УДК 004.5

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Осипов Павел Александрович[1], Минзов Анатолий Степанович[2]

[1]Магистрант;
ГБОУ ВО МО «Университет «Дубна»;
Институт системного анализа и управления;
Россия, 141980, Московская обл., г. Дубна, ул. Университетская, д. 19;
e-mail: osipov.pavel92@gmail.com.

[2]Доктор технических наук, профессор Института системного анализа и управления;
ГБОУ ВО МО «Университет «Дубна»;
Институт системного анализа и управления;
Россия, 141980, Московская обл., г. Дубна, ул. Университетская, д. 19;
e-mail: 926-565-0570@mail.ru.

В статье рассматривается внедрение систем управления и контроля доступом в образовательный процесс. В результате работы были разработаны лабораторные работы с кратким теоретическим описанием всех рассмотренных типов систем контроля и управления доступом.

Ключевые слова: СКУД в образовании, биометрические системы, *RFID*-карты, ключи *iButton*, домофоны, *usb*-ключи *eToken*.

SYSTEM OF ACCESS CONTROL IN CORPORATE INFORMATION SYSTEMS

Osipov Pavel[1] , Minzov Anatoliy[2]

[1]Graduate student of the Department of System Analysis and Management,
Dubna State University;
Institute of the system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: osipov.pavel92@gmail.com.

[2]Doctor of Technical Sciences, Professor of the Institute of System Analysis and Management;
Dubna State University;
Institute of the system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: 926-565-0570@mail.ru.

The article discusses the implementation of access control systems in the educational process. As a result of laboratory work with a brief description of all the theoretically discussed types of access control have been developed.

Keywords: Access Control System in the Education, biometric systems, RFID-cards, the iButton keys, intercoms, eToken usb-keys.

Введение

Системы контроля и управления доступом (СКУД) в настоящее время получили довольно широкое распространение. СКУД используются для поддержания и обеспечения режима безопасности на предприятии, в том числе и для обеспечения защиты информации в корпоративных информационных системах.

Использование СКУД позволяет не только контролировать доступ к защищенному объекту, но и сделать этот процесс более удобным и быстрым. А программное управление позволяет гибко

настроить функционирование СКУД. Например, доступ по расписанию, когда для каждого клиента задается расписание доступа к защищенному объекту, обеспечивается разграничение уровней доступа, контроль соблюдения режима работы и контроль за передвижением клиента.

СКУД позволяет обеспечить защиту информации в корпоративных информационных системах при недобросовестной конкуренции в условиях современного бизнеса. В таких условиях для любого предприятия встает проблема обеспечения безопасности его основных активов [1].

СКУД могут сыграть решающую роль при расследовании инцидентов, так как эти системы ведут журналы событий, в которые заносится информация о всех взаимодействиях пользователя со СКУД.

Таким образом, внедрение в образовательную программу таких систем позволяет обеспечить студентов необходимыми знаниями администрирования и проектирования программного обеспечения СКУД систем, которые они смогут применить в реальных проектах.

Цель настоящей статьи заключается в описании разработанной методики обучения студентов Института системного анализа и управления государственного университета «Дубна» технологиям контроля и управления доступом к информационным системам. Эта работа в полном объеме реализуется в учебных программах бакалавриата по направлению 09.03.02 («Информационные системы и технологии») по профилю «Безопасность информационных систем», а также используется для ознакомления студентов с технологиями контроля и управления доступом к информационным системам в дисциплине «Информационная безопасность и защита информации» при поведении занятий по магистерским программам:

- 090403 (Прикладная информатика) «Системы корпоративного управления»
- 220105 (Системный анализ и управление) «Системный анализ данных и моделей принятия решений»
- 220101 (Системный анализ и управление) «Теория и математические методы системного анализа и управления в технических системах»
- 220102 (Системный анализ и управление) «Системный анализ проектно-технологических решений».

Общие сведения о СКУД

Система контроля и управления доступом представляет собой совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью [2].

Разработка и постановка на производство средств и систем контроля управления доступом должны производиться в соответствии с ГОСТ Р 15.201.

Средства СКУД должны обеспечивать непрерывное функционирование и работу в автоматическом режиме, за исключение случаев чрезвычайных, аварийных и тревожных ситуаций, а также по требованию заказчика.

СКУД должна защищать объект от несанкционированного доступа, контролировать и вести учет посетителей охраняемого объекта. Кроме того, СКУД не должны создавать препятствий для доступа к объектам со свободным входом [1].

Для непрерывного функционирования СКУД должны быть снабжены резервным источником питания, переход на который должен осуществляться в автоматическом режиме без нарушения установленных режимов работы и функционального состояния.

Основными частями СКУД являются:

- Устройства преграждающие управляемые;
- Устройства считывающие;
- Идентификаторы (ИД);
- Средства управления в составе аппаратных устройств и программных средств.

В состав СКУД могут входить другие дополнительные средства: источники электропитания; датчики (извещатели); дверные доводчики; световые и звуковые оповещатели; кнопки ручного управления устройствами; устройства преобразования интерфейсов сетей связи; аппаратуру передачи данных по различным каналам связи и другие устройства, предназначенные для обеспечения работы СКУД [2].

В состав СКУД могут входить также аппаратно-программные средства и средства вычислительной техники (СВТ) общего назначения (компьютерное оборудование, оборудование для компьютерных сетей, общее программное обеспечение) [2].

Постановка задачи

Цель: внедрение СКУД в образовательный процесс для ознакомления с технологиями управления и исследования таких систем.

Исходные данные: Лаборатория технических средств защиты информации Института системного анализа и управления Университета «Дубна».

Априорные представления: студент способный администрировать СКУД и проводить исследования по определению погрешности аутентификации с использованием различных технических систем управления доступом.

Ожидаемый результат: студент, имеющий базовые знания по всем типам СКУД, рассмотренным в ходе практических занятий, ознакомленный с их администрированием и способный к исследованию и совершенствованию этих систем.

Задачи, решаемые с использованием СКУД

В ходе изучения СКУД решаются следующие задачи:

- Получение студентами базовых теоретических сведений по функционированию биометрических систем, систем на основе RFID-карт, ключей iButton, домофонов, usb-ключей eToken.
- Знакомство с реальным оборудованием СКУД на специализированном стенде и обучение его администрированию.
- Исследование погрешностей аутентификации пользователей СКУД.
- Формирование представления у студентов об возможности использования СКУД в повседневной жизни при защите информации в корпоративных информационных системах.

Системы контроля доступа на основе биометрических систем

Средства биометрической аутентификации, основанные на методах распознавания геометрии лица и отпечатков пальцев. В ходе лабораторной работы обучающиеся знакомятся с теоретическими основами биометрической аутентификации, а также на практике знакомятся с биометрическим терминалом *ZKTeco uFace* 302 и биометрическим замком *ZKBiolock* L4000.

ZKTeco uFace 302 – мульти-биометрический терминал идентификации (см. рис. 1). Оснащен инфракрасной камерой высокого разрешения, которая позволяет идентифицировать пользователя в темноте, и сканером отпечатков пальцев [3].

Рис. 1. Стенд с биометрическими СКУД

*ZKBiolock L*4000 (рис. 1) – биометрический замок, позволяющий идентифицировать пользователя по отпечатку пальца или с помощью ввода пароля. Замок имеет автономное питание за счет 4-х батареек типа *AA*. В случае отказа батареек биометрический замок можно открыть с помощью механического ключа или с использование батарейки типа «крона» на 9*B* [4].

Системы контроля доступа на основе бесконтактных RFID-карт

В ходе лабораторной работы обучающийся работает со СКУД на основе бесконтактных *RFID*-карт. Лабораторный стенд состоит из двери, электромагнитного замка, контроллера *HID EdgePlus Solo ES*400 и считывателя *HID RW*100 *Mullion* (рис. 2).

Контроллер *HID EdgePlus Solo ES*400 [5] обеспечивает управление электромагнитным замком двери. Управление контроллером происходит по сети с помощью веб-браузера. Считыватель *RFID*-карт *HID RW*100 *Mullion* производит считывание идентифицирующих данных с карты пользователя и передачи их на контроллер, который в свою очередь принимает решение о возможности или невозможности предоставления доступа идентифицирующему пользователю.

Из дополнительных возможностей *HID EdgePlus Solo ES*400 стоит отметить то, что имеется возможность гибкой настройки доступа по расписанию, которая рассмотрена в ходе выполнения лабораторной работы. Все взаимодействия с контроллером осуществляются с помощью веб-интерфейса с использование браузера *Internet Explorer*. *IP*-адрес для доступа к веб-интерфейсу: «169.254.242.121». В рамках учебной лаборатории стенд включен в локальную образовательную сеть и доступен для администрирования с любого учебного компьютера университета «Дубна».

Рис. 2. Учебный стенд «Учтех-профи» на основе RFID-карт

Системы контроля доступа на основе домофонов и на основе IButton

В ходе работы рассматриваются принципы работы СКУД на основе домофона и *IButton*. Учебный стенд СКУД состоит из контроллера *IronLogic Z-5R* [6], считывателя ключей IButton, дубликатора электронных ключей *Keymaster 3RF*, ключей *IButton*, домофона (рис. 3).

Домофон представляет собой набор электронных устройств, обеспечивающих двухстороннюю связь «дом-улица» в многоквартирных домах, коттеджах и в частных домах.

IButton-устройство представляет собой компьютерный чип, заключенный в корпусе из нержавеющей стали. Устройства *IButton* используют корпус из нержавеющей стали, как электронный коммуникационный интерфейс.

Keymaster 3RF – это устройство, предназначенное для создания дубликатов электронных ключей, как контактных, так и бесконтактных (работающих на частоте 125 *KHz*). Дубликатор может питаться от внешнего источника питания, от элемента питания или от *USB*-порта компьютера [7].

Рис. 3. Учебный стенд СКУД на основе IButton и домофона

Системы контроля доступа на основе eToken

В ходе лабораторной работы рассматривается многофакторная авторизация в ОС *Windows* с использование *USB*-устройства *eToken*. В состав учебного стенда входят *USB*-устройство *eToken*, программное обеспечение *eToken PKI Client*, программное обеспечение *EIDAuthenticate*.

USB-ключ *eToken PRO* (*Java*) представляет собой персональное устройство аутентификации и защищенного хранения пользовательских данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронно-цифровой подписью (ЭЦП). Устройство имеет возможность двухфакторной аутентификации, при которой пользователь авторизуется, представляя *USB*-ключ *eToken* и персональный *PIN*-код пользователя [8].

Утилита *eToken PKI Client* предоставляет администратору инструменты для работы с устройствами *eToken,* а также для задания политик использования устройств пользователями. Пользователи могут использовать эту утилиту для выполнения базовых операций с *eToken*, таких как: смена пароля, просмотр сертификатов, хранящихся в памяти устройства. Кроме того, утилита *eToken PKI Client* позволяет пользователям и администраторам легко экспортировать и импортировать сертификаты между *eToken* и компьютером [9].

EIDAuthenticate используется для аутентификации с помощью смарт-карт на автономных компьютерах, или для защиты доменных учетных записей пользователей. Позволяет создавать самоподписанные сертификаты пользователей.

Заключение

Внедрение СКУД в учебный процесс позволяет повысить уровень подготовки студентов в области знания технических средств защиты информации и управления ими. Стенд может также

использоваться для проведения научно-исследовательских работ студентов при разработке алгоритмов и программ аутентификации пользователей по биометрическим признакам.

Список источников

1. Невский А.Ю., Баранов О.Р. Технические средства охраны: учебное пособие / А.Ю. Невский, О.Р. Баранов. – М. : ВНИИ геосистем, 2015. – 186 с. : ил.
2. ГОСТ Р 51241-2008. СРЕДСТВА И СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ. Классификация. Общие технические требования. Методы испытаний.
3. iFace Series Installation Guide. – [Электронный ресурс]. URL: https://www.zkteco.com/upload/4file/fronts/2015/20150422/201504220644315457.pdf. – Дата обращения: 22.06.2016.
4. User manual of ZKBiolock L4000. – [Электронный ресурс]. URL: http://www.zkteco.co.za/manuals/L4000_User_Manual.pdf. – Дата обращения: 22.06.2016.
5. EdgeSolo Руководство по эксплуатации – Русский – HID Global Corporation, 2009.
6. IronLogic Z-5R – Инструкция по подключению и эксплуатации.
7. KeyMaster 3RF – Инструкция по эксплуатации.
8. Компания «Аладдин Р.Д.». – [Электронный ресурс]. URL: http://www.aladdin-rd.ru/catalog/etoken/java/.
9. eToken PKI Client 5.1 SP1 – Руководство пользователя.
10. Афанасьев А. А., Веденьев Л. Т., Воронцов А. А. и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. – М. : Горячая линия – Телеком, 2009. – 552 с.: ил.
11. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. / Ворона В. А., Тихонов В. А. – М. : Горячая линия – Телеком, 2010. – 272 е.: ил.
12. Волхонский В.В. Системы контроля и управления доступом. / Волхонский В.В. – СПб: Университет ИТМО, 2015. – 200 с.