Акишин Андрей Владимирович,
Доцент 32 кафедры 3 факультета
ФГБОУ ВО «Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко», Краснодар

Юминов Андрей Павлович, слушатель
ФГБОУ ВО «Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко», Краснодар

Лимаренко Александр Игоревич, слушатель
ФГБОУ ВО «Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко», Краснодар

Ушаков Сергей Павлович, слушатель
ФГБОУ ВО «Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко», Краснодар

Назаренко Евгений Эдуардович, слушатель
ФГБОУ ВО «Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко», Краснодар

ВОЗМОЖНОСТИ СОВРЕМЕННЫХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ К КОНФИДЕНЦИАЛЬНЫМ ИНФОРМАЦИОННЫМ РЕСУРСАМ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

Аннотация: Системы контроля и управления доступом (СКУД) представляют собой комплексные решения для обеспечения информационной безопасности и защиты данных на объектах информатизации. Системный подход к построению СКУД включает организационные, программные и аппаратные компоненты, а также принципы непрерывного развития и адаптации к новым угрозам. Ограничение доступа становится важным инструментом в борьбе с угрозами безопасности, обеспечивая надежную защиту информации и материальных ценностей.

Ключевые слова: система контроля и управления доступа (СКУД), объект информатизации (ОИ), несанкционированный доступ, программно-аппаратные средства, защита информации.

Системный подход к построению системы защиты подразумевает под собой наилучшее сочетание связанных друг с другом организационных, программных, аппаратных, физических и других свойств. Применяется на всех этапах обработки информации, а также подтверждается практикой создания как отечественных, так и зарубежных систем. Теперь о принципе непрерывного развития системы. Этот принцип является одним из фундаментальных для компьютерных информационных систем, и не менее важным для систем информационной безопасности. Способы реализации угроз информации постоянно совершенствуются, а потому обеспечение безопасности информационных систем должно быть непрерывным. Этот процесс заключается в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования систем безопасности, непрерывном контроле, выявлении ее узких и слабых мест, потенциальных каналов утечки информации и новых способов несанкционированного доступа. Несанкционированный доступ к информации возможен в любой системе, от небольших организаций до крупных государственных учреждений. Тщательное внимание к защите данных и создание пунктов информационной безопасности может минимизировать потери и предотвратить попытки кражи или копирования данных. Особое внимание следует уделить работе с

уполномоченными сотрудниками, имеющими доступ к критически важной информации. Защитные меры должны быть приняты заранее, поскольку уступка инициативы может привести к потере данных. Современные достижения науки и техники обусловили широкое внедрение в нашу жизнь множества электронных систем. Многие из них предназначены для выполнения монотонных, рутинных, но важных действий по авторизации, контролю, а также сбору информации о полученных результатах. Система контроля и управления доступа – одна из таких систем. Это совокупность программно-аппаратных технических средств контроля и средств управления, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через «точки прохода»: двери, ворота, КПП. Возможна интеграция данного оборудования с охранной, противопожарной сигнализациями и другими техническими средствами. СКУД могут быть наиболее доступным решением задач по обеспечению безопасности частных лиц и жилых объектов. Примечательно, что за счет простых и доступных технологий, которые умещаются в стандартные процессы автоматизации, можно достигать высокой эффективности работы контролирующих средств.

Задачи, выполнимые СКУД:

– Предотвращение хищения имущества;
– Защита материальных ценностей от повреждения;
– Контроль посещения объектов;
– Защита конфиденциальной информации;
– Регулировка потока;
– Контроль въезда и выезда транспорта.

Классификацию СКУД проводят по нескольким параметрам. Рассмотрим основные из них.

По методу управления:

– **Автономные**. В базу данных вносят коды карт доступа, которым вход разрешен. При совпадении данных замок открывается. Эти системы не требуют подключения к ПК, просты в использовании.

– **Сетевые** (централизованные). Эти СКУД имеют больше возможностей. Они могут настраивать доступ на объект по расписанию, контролируют график работы пользователей, интегрируются с видеокамерами и другими системами. Эти СКУД управляются дистанционно и подключаются к ПК.

– **Универсальные**. Включают в себя функции автономных и сетевых систем. Устройства могут переходить в автономный режим работы при необходимости;

– **Биометрические**. Современные СКУД, работающие на основе индивидуальных данных каждого пользователя. В программу заносятся отпечатки пальцев, рисунок сетчатки глаза, геометрия лица персонала – на основе этих показателей осуществляется доступ к объекту. Преимущество – высокий уровень безопасности.

По уровню идентификации:

– **Одноуровневые**. Идентификация посетителей производится по одному признаку, к примеру, с помощью считывания кода карты.

– **Многоуровневые**. Доступ на объект осуществляется по нескольким признакам: по коду карты и биометрическим данным.

По числу контролируемых точек доступа:

– Малой емкости – менее 80 точек;
– Средней емкости – до 250 точек;
– Большой емкости – более 256 точек.

Параметры, по которым различают различные виды СКУД:

– Уровень распознавания;
– Число настроек;
– Численность проходящих через СКУД сотрудников;
– Количество человек, которое может запомнить система;
– Устойчивость к воздействию внешней среды.

Характеристики для классификации систем контроля и управления доступом:

– Уровень эффективности защиты СКУД от поломки;

– Степень конфиденциальности;

– Возможность оперативного внесения изменений в программное обеспечение;

– Автономная идентификация;

– Возможности внедрения пропускной системы для сотрудников с разными полномочиями;

– Сбор и анализ информации;

– Надежность работы замочных механизмов;

– Распечатка необходимых данных.

В состав СКУД входят следующие компоненты:

1) Пользовательский идентификатор – им может быть как электронное устройство, карта, брелок, так и человеческий орган. Если это электронное устройство, то, как правило, внутри него имеется чип с антенной или используется магнитная полоса. Если ли же это человеческий орган, то, в основном, используют отпечаток одного из пальцев (например, большого пальца правой руки) или же всей руки сразу, либо радужную оболочку глаза, или иные биометрические признаки личности: черты лица, геометрия кисти руки, рисунок сосудов за сетчаткой глаза, расположение вен на руке, динамические характеристики почерка, особенности речи, динамика ударов по клавишам и т.д. Любому пользовательскому идентификатору присваивается уникальный цифровой код, который, в свою очередь, содержит необходимую информацию о правах доступа его владельца;

2) Считыватель – устройство, выполняющее считывание информации с пользовательского идентификатора. Как правило считыватели устанавливаются как на входе, так и на выходе;

3) Преграждающее устройство – шлагбаумы, двери с замками, ворота. Турникеты;

4) Контроллер СКУД – ключевой электронный модуль, реализующий идентификацию объектов доступа, по полученной информации от считывателей и осуществляющий управление разграничением доступа на территорию, управление преграждающими и сигнализирующими устройствами, получение событий от различных датчиков и принятие соответствующих решений с передачей их исполнительным устройствам и программному обеспечению;

5) ПО СКУД – элемент системы, с помощью которого можно централизованно управлять контроллерами системы контроля доступа, используя персональный компьютер (ПК), вести мониторинг происходящих событий, формировать отчеты и т.д.;

6) Кнопка RTE (Request to exit), иначе – кнопка выхода, предназначена для кратковременного переключения исполнительного устройства в положение «открыто», при этом контроллер системы контроля доступа лишь запоминает сам факт выхода через точку прохода, личностные данные при этом не известны.

7) Конвертеры среды для подключения модулей к СКУД друг к другу и к ПК, предоставляющие возможность организовать контроль доступа и учет рабочего времени на предприятии с несколькими проходными и большим количеством дверей или турникетов. Как правило, контроллер подключается к компьютеру с помощью специального конвертера (USB или TCP\IP) по протоколу RS-485;

8) Вспомогательное оборудование (датчики, кнопки, блоки бесперебойного питания и т.п.).

Как российские, так и зарубежные производители предлагают различные варианты СКУД, каждая из которых обладает своими особенностями. Рассмотрим некоторые из них.

Российские разработки

ParsecNET 3 – система контроля доступа, предназначенная для организации контроля и управления доступом на различных точках доступа, получения отчетности о всех событиях в системе, интеграции с другими системами для решения возникающих на объекте задач.

Основой аппаратной части системы являются контроллеры. К ним подключается необходимое дополнительное оборудование: считыватели, интерфейсные модули, охранные датчики и прочее.

ParsecNET 3 используется на предприятиях различного масштаба. На сегодняшний день система установлена более чем на 15 тысячах объектов как в России, так и за границей.

GATE – сетевая система контроля доступа для объектов различного масштаба (от небольшого офиса до крупного предприятия). Привлекает простотой настройки и обслуживания. Основным элементом системы является контроллер GATE-4000. Для управления системой используется специализированное программное обеспечение, работающее под управлением Windows.

Программное обеспечение GATE предназначено для выполнения следующих основных задач

- Конфигурирование системы.
- Работа с пользователями (выписка и удаление пропусков, изменение прав доступа).
- Мониторинг (просмотр событий в реальном времени).
- Контроль за перемещением персонала.
- Выполнение команд управления (блокировка, открывание двери).
- Чтение событий из памяти контроллеров и сохранение их на жестком диске компьютера.
- Получение отчетов о событиях системы.
- Учет рабочего времени персонала.
- Создание отчетов об опоздавших и ушедших раньше.
- Фотоверификация.
- Поддержка временных пропусков.

Аппаратно-программный комплекс Комендантъ. Основное назначение– автоматизация управления, контроля, кадрового учета, мониторинга действий персонала и посетителей, учета рабочего времени сотрудников организаций – на уровне обеспечения централизованного управления физическим доступом сотрудников (посетителей) к помещениям предприятия с осуществлением видеофиксации, автоматизации работы инженерных систем, мониторинга использования персональных компьютеров, записи телефонных разговоров.

Комплекс предоставляет статистику действий персонала в рабочее и нерабочее время для использования полученных данных в кадровой работе. Возможности многоуровневой системы учета рабочего времени сотрудников, интегрированной в программное обеспечение Комендантъ, позволяют оценивать действия персонала не только на уровне физического доступа на предприятие, но и на уровне статистики телефонных соединений с мониторингом времени работы сотрудников за персональными компьютерами.

Разработки США

WIN-PAK XE (Xpress Edition) – это базовый пакет программного обеспечения, поддерживающий только функции СКУД, разработанный компанией Honeywell. Он предназначен для управления контроллерами NetAXS и NS2/NS2P с одной рабочей станции. Предоставляет единый пользовательский интерфейс для работы с различными контроллерами и считывателями системы контроля доступа. В отличие от программных

продуктов других фирм-производителей WIN-PAK не имеет лицензионных ограничений по числу считывателей, что снижает стоимость при расширении системы.

Система контроля доступа Casi Rusco (General Electric) работает с большим количеством считывателей и поддерживает операционные системы как Windows, так и Linus/Unix, и базы данных SQL, Oracle, DB2.

Система контроля доступа OnGuard Access компании Lenel Systems International является составной частью платформы OnGuard и может обслуживать как небольшие, так и крупные объекты: офисные здания, аэропорты, учебные заведения и др. Она состоит из программного модуля OnGuard Access и аппаратной части – контроллеров, модулей входов/выходов для охранных датчиков / исполнительных устройств, модулей управления RFID и биометрическими считывателями и считывателей различных производителей.

Разработки Европейских стран

Nedap – AEOS (Голландия) – это система контроля доступа и управления безопасностью, основанная на интеллектуальной сетевой технологии. В AEOS основные функциональные возможности формируются согласно пожеланиям конечного пользователя путем передачи информации между равноправными узлами сети и гибкими поведенческими компонентами. AEOS основана на интернет-технологии. Это означает, что можно подключиться к системе с помощью веб-браузера с любого компьютера.

Все права доступа и программированные действия определяются и обрабатываются на самом низком уровне системы. Управление системой и необходимый уровень безопасности гарантированы, несмотря на доступность сети или сервера. Система AEOS может функционировать независимо от сервера. Собственные IP-контроллеры AEOS (AEpu) могут напрямую связываться друг с другом и с другими IP устройствами, например, с камерами наблюдения.

Система контроля доступа **SMARTair** (Швеция) – решение компании ASSA ABLOY. Это платформа контроля доступа, основанная на автономных устройствах с возможностью онлайн управления, обеспечивающая максимальную безопасность и удобство. Система Smartair предоставляет полный контроль доступа в реальном времени. Системы контроля доступа ASSA ABLOY позволяют администраторам контролировать доступ к защищенным областям посредством физических, логических, электронных, автономных, онлайн и беспроводных решений.

Продукт **Kaba evolo smart** компании Dormakaba (Швейцария) позволяет организовать систему контролируемого доступа при помощи смартфона. Приложение для Android регулирует список людей, которые могут получить доступ к двери. Доступ может быть ограничен или изменен в любое время.

Реализация СКУД на объекте информатизации

Объект информатизации – это совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров. СКУД, в свою очередь, не позволяет злоумышленнику получить несанкционированный доступ к информации, обрабатываемой на объекте информатизации, путём защиты от несанкционированного физического доступа к ОИ, хищения носителя информации, диверсия в отношении ОИ и его элементов.

Предложить один единственный универсальный вариант реализации СКУД невозможно, так как многое зависит от различных факторов, таких как выделяемый бюджет, условия размещения, географическое положение, численность личного состава и др. При формировании СКУД на объекте информатизации важно сочетать различные средства зашиты и контроля в целях повышения эффективности системы. Так, одной наиболее удачной реализацией пользовательского идентификатора для прохода на территорию является геометрия лица методом 2D распознавания. Данный метод не требует больших затрат и позволяет исключить затор, что крайне важно, так как поток входа и выхода людей неравномерен. Он наблюдается перед началом рабочего дня и соответственно по его окончанию. Находящийся же на КПП (проходной) персонал позволяет исключить попытку обмана системы распознавания. Значительным недостатком данного метода является необходимость в хорошей освещенности помещения, где размещено устройство распознавания.

Наиболее очевидной составляющей систем контроля доступа являются разнообразные преграждающие устройства. В зависимости от решаемых задач различают несколько их разновидностей. Когда требования к безопасности территории повышены, преграждающие устройства устанавливаются на входе или въезде на объект.

В качестве преграждающего устройства подойдут турникеты. Существуют различные виды турникетов:

– Триподы – простые барабанные конструкции с тремя планками (обычные и тумбовые);

– Створчатые – турникеты, преграждающие путь раскрыванием створок, расположенных друг против друга;

– Роторные – полуростовые и полноростовые конструкции, представленные рядом планок, которые закреплены на вращающейся вертикальной оси.

Наибольшую защищенность обеспечат полноростовые створчатые турникеты, так как нарушитель не сможет их банально перепрыгнуть или преодолеть каким-либо образом, не прибегая к физическому воздействию. Для экстренных ситуаций должен быть предусмотрен как механизм, блокирующий турникет в случае попытки незаконного проникновения на территорию, так и кнопка выхода, обеспечивающая выход за территорию, для оперативной эвакуации (например, в случае возникновения пожара или других происшествий).

Программно-аппаратная часть СКУД реализуется на основе сетевой СКУД GATE от отечественного производителя ООО «Равелин Лтд.». Контроллер обладает невысокой стоимостью (около 7 тыс. рублей), а ПО позволяет выполнять задачи по конфигурированию всей системы, контролю за перемещением персонала, хранению событий из памяти контроллеров на жестком диске, фотоверификации.

Таким образом, системы контроля и управления доступом представляют собой важный элемент информационной безопасности организаций, обеспечивая защиту конфиденциальной информации и предотвращая несанкционированный доступ. Эффективная реализация СКУД требует комплексного подхода, включающего организационные, программные и аппаратные компоненты, а также постоянное обновление в ответ на новые угрозы.

Разнообразие типов СКУД позволяет адаптировать решения под конкретные нужды организаций. Примеры успешных разработок, как отечественных, так и зарубежных, демонстрируют широкий спектр возможностей в этой области.

Успешная интеграция СКУД с другими системами безопасности, а также внимательный подход к выбору компонентов с учетом бюджета и численности персонала, являются ключевыми факторами для достижения надежной защиты информации и материальных ценностей на ОИ. Таким образом, СКУД становятся необходимым инструментом для обеспечения безопасности в организациях любого масштаба.

Список литературы:

1. ГОСТ Р 51275-2006. Объект информатизации. Факторы, воздействующие на информацию [Текст]. – Москва: Стандартинформ, 2006. – 11 с.

2. Козловская Д. А. Разработка системы контроля и управления доступом: понятие, характеристика и основные требования [Текст] / Д. А. Козловская // Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. – Санкт-Петербург, 2021.

3. Козлов А. Е. Системы контроля управления доступом: российский опыт [Текст] / А. Е. Козлов // ПАО «Арсеньевская авиационная компания «Прогресс» имени Н.И. Сазыкина. – Арсеньев, 2020.

4. Существующие Программные средства для поддержки принятия управленческих решений должностными лицами подразделения информационной безопасности при выявлении угроз / Н. В. Хечиев, А. П. Челышев, Д. А. Охотин [и др.] // Флагман науки. – 2025. – № 1 (24). – С. 433-436. – EDN WPWGFD.

5. Оленева, Н. Р. Системы контроля управления доступом российского и зарубежного производства / Н. Р. Оленева, Д. С. Семяшкина // ИТ Арктика. – 2019. – № 1. – С. 93-103. – EDN GQSTVR.

6. Свидетельство о государственной регистрации программы для ЭВМ № 2022681723 Российская Федерация. Программа поддержки принятия решений о допуске персонала на охраняемые объекты: № 2022680849: заявл. 24.10.2022: опубл. 16.11.2022 / А. В. Акишин, М. Ф. Ковнацкий, С. Н. Ершов [и др.]. – EDN FNUSYP.

7. Существующие методы оценки эффективности разработки программного обеспечения для поддержки принятия решений должностными лицами подразделения технической защиты при выявлении информационных угроз / Н. В. Хечиев, А. А. Максаков, Д. А. Охотин [и др.] // Флагман науки. – 2025. – № 1 (24). – С. 430-432. – EDN AVCODU.