возможность одновременного приема и комплексной обработки сигналов, поступающих от узла ДТ 9 и данных, поступающих от узла ДП 13 с распознаванием (идентификацией) активности узла ГЭМП 8 по одновременному наличию излучаемого им ЭМП 11 и уровню потребляемого им тока, синтеза устойчивой к воздействию внешних факторов обратной связи в виде функциональной зависимости между процедурой доверенной загрузки операционной системы узла СБ ПЭВМ 1 и активностью узла ГЭМП 8 для контроля и управления доступом к функциям АРМ с использованием результатов упомянутой идентификации наличия или отсутствия активности узла ГЭМП 8 путем эмуляции, соответственно, подключения или отключения USB- ключа 12 к узлу СБ ПЭВМ 1.

Комплекс (фиг.2) функционирует следующим образом.

В исходном состоянии комплекс выключен. Для обеспечения возможности использования комплекса по назначению на узле СБ ПЭВМ 1 инсталлируется пакет программного обеспечения (ПО). При этом на СБ ПЭВМ 1 осуществляется установка операционной системы (ОС), обеспечивающей управление функциями программно-аппаратных средств комплекса, формирование интерфейса пользователя с предоставлением ему возможностей ввода и/или вывода информации с помощью клавиатуры 7, узла МТМ 10, монитора 3 и принтера 6, установки программного обеспечения, ориентированного для обработки информации, необходимой пользователю, установки программного обеспечения для защиты ОС и пользовательской информации от вирусов, установки программного

обеспечения для шифрования данных и программного обеспечения для выполнения доверенной загрузки ОС с использованием USB-ключа 12. Также инсталлируются драйверы для работы аппаратных узлов комплекса (монитора 3, принтера 6 и др.) под управлением ОС, установленной на СБ ПЭВМ 1. После установки ПО, необходимого для функционирования комплекса, к нему может быть допущен персонал для использования комплекса по назначению.

Работа на комплексе начинается с того, что активируется (включается) узел ГЭМП 8, который в локальной зоне размещения аппаратных узлов комплекса формирует ЭМП 11 для маскировки/ подавления ПЭМИН, которые образуются в процессе функционирования программно-аппаратных узлов комплекса.

ЭМП 11 принимается узлом ДП 13, который выполняет его широкополосную демодуляцию. ДП 13 настроен таким образом, что при наличии на его входе интенсивного ЭМП 11, на выходе ДП 13 формируется сигнал высокого уровня, который подается на первый порт узла МК 15.

При включении узла ГЭМП 8 в цепи его электропитания протекает ток, который фиксируется узлом ДТ 9. Так как ДТ 9 выполнен с возможностью измерения величины тока, потребляемого узлом ГЭМП 8 от узла БЭР 4, то данные, полученные от узла ДТ 9 постоянно подаются на узел МК 15. В простейшем случае, логика работы узла ДТ 9 может быть основана на контроле уровня тока, потребляемого узлом ГЭМП 8. Например, путем формирования на выходе узла ДТ 9 логической единицы (высокого уровня напряжения), при превышении тока, потребляемого узлом ГЭМП 8, заданного порогового значения и формирования на выходе узла ДТ 9 логического нуля (низкого уровня напряжения), при уровне тока, потребляемого узлом ГЭМП 8, ниже установленного порога. Сигнал с узла ДТ 9 подается на второй порт узла МК 15. При одновременном получении высоких уровней сигналов от узлов ДП 13 и ДТ 9, узлом МК 15

осуществляется включения коммутатора 14. При включении коммутатора 14 выполняется коммутация USB -ключа 12 к порту узла СБ ПЭВМ 1.

Когда сигналы, поступающие с узлов ДП 13 и ДТ 9, имеют уровень, соответствующий логической единице, то доступ к функциям комплекса – открыт. Персонал, допущенный к АРМ, может использовать комплекс по назначению. Доверенная загрузка ОС на СБ ПЭВМ 1 с аутентификацией пользователя по USB -ключу 12 – обеспечивается.

Если по какой либо причине узел ГЭМП 8 будет деактивирован, то на вход узла ДП 13 перестанет поступать ЭМП 11 и ток, потребляемый узлом ГЭМП 8, существенно снизится или прекратится совсем. В результате этого, на выходе узлов ДП 13 и ДТ 9 появятся сигналы, соответствующие логическому нулю. При наличии в локальной зоне размещения комплекса интенсивных радиоизлучений от посторонних ИРИ, они могут детектироваться узлом ДП 13 и приводить к формированию на его выходе уровня, соответствующего логической единице. Для нейтрализации влияния внешних факторов, узел МК 15 вырабатывает сигналы, соответствующие эмуляции подключения USB -ключа 12 к порту узла СБ ПЭВМ 1, только при одновременном наличии сигналов логической единицы на выходах узлов ДП 13 и ДТ 9.

После активации узла ГЭМП 8, комплекс возвращается в рабочее состояние и доступ к системным и информационным ресурсам комплекса – возобновляется.

Таким образом, узлом МК 15 обеспечивается одновременный прием и комплексная обработка сигналов, поступающих от узла ДТ 9 и данных, поступающих от узла ДП 13. Это позволяет надежно распознавать (идентифицировать) активность узла ГЭМП 8 по одновременному наличию излучаемого им ЭМП 11 и уровню потребляемого им тока. Это также обеспечивает формирование устойчивой функциональной зависимости между процедурой доверенной загрузки операционной системы узла СБ ПЭВМ 1 и активностью узла ГЭМП 8. Наличие устойчивой к воздействию

внешних факторов обратной связи между доступом к функциям комплекса и активностью узла ГЭМП 8 обеспечивает надежный контроль и управление доступом к функциям комплекса с использованием результатов упомянутой идентификации наличия или отсутствия активности узла ГЭМП 8 путем эмуляции подключения или отключения USB- ключа 12 к порту узла СБ ПЭВМ 1.

Техническим результатом, достигаемым при реализации данной полезной модели, является повышение надежности идентификации активности узла ГЭМП 8, что достигается за счет увеличения количества и информативности используемых признаков, снижение вероятности утечки информации по техническому каналу типа ПЭМИН, что достигается за счет сокращения времени эксплуатации комплекса в не защищенном режиме - при деактивированном (выключенном) узле ГЭМП 8 и повышение устойчивости к воздействию внешних факторов обратной связи между доступом к функциям комплекса и активностью узла ГЭМП 8, что достигается за счет непосредственного контроля (измерения) его рабочих электрических параметров.

При реализации комплекса, его алгоритм функционирования может быть представлен в следующем виде:

– Начало;

– Запуск операционной системы на СБ ПЭВМ 1;

– Проверка-1: сигнал логической единицы с выхода узла ДП 13 – есть? Если нет, то возврат, если – Да, то переход к проверке -2;

– Проверка-2: сигнал логической единицы с выхода узла ДТ 9 – есть? Если нет, то возврат, если – Да, то продолжение;

– Запуск пользовательской программной среды, выполнение работ на АРМ;

– Проверка-3: сигнал логической единицы с выхода узла ДП 13 – есть? Если нет, то блокировка доступа к интерфейсу пользователя, запрос авторизации пользователя. Если – Да, то переход к проверке -4;

– Проверка-4: сигнал логической единицы с выхода узла ДТ 9 – есть? Если нет, то блокировка доступа к интерфейсу пользователя, запрос авторизации пользователя. Если – Да, то продолжение;

– Завершение работы: выключение СБ ПЭВМ 1, отключение USB- ключа 12, выключение ГЭМП 8;

– Конец.

Узлы СБ ПЭВМ 1, СФ 2, монитора 3, БЭР 4, принтера 6, клавиатуры 7, ГЭМП 8, МТМ 10, USB- ключа 12, широкополосного детектора электромагнитного поля 13, коммутатора 14 и МК 15, могут быть аналогичными соответствующим признакам и свойствам АРМ- прототипа и не требуют доработки при их реализации.

Узел ДТ 9 может быть может быть реализован на датчиках тока открытого типа фирмы Honeywell, которые построены на базе интегрированных линейных датчиков Холла типа 91SS12-2 и SS94A1 [Л14], обладающих повышенной температурной стабильностью и линейностью характеристики. Эти датчики имеют аналоговый выход, напряжение на котором прямо пропорционально величине тока, протекающего через контролируемый проводник. При этом, дополнительная регулировка чувствительности производится путем увеличения числа витков проводника с током вокруг кольца магнитопровода датчика. Альтернативным вариантом реализации узла ДТ 9 является использование компенсационных датчиков тока, например, модели CSNE151, CSNE381 [Л14], которые позволяют бесконтактным способом измерять постоянный, переменный и импульсный токи в широком диапазоне их значений (до ±1200 А). Эти датчики преобразуют токовый выход в напряжение, имеют регулировку чувствительности, которая также осуществляется путем увеличения числа витков проводника вокруг кольца магнитопровода датчика или установкой перемычек, задающих число витков внутренней компенсационной катушки датчика.

При реализации узлов данного комплекса могут быть также использованы технологические, конструктивные и программно-аппаратные решения, известные из [Л15- Л21].

Как показано, предлагаемое техническое решение позволяет успешно решить поставленную задачу по повышению уровня защиты информации, содержащейся и циркулирующей в автоматизированном рабочем месте, от несанкционированного доступа к ней методом перехвата и анализа побочных электромагнитных излучений и наводок, возникающих в процессе эксплуатации упомянутого автоматизированного рабочего места. При этом эффективное решение упомянутой задачи обеспечивается на основе расширения функциональных возможностей автоматизированного рабочего места (АРМ) по контролю активности технических средств защиты информации от утечек по техническому каналу типа ПЭМИН, которые образуются при функционировании упомянутого АРМ, а также использованию достигаемого технического результата. Следует отметить, что благодаря использованию данного технического решения риски утечек информации, обусловленные нерегламентированными действиями персонала, при которых работа комплекса может осуществляться при деактивированных средствах активной защиты комплекса (узла ГЭМП 8), полностью устраняются. То есть, при деактивации узла ГЭПМ 8 - доступ к функциям АРМ – блокируется.

Приведенные средства, с помощью которых возможно осуществление полезной модели, позволяют обеспечить ее **промышленную применимость.**

Основные узлы комплекса экспериментально проверены и могут быть положены в основу создания образцов комплексов, обеспечивающих эффективную защиту информации от несанкционированного доступа со стороны ПФЛ, который может быть организован на основе перехвата и анализа ПЭМИН, излучаемых в процессе эксплуатации комплекса.

Разработанное авторами техническое решение и получаемый с помощью его технических результат, предоставляет возможность значительного повышения уровня защиты информации, содержащейся и циркулирующей в автоматизированном рабочем месте, от несанкционированного доступа по техническому каналу типа ПЭМИН, возникающему при эксплуатации комплекса, маскировка и/или подавление которого может нарушаться при деактивации технических средств активной защиты типа широкополосного генератора электромагнитного поля, в том числе, в результате нарушения правил эксплуатации комплекса и/или иных нерегламентированных действий персонала, эксплуатирующего данный комплекс, а также случайных воздействий внешней среды, например, действия эфирных электромагнитных полей.

Автоматизированное рабочее место с защитой информации от утечек по каналу ПЭМИН будет востребовано широким кругом потребителей, использующих вычислительную технику для обработки конфиденциальной информации, нуждающейся в защите от утечек, которые могут быть вызваны деактивацией технических средств маскировки и/или подавления канала типа ПЭМИН, который возникает в процессе эксплуатации АРМ.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Автоматизированное рабочее место, http://ru.wikipedia.org/wiki/
2. ГОСТ Р 51275-99 Защита информации. http://www.centre- expert.ru /index.php/ infosec/
3. Угрозы информационной безопасности, http://www.bre.ru/security/
4. Технический канал утечки информации. Терминология в области защиты информации. http://www.centre-expert.ru/index.php /infosec/
5. Исследования побочных электромагнитных излучений технических средств, http://www.pemi.ru/
6. Защита компьютерной информации от утечки по ПЭМИН, http://www.support17.com/component/content/39.html?task=view
7. Скрытая утечка информации. Компьютерная стеганография и ПЭМИН – вирус, http://www.cio-world.ru/bsolutions/e-safety/28763/page2.html
8. Автоматизированное рабочее место обмена закрытой документальной информацией, полезная модель № 80040, дата публикации: 20.01.2009г.
9. Доверенная загрузка, http://ru.wikipedia.org/wiki/
10. ФГУП «18 ЦНИИ» МО РФ, Патент на полезную модель «Автоматизированное рабочее место с защитой от несанкционированного доступа», зарегистрирован за № 96435 от 27.07.2010г., авторы: Галах В.П., Лакеев В.А., Егоров В.И., Хотячук В.К., Шкирин В.Г.
11. Электромагнитное излучение, http://ru.wikipedia.org/wiki/%D0%
12. Источники электромагнитных помех, http://www.obzor-electro.ru/publ/ehl_magnitnaja_sovmestimost/istochniki_ehlektromagnitnykh_pomekh/9-1-0-53
13. Электромагнитные помехи и их классификация, http://www.vxi.su/praktikum/elektromagnitnye-pomehi/
14. Датчики тока на эффекте Холла, http://news.cxem.net/articles/circuit_268.php

15. Полезная модель «Накопитель с контролем местоположения», Патент на полезную модель № 90233 от 27.12.2009г. авторы: Баталов А.В., Хотячук В.К., Хотячук К.М., Тимошкин В.С.

16. ФГУП «18 ЦНИИ» МО РФ, программа для ЭВМ «Менеджер сенсора», Свидетельство о государственной регистрации в ФИПС РФ № 2009610444 от 19.01.2009г., авторы: Хотячук В.К., Хотячук К.М. и др.

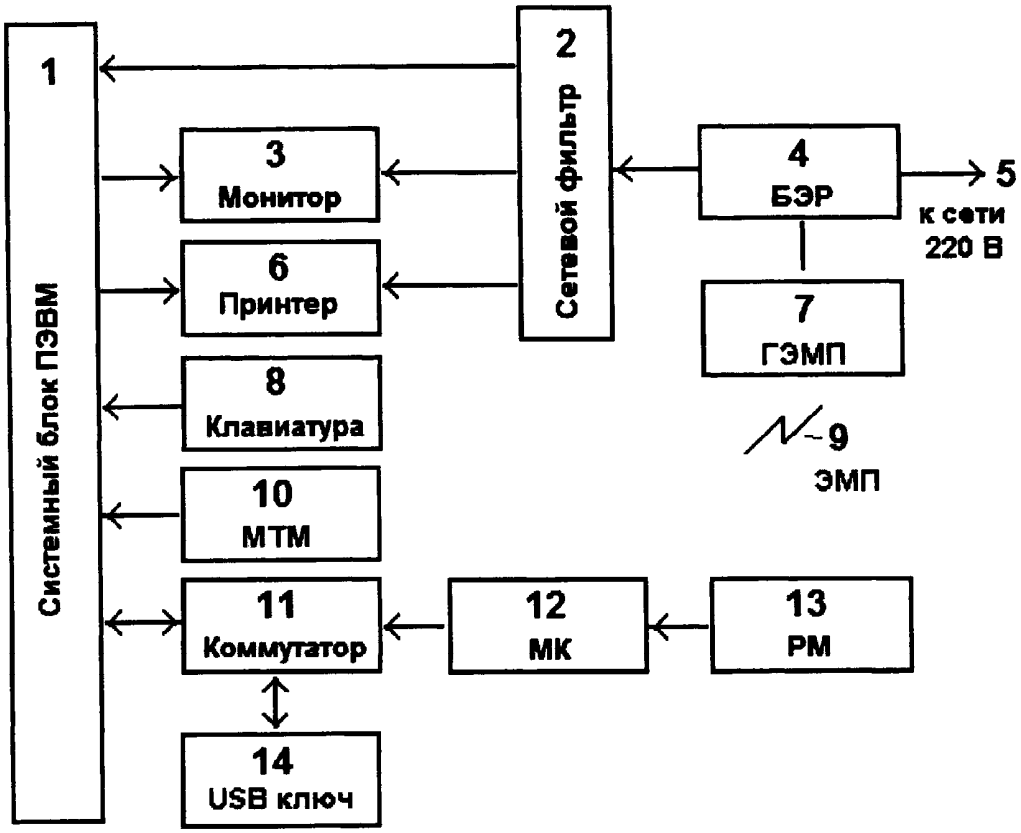
17. ФГУП «18 ЦНИИ» МО РФ, Программа для ЭВМ «Контроллер приемопередатчика», Свидетельство о государственной регистрации в ФИПС РФ № 2009610445 от 19.01.2009 г., авторы: Бакунин И.Б., Хотячук В.К., Хотячук К.М., Гончаров В.С.

18. ФГУП «18 ЦНИИ» МО РФ, Программа для ЭВМ «Монитор коммуникационного оборудования», Свидетельство о государственной регистрации в ФИПС РФ № 2009611020 от 16.02.2009 г., авторы: Васин М.С., Шелестов М.Е., Хотячук В.К.

19. ФГУП «18 ЦНИИ» МО РФ, Полезная модель «Защищенный накопитель», Патент на полезную модель № 87276 от 29.05.2009г. авторы: Хотячук В.К., Хотячук К.М., Тимошкин В.С., Покормяк Л.В.

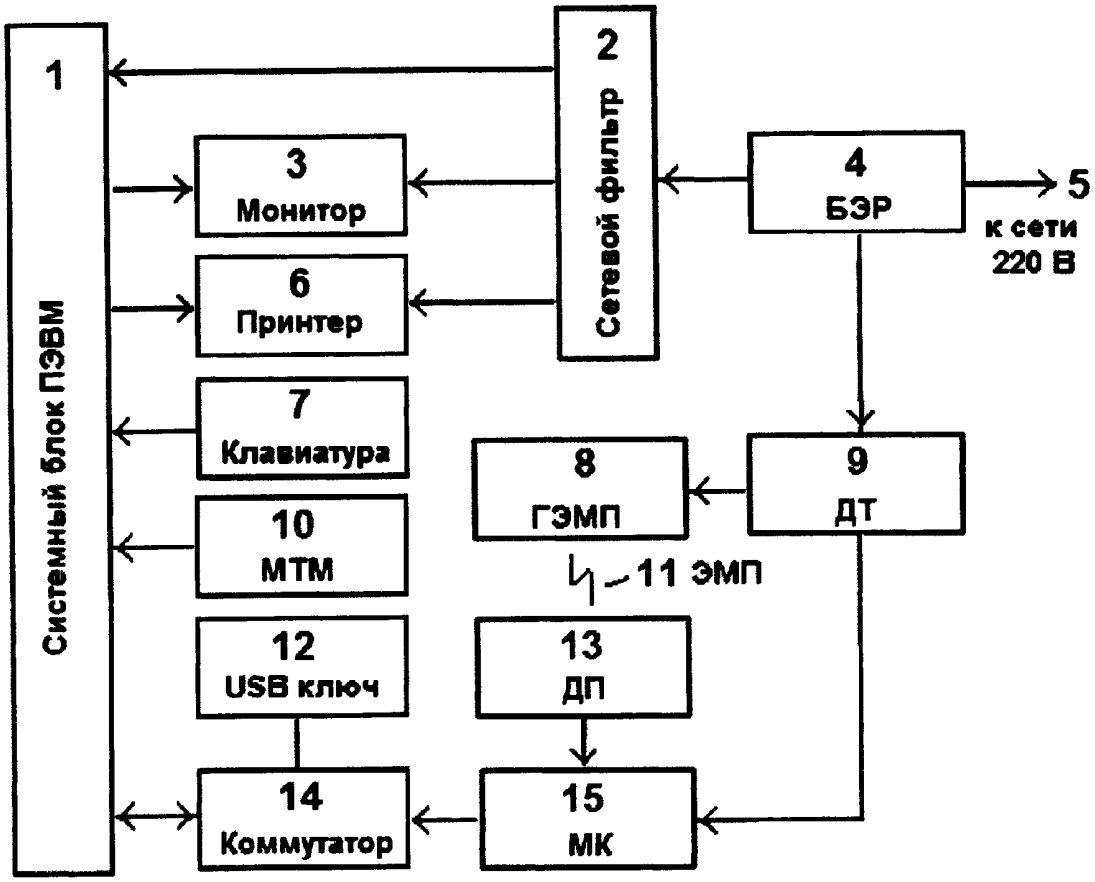
20. ФГУП «18 ЦНИИ» МО РФ, Полезная модель «Накопитель с защитой от несанкционированного доступа к памяти», Патент на полезную модель № 84594 от 10.07.2009г., авторы: Вдовин Е.И, Хотячук К.М., Хотячук В.К.

21. ФГУП «18 ЦНИИ» МО РФ, Полезная модель «Скрытый регистратор доступа на объект», Патент на полезную модель № 86026 от 20.08.2009г. авторы: Бугаенко О.В., Хотячук В.К., Хотячук К.М., Тимошкин В.С.


1
Системный блок ПЭВМ
2
Сетевой фильтр
3
Монитор
4
БЭР
5
к сети
220 В
6
Принтер
7
ГЭМП
8
Клавиатура
9
ЭМП
10
МТМ
11
Коммутатор
12
МК
13
РМ
14
USB ключ

Фиг.1

Автоматизированное рабочее место с защитой информации от утечек по каналу ПЭМИН



Фиг.2