



УКРАЇНА

(19) UA (11) 41413 (13) C2

(51) 7 E05B47/06

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ПАТЕНТУ НА ВІНАХІД

(54) ЕЛЕКТРОННА СИСТЕМА ДЛЯ КОНТРОЛЮ ДОСТУПУ ТА ДЛЯ ЗАХИСТУ

(21) 97030964

(22) 04.03.1997

(24) 17.09.2001

(31) 19609319.8

(32) 09.03.1996

(33) DE

(46) 17.09.2001, Бюл. № 8, 2001 р.

(72) Крафт Вольфганг, DE, Кортланд Андрієс, NL

(73) КРОНЕ ГМБХ, DE

(56) DE, № 4302835, М. кл. E05B47/06, H02B1/50, G08B21/00, 1994

(57) 1. Электронная система для контроля доступа и для защиты от несанкционированного открывания защищенных объектов, в частности коммутационных и распределительных шкафов в аппаратуре связи и обработки, передачи и приема данных, содержащая центральный блок регистрации данных, компьютеризированный центральный блок обработки данных, блок дальней передачи данных через линию связи и линию данных, а также средство связи для идентификационного контроля и разрешения на доступ, **отличающаяся** тем, что в пределах многоступенчатой иерархии центральный контрольный блок (CCU), по меньшей мере, через один децентрализованный мультиплексор (DCM) связи соединен, по меньшей мере, с одним локальным процессором (LDP) обработки данных, причем децентрализованный мультиплексор (DCM) связи и локальный процессор (LDP) обработки данных образованы полуавтономными блоками, а локальный процессор (LDP) обработки данных установлен в каждом защищаемом объекте, при этом между защищаемым объектом и центральным контрольным блоком (CCU) происходит постоянно актуализированный обмен данными с использованием динамического протокола о состоянии объекта, попытках доступа и т.п., электроснабжение локального процессора (LDP) обработки данных и связь происходят через один и тот же двужильный провод.

2. Система по п. 1, **отличающаяся** тем, что в и/или на объекте установлены различные датчики для контроля за общим состоянием объекта, информация которых независимо обрабатывается в локальном процессоре (LDP) обработки данных и передается в виде конкретного сообщения через децентрализованный мультиплексор (DCM) связи к центральному контрольному блоку (CCU).

3. Система по п. 1, **отличающаяся** тем, что каждый локальный процессор (LDP) обработки данных расположен на внутренней стороне двери объекта, снабжен собственным электронным замком и соединен с механическим запорным устройством.

4. Система по любому из пп. 1-3, **отличающаяся** тем, что электроснабжение обеспечивает электронное запирающее устройство двери объекта, при этом при перебое в электроснабжении гарантирован доступ имеющему на это разрешение лицу.

5. Система по п. 3, **отличающаяся** тем, что для управления доступом к объекту в локальном процессоре (LDP) обработки данных расположено считывающее устройство приближения в виде идентификационной системы, которое проверяет средство идентификации, находящееся снаружи.

6. Система по любому из пп. 1-5, **отличающаяся** тем, что использован однажды заданный идентификационный номер.

7. Система по любому из пп. 1-6, **отличающаяся** тем, что разрешение на доступ (выдача ключа) ограничено по времени.

8. Система по любому из пп. 1-7, **отличающаяся** тем, что через локальный процессор (LDP) обработки данных присоединены дополнительные датчики для сигнализации о пожаре, для измерения температуры и/или влажности и т.п.

9. Система по любому из пп. 1-8, **отличающаяся** тем, что через подходящие интерфейсы предусмотрена связь с отведенными пользователям сетями.

Изобретение относится к электронной системе для контроля доступа и для защиты от несанкционированного открывания закрытых объектов, в частности коммутационных и распределительных шкафов в технике связи и обработки, передачи и приема данных, содержащей центральный блок

регистрации данных, компьютеризированный центральный блок обработки данных, блок дальней передачи данных через линию связи и линию данных, а также средство связи для идентификационного контроля и разрешения на доступ.

(19) UA (11) 41413 (13) C2

Защита линий дальней связи от несанкционированного использования приобретает все большее значение с тем, чтобы воспрепятствовать прослушиванию частных и коммерческих линий, ведению телефонных разговоров за чужой счет, манипулированию данными, а также затруднить преднамеренное нарушение линий.

В патенте ФРГ № 4302835 С1 описано механическое запорное устройство для двери корпуса, в частности, кабельного распределительного шкафа в технике связи и обработки, передачи и приема данных, у которого блокировочный механизм снабжен двумя исполнительными ступенями для задвижки. После перемещения задвижки на ее первую исполнительную ступень открывается отверстие. Имеющее разрешение лицо получает через это отверстие в двери доступ к штепсельным гнездам или устройству для считывания магнитных карт и т.п. и может подключить средство связи, через которое может вступить в контакт с центральным постом управления, открывающим за счет дистанционной передачи вторую исполнительную ступень. Обмен информацией между центральным постом и имеющим разрешение лицом на кабельном распределительном шкафу служит для идентификационного контроля.

С помощью этого известного запорного устройства существенно повышается защита от несанкционированного манипулирования, однако, не обеспечивается постоянное актуальное наблюдение за состоянием всего кабельного распределительного шкафа и желаемыми доступа лицами.

В основе изобретения стоит задача разработки родовой электронной системы для контроля доступа и для защиты, которая повышает надежность от несанкционированного открывания и обеспечивает всегда актуальную информацию о состоянии защищаемого объекта.

Эта задача решается посредством того, что в пределах многоступенчатой иерархии центральный контрольный блок (CCU), по меньшей мере, через один децентрализованный мультиплексор (DCM) связи соединен, по меньшей мере, с одним локальным процессором (LDP) обработки данных, причем децентрализованный мультиплексор (DCM) связи и локальный процессор (LDP) обработки данных образованы полуавтономными блоками, а локальный процессор (LDP) обработки данных установлен в каждом защищаемом объекте, при этом между защищаемым объектом и центральным контрольным блоком (CCU) происходит постоянно актуализированный обмен данными с использованием динамического протокола о состоянии объекта и попытках доступа и т.п., и электроснабжение локального процессора (LDP) обработки данных и связь происходит через один и тот же двужильный провод.

За счет распределения мощности компьютера по трем иерархиям достигается то, что в защищаемом объекте установлена мощность, позволяющая производить анализ событий в объекте и на нем (распределительный интеллект).

В то время как известные системы защиты предусматривают только общую сигнализацию событий в центральный пост, согласно изобретению, сигнализируется также что, где и когда случилось. Постоянная проверка и актуализация сигналов

(данных) в режиме диалога между децентрализованными мультиплексорами DCM связи, локальными процессорами LDP обработки данных и центральным контрольным блоком CCU с использованием динамического протокола об актуальном состоянии объекта обеспечивают повышенную защиту от несанкционированного открывания, идентификацию попыток открывания, а также попыток прерывания линий, попыток излома и т.п. Каждый сбой идентифицируется как таковой, что обеспечивает очень высокую надежность системы. Не только дверь, но и весь объект защищен от взлома или саботажа.

Возможна защита оборудования очень большим числом ключей. Ключи могут при необходимости выдаваться с ограничением по времени для определенной зоны оборудования, а также по комбинированным критериям места и времени. Номер каждого ключа во всем мире ни разу не повторяется. Изменения в списке имеющих разрешение лиц возможны только в зоне центрального блока связи через авторизирующий терминал.

Электронный ключ может быть выполнен в виде стержня или карточки.

Доступ к объекту всегда гарантирован имеющему на то разрешение лицу, даже если произошел перебой в электроснабжении. Электроснабжение для электронного запирающего объекта осуществляется посредством DCM. Механическая блокировка, разъединяемая имеющим разрешение лицом даже при перебое в электроснабжении, продолжает функционировать.

Автоматическая актуализация критериев доступа происходит по всем уровням. Центральное управление и контроль посредством центрального блока связи обеспечивает обзор, актуальность и возможность эффективного вмешательства.

Изобретение более подробно поясняется ниже с помощью примера выполнения электронной системы для контроля доступа и для защиты согласно изобретению на группу кабельных распределительных шкафов. На чертеже изображают:

- фиг. 1: общий вид системы;

- фиг. 2: схему узлов и элементов LDP на внутренней стороне двери кабельного распределительного шкафа.

На фиг. 1 электронная система для контроля доступа и для защиты большого числа кабельных распределительных шкафов 1 скомбинирована с имеющейся в каждом шкафу 1 двухступенчатой механической запорной системой (не показана), например по патенту ФРГ № 4302835 С1.

На фиг. 1 система состоит из центрального контрольного блока CCU, соединенного с децентрализованным мультиплексором DCM связи, и из большого числа расположенных в кабельных распределительных шкафах 1 локальных процессоров LDP обработки данных, соединенных каждый посредством двужильного провода 2 и главного распределителя HVT с децентрализованным мультиплексором DCM.

Главный распределитель HVT может быть заменен, например, этажными распределителями в сетях зданий, если он не нужен.

В двери 3 каждого шкафа 1 расположен невидимый снаружи локальный процессор LDP обработки данных в виде электронного блока провер-

ки, взаимодействующего с двухступенчатым механическим запорным блоком. Локальный процессор LDP служит для контроля состояния шкафа 1 и проверяет дверь 3 в отношении ее положения, положения и блокирования задвижки, а также проверяет весь шкаф 1 в отношении возможных попыток взлома. Локальный процессор LDP содержит на фиг. 2 идентификационный считыватель 14 "электронного ключа", который может быть выполнен в виде карточки или стержня, и вычислительный модуль 12 с ЦПУ и памятью. Локальный процессор LDP перерабатывает все сигналы, поступающие от датчиков, например светового датчика 15, датчика 16 открывания и закрывания, в конкретные кодированные сообщения, он контролирует также любой доступ или открывание, или любые попытки открывания и саботажа, например через "саботажный выключатель" 8. Локальный процессор LDP соединен двужильным проводом 4 с децентрализованным мультиплексором DCM.

Механическое расположение элементов можно варьировать в зависимости от защищаемого объекта.

При перебое в электроснабжении локальных процессоров LDP, например, из-за повреждения телефонного кабеля во время земляных работ, их контрольная часть продолжает работать в течение нескольких часов и регистрирует, а также накапливает в это время изменения состояния шкафа 1. После восстановления электроснабжения данные автоматически передаются в центральный контрольный блок CCU.

Децентрализованный мультиплексор DCM защищает через провод 4 электроснабжение локального процессора LDP и в равной мере через кодированные протоколы обмен данными; он образует интерфейс между локальными процессорами LDP и центральным контрольным блоком CCU (центральное вычислительное устройство). Он контролирует все локальные процессоры LDP, причем между ними и децентрализованным мультиплексором DCM может быть включен главный распределитель HVT.

На фиг. 1 изображена зона контроля децентрализованного мультиплексора DCM, однако, между собой может быть соединено большое число таких зон контроля, так что несколько децентрализованных мультиплексоров DCM подклю-

ны к одному центральному контрольному блоку CCU.

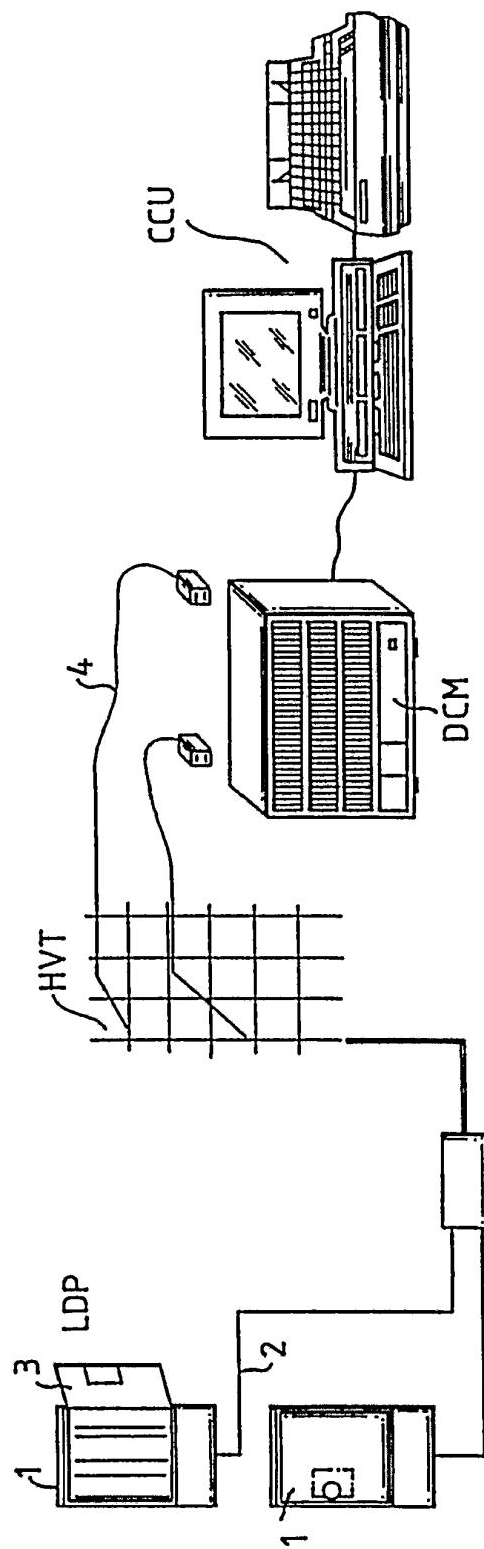
Центральный контрольный блок CCU, задача которого состоит в центральном управлении всеми децентрализованными мультиплексорами DCM, содержит сетевой файл, автоматизирующий файл (разрешения на доступ в виде сортированного в цифровой форме списка ключей и в виде актуализированного по времени списка) для электронного ключа и для статической обработки. Центральный контрольный блок CCU обнаруживает и подает тревогу, и информация из него может быть целенаправленно распределена.

Доступ к одному из шкафов 1 или его открывание обеспечивается тогда, когда имеющее разрешение лицо с помощью механического ключа размыкает первую блокировку замка и, тем самым, открывает отверстие (не показано), в которое он вставляет кодированный электронный ключ (не показан), или к которому он, согласно другой форме выполнения, подводит кодирование идентификационное средство для бесконтактного считывания.

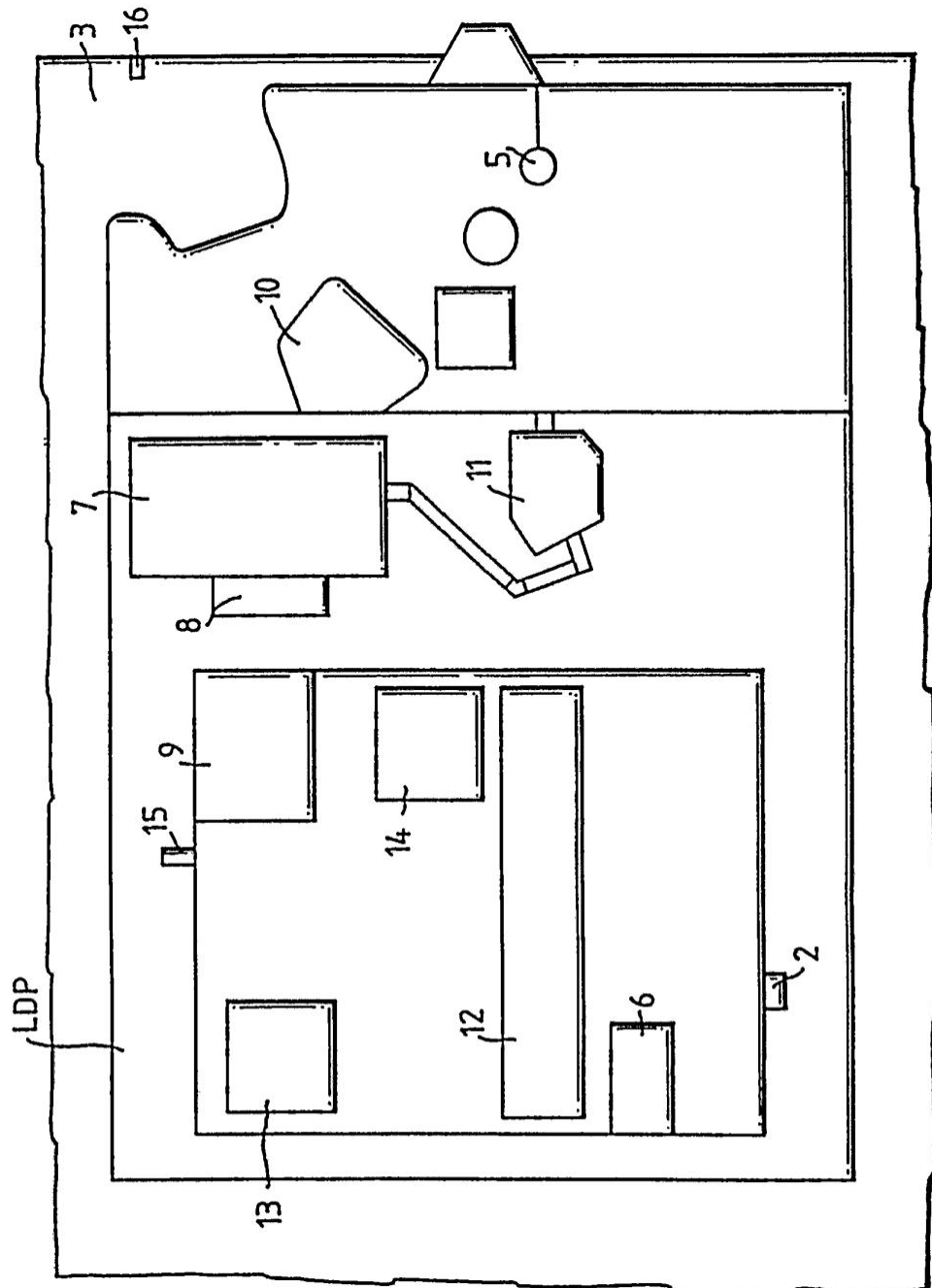
Если идентификация произошла и, тем самым, разрешение на открывание двери 3 шкафа 1 дано, то размыкается вторая, имеющая электронную защиту блокировка, после чего дверь 3 может быть открыта.

На фиг. 2 электронный ключ регистрируется антенной 5 приближения, и зарегистрированные данные направляются для обработки в вычислительный модуль 12 локального процессора LDP. Вычислительный модуль 12 проверяет, разрешен ли ключ для открывания шкафа 1. Подтвержденное разрешение для открывания передается через модем 6 к децентрализованному мультиплексору DCM. От него сигнал через вычислительный модуль 12 подается к бустеру 13 для обесточивания удерживающей катушки 7. Механическое расположение элементов можно варьировать в зависимости от защищаемого объекта.

Если имеющее разрешение лицо не откроет дверь 3 шкафа 1 в течение установленного времени, например 30 секунд, то удерживающая катушка 7 и, тем самым, электронная блокировка 11 замка снова активизируются 9 - электроника датчиков, 10 - контроль блокировки.



Фиг. 1



Фиг. 2

ДП "Український інститут промислової власності" (Укрпатент)
Україна, 01133, Київ-133, бульв. Лесі Українки, 26
(044) 295-81-42, 295-61-97

Підписано до друку _____ 2002 р. Формат 60х84 1/8.
Обсяг _____ обл.-вид. арк. Тираж 50 прим. Зам. _____

УкрІНТЕІ, 03680, Київ-39 МСП, вул. Горького, 180.
(044) 268-25-22
