

Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра математической  
кибернетики и компьютерных наук

**СИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ ГОСТЕВОГО СЕГМЕНТА  
БЕСПРОВОДНОЙ СЕТИ ГОСТИНИЧНОГО КОМПЛЕКСА**

**АВТОРЕФЕРАТ ДИПЛОМНОЙ РАБОТЫ**

студента 6 курса 611 группы

специальности 010501 – Прикладная математика и информатика

факультета КНиИТ

Харитонов Сергея Борисовича

Научный руководитель

к.ф.-м.н., доцент

\_\_\_\_\_

Иванов А. С.

Заведующий кафедрой

к.ф.-м.н.

\_\_\_\_\_

Миронов С. В.

Саратов 2016

**ВВЕДЕНИЕ.** Организации, осуществляющие деятельность в сфере услуг, должны предоставлять клиентам сервис определенного уровня, причем в перечень базовых элементов этого сервиса со временем включаются новые услуги, среди которых прочно закрепился гостевой доступ к сети Интернет. По соображениям удобства предоставления доступа в Интернет и, реже, к некоторым внутренним ресурсам информационной системы организации, чаще всего работа осуществляется по технологии Wi-Fi.

В связи с этим остро встает вопрос организации качественного, надежного и безопасного канала связи для недопущения недовольства клиентов и неавторизованного доступа во внутреннюю сеть компании. Стандарты построения беспроводных сетей постепенно устаревают, алгоритмы шифрования, используемые для защиты передаваемых данных, подвергаются компрометации, либо просто утрачивают стойкость из-за роста вычислительной мощности компьютеров.

Все перечисленные факторы обязывают рассматривать построение беспроводной сети организации как целый комплекс мероприятий, начинающийся с обследования помещений, внутри которых необходимо произвести работы, и заканчивающийся тонкой настройкой отдельных устройств, обеспечивающих функционирование как всей сети, так и отдельных её сегментов.

Не менее важным является вопрос организации централизованного управления учетными записями пользователей, имеющих доступ к создаваемой сети. Многие устройства, используемые для организации беспроводной сети, имеют встроенные механизмы авторизации и аутентификации пользователей, однако в контексте сети организации необходима интеграция с существующими решениями контроля учетных записей пользователей.

*Целью работы* является разработка системы управления доступом гостевого сегмента беспроводной сети гостиничного комплекса.

*Для этого требуется:*

- изучить требования заказчика;
- определить, с каким оборудованием предстоит работать;
- рассмотреть используемые в оборудовании стандарты и протоколы;
- предложить концепцию разрабатываемой системы;
- представить программную реализацию системы, которой мог бы

ежедневно пользоваться персонал гостиничного комплекса.

**1 Концепция системы управления доступом.** В главе приводится рассмотрение создаваемой сети с точки зрения устройств и используемых технологий, а также их применения в том виде, в котором они удовлетворяют требованиям заказчика.

**1.1 Требования заказчика.** Организация, занимающаяся гостиничным бизнесом, хочет организовать на территории гостиничного комплекса беспроводную сеть, работающую по технологии Wi-Fi, с помощью которой клиенты могли бы выходить в интернет со своих устройств. Комплекс состоит из трехэтажного здания гостиницы, двухэтажного отдельно стоящего SPA-салона и окружающей парковой зоны.

Гостиницу и SPA-салон необходимо полностью охватить зоной покрытия сети, в парковой зоне доступ к сети не нужен. Доступ к сети могут иметь только клиенты, которые заехали в гостиницу и зарегистрировались на рецепции. Решение о предоставлении доступа принимает администратор гостиницы, он же производит необходимые действия, выдавая новому клиенту учетную запись для доступа.

Требуется произвести радиообследование территории заказчика, разработать концепцию будущей системы управления доступом, подобрать необходимое оборудование и разработать программное обеспечение для ПК администратора гостиницы. По завершению внедрения системы требуется произвести обучение ответственного персонала гостиницы.

**1.2 Устройства, используемые для построения беспроводной сети.** В результате анализа требований заказчика к создаваемой сети и на основе начального радиообследования территории гостиничного комплекса было принято решение строить беспроводную сеть на основе оборудования фирмы Aruba. Из ассортимента предлагаемых решений были выбраны беспроводные точки доступа IAP-205 в количестве 14 штук (по три точки доступа на каждом этаже гостиницы, пять точек доступа в SPA-центре, располагающемся в отдельном здании). В качестве активного коммутационного оборудования были выбраны два коммутатора: S1500-24P (24-портовый) и S1500-12P (12портовый).

**1.3 Компоненты разрабатываемой системы и взаимодействие между ними.** Было принято решение установить сервер OpenLDAP для хранения информации об учетных записях клиентов гостиничного комплекса, которые они могли использовать для доступа к сети Интернет через гостевой сегмент беспроводной сети.

Логика работы системы следующая: администратор гостиницы регистрирует клиента при заезде, выдавая ему учетную запись, распечатанную на чековом принтере. Имя пользователя и пароль генерируются процедурно и заносятся на сервер OpenLDAP. При этом каждая учетная запись имеет срок действия, который совпадает со сроком бронирования номера в гостинице, либо какой-то срок действия по умолчанию, если точный срок отъезда клиента пока неизвестен.

При настройке беспроводных точек доступа в качестве механизма авторизации и аутентификации для гостевой сети указывается внешний сервер OpenLDAP. Когда клиент подключается к сети, он попадает на веб-страницу входа, где вводит предоставленные администратором логин и пароль.

Точка доступа, с которой ассоциировано клиентское устройство, осуществляет запрос на сервер OpenLDAP, по результатам которого либо выводится сообщение об ошибке в введенных учетных данных, либо

пользователь продолжает работу в сети согласно правилам фильтрации и ограничения скорости и количества трафика. Вся логика управления учетными записями закладывается в программный продукт, работающий на ПК администратора гостиницы: генерация учетных данных, задание срока действия учетных записей, удаление устаревших учетных записей. Там же ведется протокол работы системы и печать информации об учетных записях на чековом принтере для клиентов гостиничного комплекса.

Сервер OpenLDAP только обслуживает запросы точек доступа и выполняет роль хранилища. После рассмотрения существующих реализаций службы каталогов дадим обоснование выбора сервера OpenLDAP для использования в финальной версии системы управления доступом.

**2 Служба каталогов.** Службой каталогов называют программный комплекс, позволяющий управлять иерархической структурой информации о ресурсах компьютерной сети, контролировать их использование и применять ограничения доступа [2]. Первая служба каталогов, разработчиком которой являлась компания Banyan, появилась в 1984 году и называлась StreetTalk. Она была включена в состав системы управления предприятиями Banyan VINES. Система работала под управлением ОС Unix и позднее была переименована в Enterprise Network Services (ENS). В течение 80-х годов прошлого века международная организация International Telegraph and Telephone Consultative Committee разрабатывала общий стандарт для службы каталогов, называемый X.500. Его частью является протокол доступа DAP (Directory Access Protocol), однако в современных реализациях службы каталогов он используется в облегченном варианте из-за первоначальной всеобъемлющей функциональности, не нашедшей применения на персональных компьютерах, и называется LDAP (Lightweight Directory Access Protocol).

**2.1 Общее представление об элементах службы каталогов.** Как правило реализация службы каталогов состоит из базы данных, в которой размещены сведения о ресурсах информационной системы и серверного программного

обеспечения, предоставляющего механизмы доступа к этой базе. Для обеспечения отказоустойчивости и распределения нагрузки служба каталогов может быть установлена на несколько серверов.

Информация о ресурсах сети, хранящаяся в службе каталогов, обычно представлена в виде иерархической структуры, поскольку такое представление наиболее близко к реальной организационной модели большинства предприятий и организаций. В корне иерархии описывается предприятие в целом, а нижележащие уровни представляют подразделения и отдельные элементы. Такое структурированное представление ресурсов с уникальным в пределах сети именем называется доменом. Для обращения к информации в протоколе используется унифицированная схема адресации, либо собственная, либо совместимая со стандартными схемами.

**2.2 Обзор актуальных реализаций службы каталогов.** В подразделе рассматриваются особенности таких реализаций службы каталогов как NIS/YP, LDAP, Active Directory. Другие менее распространенные реализации упоминаются, но не подвергаются рассмотрению.

**2.3 Обоснование использования реализации OpenLDAP.** Выбор реализации OpenLDAP в системе управления доступом обусловлен в первую очередь наличием реализации службы каталогов, работающей по протоколу LDAP. Это наиболее универсальный и повсеместно используемый протокол, являющийся индустриальным стандартом. Также его выбор позволил избежать дополнительных трудозатрат при интеграции с беспроводными точками доступа, т.к. Aruba Instant OS поддерживает протокол LDAP.

Другим немаловажным фактором стали небольшие требования к аппаратным ресурсам. Выделение отдельного физического сервера избыточно для функционирования службы каталогов сети такого размера, как гостевая сеть гостиничного комплекса, а виртуальную машину с OpenLDAP можно развернуть

на любом гипервизоре, учитывая предпочтения заказчика и те решения, которые уже развернуты в организации.

С точки зрения итоговой стоимости проекта стоит отметить, что сервер OpenLDAP разворачивается под управлением GNU/Linux, что позволяет избежать затрат на лицензирование серверной ОС от Microsoft.

**3. Разработка ПО для ПК администратора.** Было решено разрабатывать программный продукт на языке Visual C# с использованием среды разработки Microsoft Visual Studio.

Стоит отметить, что помимо входящей в состав OpenLDAP-сервера консоли управления объектами с Web-интерфейсом существуют и отдельные программы для Windows и Linux с аналогичной функциональностью, но в рамках рассматриваемого проекта они не подходят, так как не имеют некоторых специализированных функций, необходимых для работы администратора гостиницы с системой управления доступом, а также требуют знания терминологии службы каталогов, что неприемлемо.

В главе приводится описание подготовительных работ по развертыванию сервера OpenLDAP и обеспечению его достижимости из гостевой сети и сети управления, проектирования графического интерфейса пользователя. Далее приводятся частичные листинги основных методов, вызываемых действиями пользователя, а также примеры содержимого файлов конфигурации и журналов с протоколом работы программы. Демонстрируется работа ПО с сервером OpenLDAP.

**ЗАКЛЮЧЕНИЕ.** В результате грамотного и всестороннего подхода удалось в полном объеме реализовать исходную концепцию системы управления доступом гостевого сегмента беспроводной сети гостиничного комплекса. Достигнута интеграция системы не только с построенной в соответствии со всеми требованиями заказчика беспроводной сетью, но и с существующей в организации IT-инфраструктурой.

Успешно проведенные пусконаладочные работы подтвердили исходную состоятельность выбранной концепции, представители заказчика высоко оценили и системный подход на всех этапах разработки системы, и тесное взаимодействие во время разработки со своевременным учетом всех возникающих дополнительных требований. Ответственный персонал гостиничного комплекса успешно прошел обучение и в короткие сроки освоил работу с разработанным в рамках проекта программным обеспечением, позволив гостиничному комплексу начать предоставлять более качественный и разнообразный сервис.

Произведенное положительное впечатление привело к желанию заказчика продолжить сотрудничество уже в рамках поддержки, дальнейшего улучшения и масштабирования реализованного решения.



## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Data sheet. Aruba Instant 205 / HP 205 Instant Access Point. URL: <http://www8.hp.com/h20195/V2/getpdf.aspx/c04692927.pdf?ver=1.0> (Дата обращения 19.05.2016), Загл. с экрана. Яз. англ.
2. Службы каталогов. Сетевые технологии. URL: <http://www.4stud.info/networking/directory-service.html> (дата обращения 17.01.2015), Загл. с экрана. Яз. рус. Последнее изменение страницы: 06.08.2013.
3. Руководство администратора OpenLDAP 2.4. URL: <http://proldap.ru/tr/admin24/> (дата обращения 20.01.2015). Загл. с экрана. Яз. рус. Последнее изменение страницы: 30.07.2015.
4. Введение в Active Directory. URL: <http://www.intuit.ru/studies/courses/1068/259/lecture/6608> (дата обращения 01.02.2015). Загл. с экрана. Яз. рус.
5. Настройка OpenLDAP и его взаимодействие с сетевыми сервисами. URL: <https://www.opennet.ru/base/net/openldap.txt.html> (дата обращения 09.02.2015). Загл. с экрана. Яз. рус. Последнее изменение страницы: 05.12.2005.