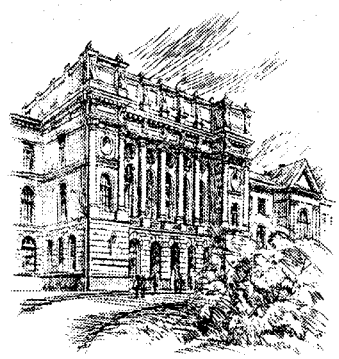
6 (69)/2008



Научно-технические ведомости СПбГПУ

Информатика
Телекоммуникации
Управление

Санкт-Петербург. Издательство Политехнического университета

Федеральное агентство по образованию
Санкт-Петербургский государственный политехнический университет

Журнал включен в "Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук".

Подписной индекс **18390** в каталоге "Газеты. Журналы" ОАО Агентства "Роспечать".

В данной статье изложена методика оценки пропускной способности сети мобильной связи стандарта CDMA2000 1X EV-DO при предоставлении услуг скоростной передачи данных, учитывающая влияние многих факторов. Данная методика может быть использована при планировании наложенной сети.

Как показали результаты анализа, большое влияние на пропускную способность оказывают сетевая загрузка и применение планировщиков каналов с более совершенными алгоритмами обслуживания.

Особое место в оценке параметров загрузки и качества предоставления услуг занимает средняя скорость, приходящаяся на абонента в прямом канале. Указанный фактор может говорить о необходимости увеличения пропускной способности сети в определённом районе зоны обслуживания.

СПИСОК ЛИТЕРАТУРЫ

1. **Голант Г. З.** Мобильный Интернет в сетях CDMA2000, под ред. Бабкова В. Ю. СПб: ИА "Энергомашиностроение", 2007, С. 137.

2. **Youngseok Lee**. Measured TCP Performance in CDMA 1x EV-DO Network, School of Computer Science & Engineering. Chungnam National University Daejon, Korea, 2006. P. 10.

3. **Choi E. H., Choi W., Andrews J. G.** Throughput of the 1x EV-DO System with Various Scheduling Algorithms. The University of Texas, USA, 2004. P. 5.

Дюгуров Д. В.

Принципы построения университетской сети с открытой инфраструктурой

Введение

Создание и рациональное использование общих вычислительных ресурсов – одна из важнейших задач информатизации в целом. Возможность масштабирования сетей, интеграции между собой уже созданных сегментов напрямую зависит от выбранных сетевых платформ. Особую актуальность эта проблема приобретает в профильных вузах. В данном случае учебному заведению необходимо решать сразу несколько задач:

подготовка специалистов (программистов, системотехников, специалистов по безопасности информации и пр.), зачастую в отрыве от реальных производств;

поиск источников финансирования;

соответствие технической базы требованиям времени;

обеспечение функционирования и развития IT отрасли в регионе.

Для этого учебное заведение должно обладать высококлассными специалистами из числа профессорско-преподавательского состава, "рабочей силой" – студентами и средствами разработки. Одним из таких инструментов должна быть распределенная сеть, состоящая из мощных вычислительных машин, адекватных им операционных систем и сред разработки. Использование такого комплекса позволит учебному заведению получать заказы, выполнять реальные проекты и погружать студентов в производственную среду без ущерба для учебного процесса и с огромной практической пользой.

В качестве решения перечисленных задач предлагается проект вычислительной сети вуза (на примере факультета информационных технологий и вычислительной техники Удмуртского государственного университета – УдГУ, имеющего компьютеры, серверные операционные системы Microsoft Windows Server 2003 SP2, клиентские операционные системы Windows XP Professional SP 2 и лицензионные средства разработки, распространяемые для высших учебных заведений). Масштабы данной сети сопоставимы с сетью крупного промышленного предприятия. Следует также отметить, что использование студентами лицензионного программного обеспечения, установленного на факультетских серверах, позволяет повысить культуру будущих специалистов и сократить количество ошибок в создаваемой ими продукции.

Наличие данного инструмента должно порождать особые содружества студентов. Так.

инициативные студенты, получая определенные заказы, могут формировать собственные команды, используя факультетскую сеть в качестве средства разработки. Образовав собственные компании после окончания вуза, они могут продолжать использовать университетскую сеть и ее ресурсы. В результате вокруг университета образуется бизнес-окружение, которое будет "потреблять" выпускников соответствующих специальностей и снабжать студентов практической работой, что является идеальным вариантом для вуза и высшего образования в целом. Это позволит университету участвовать в выгодных коммерческих проектах и повысит престиж преподавательской деятельности среди бывших студентов, обеспечивая тем самым воспроизводство кадров для университета.

Описанную выше сеть далее будем называть вычислительной сетью с открытой инфраструктурой. "Открытость" состоит в том, что студенты, обучающиеся или обучавшиеся в университете, могут использовать сетевые ресурсы для решения любых прикладных задач, им известно, как организована сеть, какие используются программные продукты и аппаратные средства. Вместе с тем часть данной сети непосредственно используется в учебном процессе как техническое средство обучения.

Существенным здесь является то, что "открытость" не является угрозой безопасности сети в целом. В большинстве случаев конфиденциальность информации о механизмах работы, об используемых протоколах, портах, способах аутентификации – это неотъемлемая часть безопасности сети. Рассекречивание данной информации сравнимо с компрометацией пароля старшего системного администратора: знание деталей сетевой иерархии позволяет взять под контроль всю сеть с удаленного компьютера, а речь о том, чтобы дать информацию о структуре факультетской сети студентам, вообще не ведется. На этапе первоначального функционирования вычислительной сети с открытой инфраструктурой ее безопасность обеспечивают встроенные стойкие алгоритмы аутентификации. В дальнейшем в систему безопасности можно вносить коррективы, используя предложения пользователей сети, обнаруживших в ней "узкие места". В этом механизме учтена и психологическая сторона вопроса: никому из пользователей не захочется сознательно портить или оставлять уязвимым инструмент, который он использует в работе.

1. Сеть с открытой инфраструктурой

Технически инфраструктуру ЛВС можно рассматривать с двух позиций. Первая (см. п. 1.1) – с точки зрения структуры объединения компьютеров в группы и связей групп между собой, вторая (пункт 1.2) – с точки зрения объединения внутренней сети и внешнего Интернета. Предположим, что корневым является домен второго уровня fitvt.ru, а поддомены adm.fitvt.ru, st.fitvt.ru, test.fitvt.ru – это административная, учебная и тестовая подсети соответственно. Однозначное соответствие элементов физической и логической инфраструктур сети в дальнейшем изложении позволяет использовать термины "подсеть" и "поддомен" как синонимы.

1.1. Внутренняя структура каждого из поддоменов состоит из одинаковых базовых элементов. При необходимости в каждом из поддоменов размещаются сервера со специфическими ролями. Общие части структуры поддоменов мы рассмотрим на примере st.fitvt.ru, а специфические серверные роли для каждой подсети описаны ниже. Схема поддомена st.fitvt.ru представлена на рис. 1.

Каждый из поддоменов содержит два контроллера домена (DC) с базой данных Активного катало-

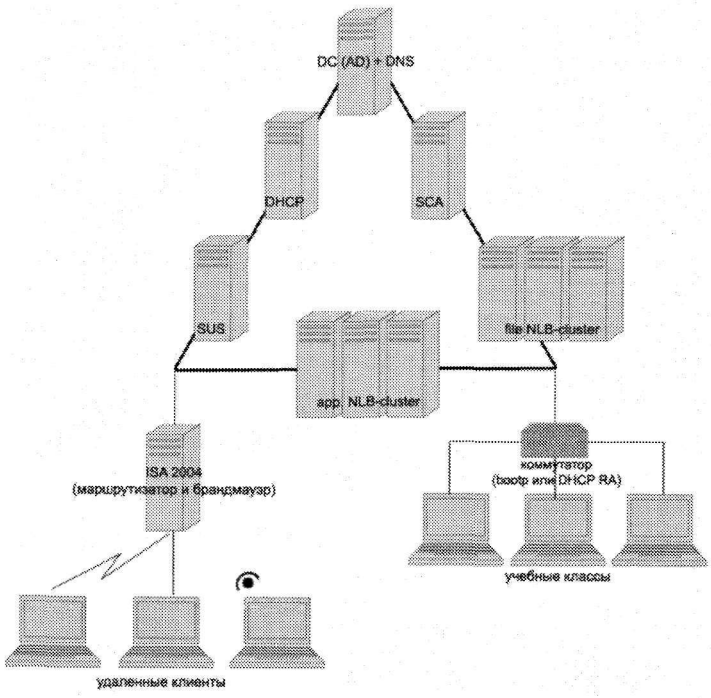


Рис. 1. Структура домена st.fitvt.ru

га (AD), один сервер разрешения имен (DNS), один DHCP-сервер, один Web-сервер, один подчиненный сервер сертификатов (SCA), один межсетевой экран (ISA), используемый для соединения подсетей друг с другом и с Интернетом. Роль DNS-сервера можно совместить с ролью контроллера домена. Это дает следующее преимущество: базу данных доменных имен можно синтегрировать в активный каталог и разрешить только безопасные обновления записей ресурсов в этой базе. Таким образом, только структуры (пользователи или компьютеры), прошедшие на контроллере домена проверку, смогут изменять записи доменных имен. Это безусловный плюс безопасности, который в принципе избавляет сеть от атак типа redirect.

Наличие DHCP-сервера обязательно лишь в студенческой и тестовой подсетях, в административной подсети надобности в этом сервере нет. В учебной подсети необходимы DHCP-ретрансляторы, так как все важные сервера сосредоточены в одном помещении, а маршрутизаторы по умолчанию не пропускают DHCP-трафик в удаленные сегменты. На Web-серверах размещаются внутренние сайты факультета, виртуальные каталоги и FTP-ресурсы студентов. Web-сервера развернуты на основе технологии IIS 6.0.

Подчиненный сервер сертификатов используется для выдачи сертификатов клиентским компьютерам и для аутентификации их на контроллере домена при подключении через VPN. Это особенно актуально для студенческой подсети, так как именно в ней таких подключений большинство. Также сервер сертификатов используется для выдачи технических сертификатов серверам подсети.

Брандмауэры устанавливаются во всех подсетях. Причем в студенческой подсети не предполагается наличие демилитаризованной зоны (DZ), а в остальных подсетях будут размещены два межсетевых экрана.

Необходимо учесть, что при большом числе VPN-подключений и Интернет-запросов один ISA-сервер не справится с работой, что вызовет неоправданные временные задержки в отображении Web-страниц и подключений к внутренним ресурсам сети. Для решения этой проблемы в студенческой подсети необходимо развернуть массив из двух-трех ISA-серверов, организованных как NLB-кластер с одним виртуальным ip-адресом.

Клиентские компьютеры во всех подсетях будут настроены как клиенты DNS, DHCP и Web-proxy одновременно. В каждой подсети будут развернуты сервера кэширования и автоматического обновления (SUS). Эти функции можно отдать ISA-серверу, если это не вызовет его перегрузку. Аппаратные брандмауэры и маршрутизаторы устанавливать не предполагается. В студенческой подсети необходим кластер серверов приложений, содержащий три-четыре компьютера с установленными на них лицензионными средами разработки и другими необходимыми средствами и кластер серверов баз данных. Все кластеры предполагается организовать на основе технологий NLB. В случае необходимости Web-кластер можно организовать, используя обыкновенные «зеркала» и настроив циклическую расстановку на серверах DNS.

Административная подсеть является копией учебной за исключением кластеров приложений и баз данных. Также в этой сети нет необходимости в массиве ISA-серверов и их настройке в качестве Web-proxy. Теоретически и в данной сети может возникнуть необходимость в DHCP-сервере, в случае если количество доступных на кафедрах портативных компьютеров резко возрастет. Внутренняя структура административного поддомена представлена на рис. 2.

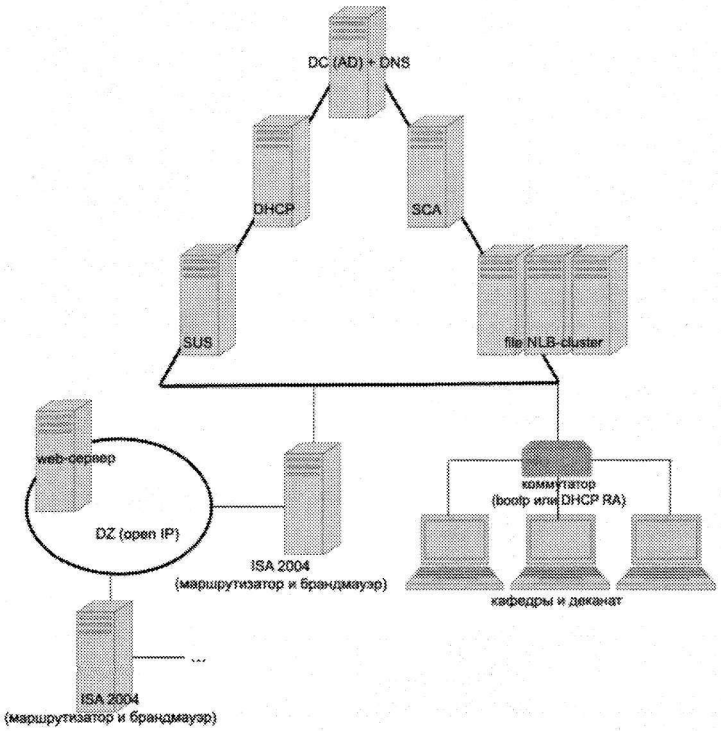


Рис. 2. Структура домена adm.fitvt.ru

Тестовая подсеть является копией студенческой подсети с той лишь разницей, что клиентских компьютеров мало, нет массива межсетевых экранов и кластера баз данных. Подчиненный сервер сертификатов тестовой подсети будет ограничен в возможностях: он будет выдавать сертификаты только для аутентификации в пределах подсети. Студенты-администраторы этой подсети не будут иметь административных полномочий на внешнем брандмауэре демилитаризованной зоны.

1.2. Предполагается разделить сеть на три части: внутреннюю, внешнюю и сеть периметра. Во внутренней подсети будут находиться административный и учебный поддомены, во внешней – пользователи Интернета и удаленные VPN-клиенты, в сети периметра – тестовый поддомен и контроллеры доменов студенческой и административной подсетей, находящихся в соответствующих демилитаризованных зонах.

Принцип разделения сети на зоны обусловливает определенное количество сетевых интерфейсов на ISA-серверах и контроллерах доменов. В ISA-серверах их должно быть не менее трех, а на контроллерах доменов – не менее двух. Это влечет определенные трудности при выборе стратегии ip-адресации, организации кластеров и обеспечении избыточности, учитывая произвол в предоставлении провайдерами внешних ip-адресов.

Для выдачи сертификатов подчиненным серверам в сети необходимо развернуть корневой сервер сертификации (RCA). Как базовый элемент системы безопасности сети он не будет входить ни в какие домены и устанавливается в отдельном помещении (желательно в сейфе). Доступ к нему должен быть только у старшего администратора сети. Этот сервер не подключается в корпоративную сеть факультета, а остается изолированным, выданные же им сертификаты должны устанавливаться на подчиненные сервера сертификации старшим администратором сети при помощи переносных носителей.

Схема сети представлена на рис. 3.

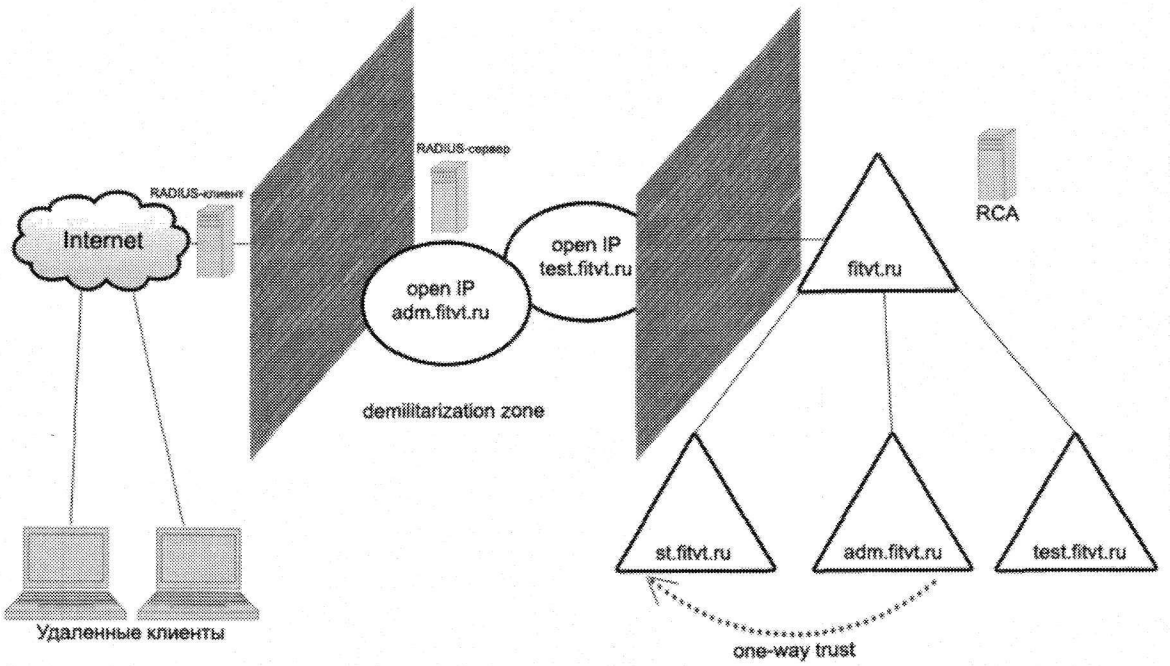


Рис. 3. Структура сети

Между административным и учебным поддоменом предполагается установить одностороннее доверие. В этом случае пользователи, прошедшие проверку на контроллерах административного поддомена, будут иметь доступ к ресурсам учебного поддомена без повторного опознавания, а пользователям учебной подсети нужно аутентифицироваться повторно при доступе к ресурсам административной подсети.

Межсетевые экраны оставляют настроенными по умолчанию, что означает, что все порты и все протоколы связи на первом этапе будут закрыты и запрещены. Открывают порты и устанавливают разрешающие правила для протоколов лишь по мере необходимости, после детального анализа исходящего сетевого трафика в поддоменах.

Для обеспечения отказоустойчивости на Web-серверах устанавливают аппаратные RAID-5

контроллеры и не менее четырех жестких дисков. Проводится также ежемесячная полная архивация контроллеров доменов, клиентских компьютеров административного поддомена, DNS-серверов, Web-серверов и серверов баз данных. Кроме того, планируется проводить разностные архивации указанных объектов в течение недели по установленному графику. Такая стратегия архивации требует большого количества свободного дискового пространства, но позволяет восстановить систему после сбоя за наименьшее время. Носители с архивами рекомендуется хранить в надежном, защищенном месте.

Обслуживает сеть команда администраторов. Роли каждого из них должны быть четко разделены. Во-первых, необходимо выделить группу администраторов поддоменов, у которых будут всеобъемлющие права доступа в пределах своих подсетей, затем создать группу операторов архива – они будут иметь возможность архивировать и восстанавливать систему после сбоя в пределах своих поддоменов, и наконец создать группу операторов серверов – они будут следить за производительностью серверных систем и оценивать показания счетчиков, сравнивая их с "базовой линией".

В сети должен быть один или два старших администратора, имеющих права полного доступа в пределах всей сети. Совмещать указанные должности крайне не рекомендуется.

Пользователи сети получают разрешения на доступ к объектам от администраторов своих поддоменов. По умолчанию при создании нового пользователя в активном каталоге для него создается папка профиля, выделяются места на Web-сервере согласно установленной квоте и даются разрешения на запуск необходимых программ. Остальные ресурсы сети остаются для него закрытыми, получить к ним доступ можно только по согласованию с администратором.

Стратегия ip-адресации, правила архивирования, квалификационные требования к администраторам серверов и членам других сервисных групп, разрешающие правила брандмауэра, квотирование дискового пространства и прочие элементы безопасности должны быть утверждены в форме единого документа приказом декана и соблюдаться неукоснительно.

2. Концепция региональной информатизации

В настоящее время федеральная программа информатизации предусматривает подключение школ к Интернету, наличие сайтов министерств и ведомств и другое, но не дает рекомендаций и пояснений по поводу каналов подключения, хост-машин и прочей технической составляющей процесса.

Необходимо разработать стандарт, предусматривающий внутреннюю и внешнюю структуры вычислительных сетей в бюджетных организациях в зависимости от их типа, и принять законодательный акт, делающий такую структуру официальной.

Разработку технической документации для школ, больниц и прочих учреждений необходимо предоставить специалистам, высшие же учебные заведения, готовящие соответствующих профильных специалистов, в состоянии разработать такие проекты сами и представить их на утверждение в министерство образования. Вычислительная сеть с открытой инфраструктурой на базе факультета ИТиВТ УдГУ является первым таким проектом.

Ключевое звено системы – полноценный домен (не сайт и не портал!) факультета, зарегистрированный во всемирной сети Интернет и размещенный на собственной хост-машине, обслуживаемой собственными администраторами.

Сети на базе серверных продуктов Microsoft легко интегрируются друг с другом, поэтому после организации сетей на основе доменов в различных учреждениях объединение их в единый домен – дело времени и договоренности с балансодержателем внешних региональных сетей связи. Единые сети позволят создать резервные централизованные хранилища информации, такие как общие библиотечные фонды, записи банковских операций, различные реестры и кадастры, организованные в едином формате и обслуживаемые единообразно.

Стойкость алгоритмов шифрования и ЭЦП, используемых для аутентификации пользователей и компьютеров, реализованное Microsoft, полностью соответствуют североамериканским и западноевропейским стандартам безопасности и вполне могут быть приняты в качестве региональных или федеральных стандартов в России.

Разграничение прав доступа на основе ролей, групповой принадлежности и файловой системы – наиболее гибкий метод из всех возможных. Применение его в вычислительной сети с открытой инфраструктурой позволяет не только легко управлять имеющимися и создавать новые типовые объекты безопасности, но и без дополнительных транзакций удалять объекты безопасности из каталога. К примеру, при должной интеграции автоматизированной системы управления университетом и домена с активным каталогом удаление

сотрудника из каталога при его увольнении автоматически запретит доступ его учетной записи к общим объектам и т. п.

Использование таких сетей в высших учебных заведениях позволит внедрить электронный студенческий билет и зачетную книжку – пластиковую карту с фотографией студента, на магнитной полосе которой будет записана информация о прослушанных курсах, экзаменационных отметках, ежедневных опозданиях и взятых в библиотеке книгах. Подобные пластиковые карты можно ввести и для преподавателей: они могут являться ключами к аудиториям, защищенным компьютерам, по ним можно получать льготу при путешествиях, посещениях музеев федерального значения и т. д.

Безусловно все это возможно только в случае принятия соответствующих нормативно-правовых актов и должного финансирования проводимых работ. Проект организации ЛВС с открытой инфраструктурой является базовым и ставит своей целью не только организацию учебного процесса, но и возможность показать жизнеспособность данных систем на практике. В этом проекте предпочтение продуктам Microsoft было отдано по следующим причинам:

разрабатывать собственную систему накладно, к тому же это приводит к несовпадению форматов выходных данных в разных системах;

добиться схожих результатов можно также при помощи бесплатных операционных систем и платформ, но это было бы нецелесообразно, поскольку Удмуртский университет является академическим партнером Microsoft.

В этой связи нельзя не отметить работу Microsoft в области упрощения инструментария настройки и лояльную политику по отношению к вузам в части цен на программные продукты. Гибкость, масштабируемость, безопасность, контролируемость, адекватность – неоспоримые преимущества ЛВС на базе продуктов Microsoft перед аналогами.

СПИСОК ЛИТЕРАТУРЫ

1. Блэк Ю. Сети ЭВМ: протоколы, стандарты, интерфейсы. М.: Мир, 1990. 510 с.

2. Макин Дж., Маклин Й. Внедрение, управление и поддержка сетевой инфраструктуры Microsoft Windows Server 2003. М.: Русск. редакция, 2004. 594 с.

3. Брэгг Р. Безопасность сети на основе Microsoft Windows Server 2003. М.: Русск. редакция, 2005. 632 с.

4. Рэтлиф Б., Баллард Дж., Microsoft ISA Server 2004. М.: Русск. редакция, 2006. 382 с.

5. Непейвода Н. Н. Сообщество открытого софта как реализация принципов анархизма // Тр. Первой конференции свободного программного обеспечения в высшей школе. Переславль Залесский, 2006. С. 19, 20.

Хромов В. В., Есипов А. В.

Оценка вероятностно-временных характеристик класса алгоритмов передачи данных по каналу с независимыми ошибками

В настоящее время для передачи информации в каналах низкого качества активно применяются протоколы, предусматривающие синхронный прием повторений канального кадра с последующим мажоритарным исправлением искаженных символов. Информация, подлежащая передаче – шифроблоки системы шифрования с закрытым ключем. Сообщение состоит из N таких блоков, значение N может варьироваться от одного блока до нескольких десятков. Протокол обеспечивает высокую помехоустойчивость, однако остается открытым вопрос о его надежности. Угрозу создает возможность того, что информация, подвергшаяся в канале искажению, может быть признана истинной. В работе предлагается методика расчета вероятностно-временных характеристик приема и оценка информационной безопасности протокола через вероятность ложного приема.

Алгоритм передачи данных. Одним из важнейших этапов выбора протокола передачи является определение способа кадровой синхронизации. Известны три способа кадрирования [3]: знаковое, битовое кадрирование с флагом и кадрирование с указанием длины кадра в поле заголовка. Каждый из этих способов имеет свои достоинства и недостатки. В решаемой нами задаче предлагается