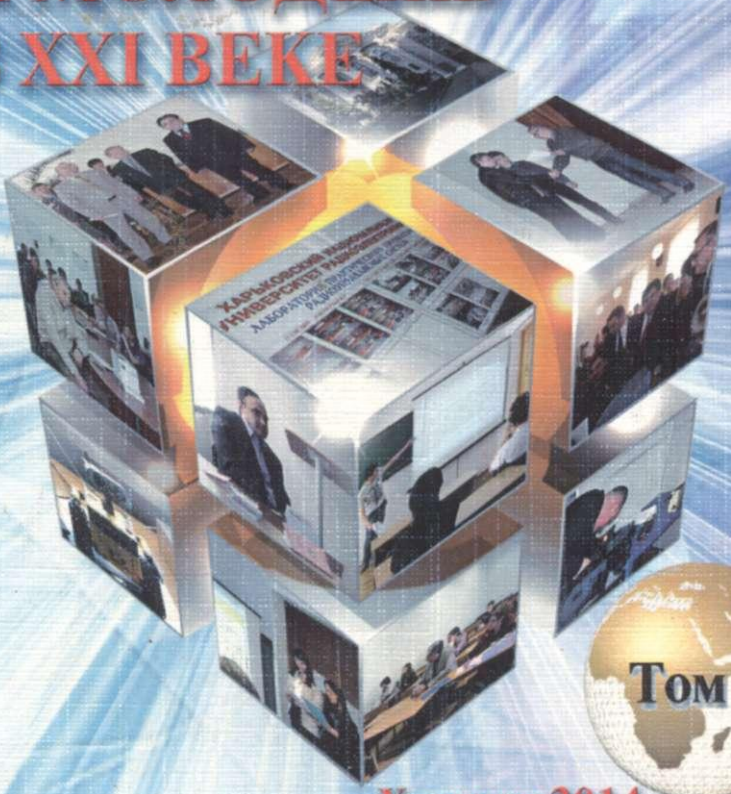
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ

ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ РАДИОЭЛЕКТРОНИКИ

МАТЕРИАЛЫ XVIII МЕЖДУНАРОДНОГО МОЛОДЕЖНОГО ФОРУМА

РАДИОЭЛЕКТРОНИКА И МОЛОДЕЖЬ В XXI ВЕКЕ



Том 4

Харьков 2014

КРИТЕРИИ ОЦЕНКИ И КЛАССИФИКАЦИЯ СРЕДСТВ И СИСТЕМ КОНТРОЛЯ ДОСТУПА

Щеголев Д.Ю.
Научный руководитель – доц., к.т.н. Токарь Л.А.
Харьковский национальный университет радиоэлектроники
(61166, г. Харьков, пр. Ленина,14, каф Телекоммуникационных систем)
e-mail: afzkkh@gmail.com, тел. (095) 917-58-27

Currently, the construction of integrated information security systems , special attention building access control systems that part of a huge complex administrative and hardware. System access control system (ACS) - a very important part to build and security in the enterprise. System access control system (ACS) - a set of technical or hardware and software designed to provide authorized access to the individual zones (groups of rooms , fenced area) and specific space , operational control and logging of access or attempt to access facility staff or unauthorized persons .

В настоящее время при построении комплексных систем защиты информации, особое внимание уделяется построению систем контроля управления доступом, что является неотъемлемой частью огромного комплекса административно-аппаратной части. Системы контроля и управления доступом (СКУД) - совокупность технических или технических и программных средств, предназначенных для обеспечения санкционированного доступа в отдельные зоны (группы помещений, огражденная территория) и конкретные помещения, оперативного контроля и регистрации событий, связанных с доступом или попыткой доступа персонала учреждения или посторонних лиц.

Решение проблемы идентификации может осуществляться двумя раз личными путями: с использованием специализированных элементов-ключей; опознаванием конкретного лица по его неотъемлемым характеристикам.

В особенно ответственных случаях оба эти подхода могут быть использованы одновременно, хотя использование второго пути существенно ограничивается очень высокой стоимостью аппаратуры опознавания (по отпечаткам пальцев, голосу, рисунку сетчатки глаза и т.д.). Поэтому чаще всего используется первый подход.

Ключи, используемые в системах контроля доступа, могут быть основаны на разных принципах работы: механических, логических, магнитных, электромагнитных, электронных.

Электромагнитные и электронные ключи в настоящее время считаются наиболее эффективными. При использовании любого типа ключа важно одно - этот ключ должен иметь возможность однозначно ассоциироваться с конкретным лицом - владельцем ключа. Кроме того, его подделка должна быть максимально затруднена, что опять же на

сегодняшний день дает явное преимущество электронным ключам, основанным на новейших технологиях.

Как правило, в автоматизированных системах контроля доступа сочетаются контроль обоих видов. При этом может происходить детализация понятия зоны контроля, при которой вся контролируемая территория может разбиваться на несколько непересекающихся зон контроля со своими особенностями доступа. Каждой зоне контроля и каждому помещению с контролируемым входом присущи свои ограничения на вход.

Общий принцип должен быть следующим: чем более ответственный уровень администрации дает права доступа к конкретному объекту (зоне, помещению) и чем меньше лиц имеют такие права, тем более ограниченным должен быть режим доступа и более строгими требования к идентификации.

Режим доступа для помещений должен быть, как правило, более жесткий, чем для зон контроля. Необходимо различать ситуации, когда вход и выход осуществляются по разным правилам.

Режимы запрета доступа могут применяться в том случае, если необходимо предотвратить доступ ко всем или некоторым помещениям (зонам) на временной или постоянной основе всем, кроме ограниченного числа специально уполномоченных лиц. Запрет доступа может быть плановым или экстренным, при возникновении особых ситуаций. Режимы доступа в соответствии с присвоенными правами являются основными в системах контроля доступа.

Способ предоставления конкретному лицу прав доступа существенным образом влияет на надежность контроля доступа в целом. Поэтому наиболее целесообразно предоставить такую возможность только одному сотруднику - Администратору Системы Контроля Доступа, который действует на основе принятых в организации административных процедур.

Должна быть исключена возможность изменения предоставленных прав другими лицами, в том числе и их владельцами. Применительно к автоматизированным системам это требует ограничения доступа к используемым техническим средствам. При оперативном контроле о любых попытках нарушения установленного режима доступа немедленно сообщается специальному лицу - дежурному системы контроля доступа.

В работе был проведен анализ критериев оценки средств и систем контроля управления доступом, а также была приведена классификация аппаратной части.

Список литературы:

1. Компьютерная преступность и информационная безопасность / А.П. Леонов [и др.]; под общ. Ред.А.П. Леонова. – Минск: АРИЛ, 2000. – 552 с.