Г. А. Наурусова[1], Ю. Е. Карякин[2], Я. В. Волох[3]
[1]Военная академия материально-технического обеспечения имени генерала армии А. В. Хрулева, г. Санкт-Петербург
[2]Тюменский государственный университет, г. Тюмень
[3]ООО «Курсорс», г. Санкт-Петербург

УДК 004

ПРОЕКТИРОВАНИЕ ПРОЦЕССА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ СИСТЕМ БЕЗОПАСНОСТИ

Аннотация. *В работе исследованы основные представления систем безопасности, в частности, систем контроля и управления доступом. Определены классификация систем контроля и управления доступом, требования к их оптимизационной работе. Проведено функциональное моделирование систем контроля и управления доступом для типового объекта.*

Ключевые слова: *безопасность, проектирование процесса, система безопасности, система контроля и управления доступом, функциональное моделирование.*

Введение. Система безопасности представляют совокупность правовых, организационных, инженерно-технических, программно-аппаратных и силовых средств и мер, обеспечивающих безопасность организации. В современном мире одних силовых мер в качестве охранных предприятий зачастую недостаточно, поэтому все больше организации применяют специальные системы программно-аппаратных и технических средств. Примером таких систем служат системы контроля и управления доступом (СКУД).

Безопасность определяет высокую степень защищенности и низкий уровень риска для людей и общества в целом, объектов или систем. Если рассматривать это состояние с точки зрения предприятия или организации, то оно затрагивает не только сотрудников, но и все объекты предприятия, сооружения, прилегающую территорию, а также информацию, являющуюся закрытой для третьих лиц. Основным методом обеспечения данного свойства является автоматизация системы безопасности.

Сегодня СКУД занимаются не только обеспечением безопасности на предприятии, но и выполняют много дополнительных функ-

ций: функцию учета рабочего времени с последующим расчетом заработной платы, ведение базы посетителей, интеграцию с другими системами предприятия (системой видеонаблюдения, охранной, пожарной и так далее) [6].

Сегодня применение СКУД объясняется не только нуждой в обеспечении безопасности. Кроме уже описанных выше основных целей, СКУД также занимаются выполнением ряда дополнительных, например:

- учетом рабочего времени (позволяют контролировать время входа\выхода сотрудников на предприятии и рассчитывать количество затраченного времени);
- интеграцией с системой бухгалтерского учета;
- ведением базы доступа к объектам (в том числе используется в сфере услуг для подсчета количества посетителей, зависимость числа от времени и других факторов);
- взаимодействие с системами безопасности (видеонаблюдение, охранная сигнализация, пожарная сигнализация, системы обеззараживания).

Проблема исследования. В соответствии с ГОСТ Р 51241-2008 системы контроля и управления доступом классифицируются по четырем признакам:

- способ управления;
- число контролируемых точек доступа;
- функциональные характеристики;
- уровень защищенности от НСД к информации [5].

Самый значимый признак классификации — первый. От выбора способа управления исполнительными устройствами в СКУД зависят во многом и выполняемые функции, и число охраняемых объектов и КПП. Часто и наоборот, предъявляемые к СКУД функциональные требования определяют способы взаимодействия. Итак, подобные системы делятся на централизованные, автономные и универсальные.

Первые применяются в больших организациях и на больших площадях. Их отличает то, что все контроллеры в такой СКУД соединены

в сеть и подключены либо к компьютеру, либо к главному контроллеру. Такой способ организации системы позволяет вести централизованный учет данных на одном сервере, а значит, и более быстрое составление отчетности или поиск информации в записях. Недостатком такой системы является, конечно, уязвимость сетевой архитектуры. То есть, если злоумышленник сможет проникнуть в сеть, то он сможет управлять всеми контроллерами. Именно поэтому на важных объектах сетевые СКУД проектируются и монтируются отдельно от других сетей. С другой стороны, включение СКУД в существующую сеть сильно экономит финансы предприятия.

Второй тип СКУД — автономные. Их часто еще называют «однодверными». Такие системы не требуют больших каналов связи, сети и так далее. Часто они состоят из некоторого запорного устройства, считывателя, контроллера, возможно, аварийной кнопки. Соответственно, недостаток таких систем в их ограниченной функциональности, так как они не могут ни учитывать рабочее время, ни вести журнал (в основном). Опять же, такие системы намного дешевле сетевых, поэтому очень популярны на небольших предприятиях, в том числе часто в школах. Дополнительный функционал их ограничен: можно встретить системы с GSM-модулем, они способны посылать уведомления по сети, иногда встречается связь с интернетом. В современных СКУД часто реализована функция «antipassback», т. е. карта работает сначала на вход, а потом только на выход.

Последний вид СКУД комбинирует в себе признаки предыдущих двух. Такие системы в основном работают так же в сетевом режиме с централизованной схемой, но при возникновении сбоев, отключении энергопитания и тому подобному переходят в автономный режим, что позволяет повысить надежность системы.

По второму признаку СКУД делятся:

- на системы с малой емкостью (менее 64 точек);
- системы со средней емкостью (до 256 точек);
- системы с большой емкостью (более 256 точек).

Логично предположить, что все автономные (однодверные) системы относятся к первому виду, так как функционируют отдельно друг от друга.

По функциональным возможностям СКУД делятся на системы с ограниченными возможностями, расширенными возможностями, и отдельно выделяются многофункциональные системы. По уровню защищенности от НСД к информации системы делятся на СКУД с нормальным, повышенным и высоким уровнем защиты.

Материалы и методы. Технологии проектирования, разработки, внедрения и использования СКУД во многом зависят от предприятия, для которой эта система разрабатывается. Для подобных систем определены основные принципы, которым необходимо следовать в работе:

- стоит уделять внимание минимизации элементов СКУД, то есть отдавать предпочтение, например, восьмипортовому коммуникатору вместо двух- четырехпортовых;
- предпочтительно разрабатывать систему для конкретного предприятия, с полным грамотно оформленным техническим заданием и учетом всех пожеланий заказчика;
- обязателен учет аварийных режимов работы системы, сбоев; следует обеспечить устройства резервным питанием, а в случае эвакуации предусмотреть открывание механизмов (для этого надежнее использовать нормально открытые защелки и замки);
- для обеспечения высокого уровня защищенности системы необходимо связывать ее компоненты в отдельную линию; включение системы в локальную вычислительную систему хоть и дает выигрыш в экономическом плане, но не обеспечивает безопасность на должном уровне;
- для обеспечения на объектах с большим потоком должной проходимости в СКУД-системах стоит использовать бесконтактные карты Proximity; остальные технологии либо не обеспечат защищенности, либо будут тормозить систему;

• использование систем, базирующихся на web-технологиях, оправдано на небольших предприятиях или в корпоративных системах, в которых информация по каждому из отделений должна быть доступна;

• при проектировании системы и подборе оборудования стоит учитывать предполагаемое количество пользователей и подбирать контроллеры таким образом, чтобы памяти устройств хватило на хранение данного числа ключей;

• при проектировании связей между элементами системы стоит учитывать особенности выбранных стандартов, например, стандарт RS-485 не приемлет разветвленную топологию, стандарт RS-232 работает на небольших расстояниях до 15 м.

В настоящее время довольно большое число компаний занимаются системами безопасности, куда входят и СКУД. Каждая из них зарекомендовала себя как специалист того или иного профиля, отличается своим качеством или же полностью обслуживает свой регион. Эти организации сегодня занимаются не только производством и продажей оборудования для систем безопасности, видеонаблюдения, пожаротушения и так далее, но и предоставляют комплексные услуги по проектированию и разработке таких систем, включая монтажные работы и дальнейшую поддержку. Примеров таких организаций достаточно: PERCo, Gate, BAS-IP, RusGuard, Parsec, Smartec, ITV, SmartScan, BioSmart, Болид.

Практически главное правило проектирования СКУД по мнению экспертов этой области [1] — проектирование под конкретную организацию. Они считают, что такие системы уникальны для каждого предприятия и должны проектироваться исходя из структуры организации и пожеланий заказчика.

В данном исследовании не стояла цель разработать СКУД под конкретного заказчика, наоборот, сделать прототип несколько универсальной системы (небольшой, автономной, с дополнительным функционалом) для создания в дальнейшем готового продукта и дальнейшей возможной его коммерциализации. Опять же, хорошо, если у такого продукта будет возможность интегрироваться в бо-

лее сложные сети. Поэтому в данном исследовании проектирование и моделирование ведется как для комплексной сетевой СКУД, а проектирование аппаратного и программного обеспечения описывается для прототипа автономной системы как задел на дальнейшее развитие.

Поскольку СКУД разрабатывается унифицировано, рассмотрим проектирование как для типового объекта.

Для того, чтобы перед проектированием системы понять структуру и связи ее процессов, проведем функциональное моделирование. Для моделирования была выбрана среда Microsoft Visio.

Субъектом данного моделирования является СКУД для типового объекта. Рассматривать систему будем с точки зрения оператора СКУД, с точки зрения поставщика СКУД.

Контекстная диаграмма позволяет увидеть по принципу «черного ящика» входную и выходную информацию для процесса Контроль и управление доступом. Также на диаграмме отображаются управленческие объекты и механизмы исполнения.

Для осуществления контроля и управления доступом входными потоками будут:

- заказ;
- идентификаторы карт;
- данные пользователей;
- структура и планы предприятия.

Выходными потоками являются:

- разграничение доступа;
- работа системы оповещения;
- ведение базы посетителей.

Потоки управления:

- законы и нормативные документы РФ;
- нормативные документы организации.

Механизмы исполнения:

- персонал организации;
- персонал обслуживающей компании.

Контекстная диаграмма представлена на рис. 1.

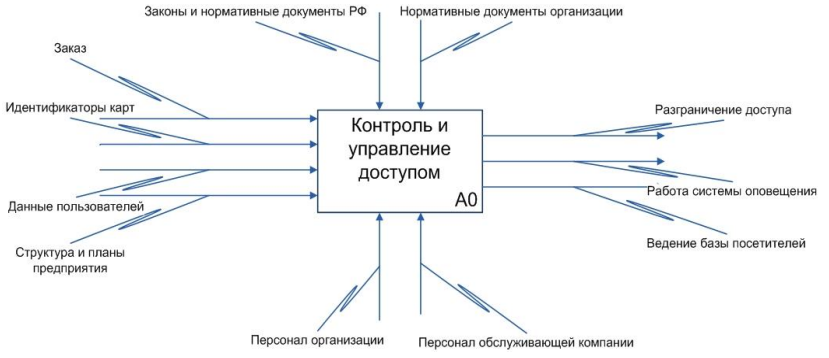

Рис. 1. Контекстная диаграмма

Описание вышеуказанных параметров представлено в табл. 1.

Таблица 1

Описание информационных потоков контекстной диаграммы

Объект	*Название*	*Описание*
1	*2*	*3*
Вход	1. Заказ 2. Идентификаторы карт 3. Данные пользователей 4. Структура и планы предприятия	1. Информация от организации, запрос на разработку СКУД, информацию о бюджете разработки, ТЗ. 2. Каждая из приобретенных бесконтактных карт имеет уникальный идентификатор, по которому в будущем в системе будут определяться права доступа к объекту. 3. Данные о пользователях системы, личные данные о пользователях, как о физических лицах, и данные о сотруднике. 4. Требующиеся для разработки проекта системы чертежи включаемых объектов, требуемая структура системы

Окончание табл. 1

1	*2*	*3*
Выход	1. Разграничение доступа 2. Работа системы оповещения 3. Ведение базы посетителей	1. Процесс определения прав доступа каждого идентифицирующегося пользователя к объекту и разрешение/запрещения доступа. 2. Отсылка оповещений о входе/выходе пользователя определенному адресату сообщения. 3. Логирование входов\выходов пользователей системы для ведение отчетности и ее дальнейшего использования
Управление	1. Законы и нормативные документы РФ 2. Нормативные документы предприятия	Правовое обеспечение системы
Механизмы	1. Персонал организации 2. Персонал обслуживающей компании	1. Служба охраны организации-заказчика, персонал организации. 2. Персонал компании, реализующей заказ

Заключение. Следует отметить, что идентификаторы карт могут не входить изначально в систему, а определяться после их закупки компанией-разработчиком или же заказчиком. Данная контекстная диаграмма показывает укрупненный процесс относительно разработки СКУД.

В современном мире системы безопасности имеют значимую роль во многих областях общества. Автоматизация процессов управления объектами в данных системах способствует высокой стабильности их работы. Необходимость перехода подобных систем на отечественные устройства обеспечивает импортозамещение и независимость от иностранных поставщиков, что так же приводит к повышению уровня безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Проектирование СКУД: эксперты советуют : [сайт]. — URL: http://www.secuteck.ru/articles2/sys_ogr_dost/proektirovanie-skyd-eksperti-sovetyut/ (дата обращения: 13.05.2022). — Текст : электронный.
2. НВП «БОЛИД» / О компании : [сайт]. — URL: http://bolid.ru/ about/ (дата обращения: 13.05.2022). — Текст : электронный.
3. НВП «БОЛИД» / Структурная схема ИСО «ОРИОН» : [сайт]. — URL: http://bolid.ru/production/orion/about-orion/orion_structurnaya_shema.html (дата обращения: 13.05.2022). — Текст : электронный.
4. Безопасность средств безопасности: СКУД : [сайт]. — URL: https://habrahabr.ru/post/277279/ (дата обращения: 13.05.2022). — Текст : электронный.
5. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. — Взамен ГОСТ Р 51241-98; введ. 2009-08-31. — Москва : Стандартинформ, 2009. — 31 с. — Текст : непосредственный.
6. Ворона В. А. Системы контроля и управления доступом : учебное пособие / В. А. Ворона, В. А. Тихонов. — Москва : Горячая Линия — Телеком, 2010. — 272 с. — Текст : непосредственный.
7. Платт Ч. Электроника для начинающих : пер. с англ. / Ч. Платт. — Санкт-Петербург : БХВ-Петербург, 2012. — 480 с. — Текст : непосредственный.

А. О. Третьяк, Я. А. Шенцов, Т. Ю. Чернышева

Тюменский государственный университет, г. Тюмень

УДК 004.031.2

МОБИЛЬНОЕ ПРИЛОЖЕНИЕ-ПОМОЩНИК ДЛЯ БОРЬБЫ С ЦИФРОВОЙ ЗАВИСИМОСТЬЮ

Аннотация. *В работе представлен ИТ-проект, его функционал и реализация. Также описано, как мобильное приложение помогает в борьбе с цифровой зависимостью. Для реализации проекта использован язык Kotlin. В качестве IDE — Android Studio. СУБД — SQLite.*

Ключевые слова: *цифровая зависимость, блокировка отвлекающих мобильных приложений, режим «Без телефона», продуктивность.*