Д. М. Левинсон

# Аудит информационной системы ЗАО «Челябинск-Восток-Сервис»

Научный руководитель: к.ф.-м.н. В. Н. Юмагужина

Аннотация. В статье описывается аудит информационной системы ЗАО «Челябинск-Восток-Сервис». Представлены обзор, выводы и рекомендации по структуре данного предприятия.

## 1. Введение

В каждой компании имеется три политики безопасности: одна зафиксирована на бумаге, вторая хранится в головах сотрудников, а третья непосредственно реализуется в сети. Цель аудита безопасности — объединить их и сохранить в этом состоянии. Оценка безопасности представляет собой тщательный анализ текущего состояния компании в отношении безопасности информации. Оценка — это не аудит; последний проводится для проверки соответствия имеющимся политикам и представляет очень подробное рассмотрение конкретной системы или сети. Аудиты безопасности периодически выполняются, чтобы сопоставить используемые методы работы с политикой безопасности компании и убедиться, что ожидаемые результаты достигнуты и меры безопасности эффективны. Аудиты безопасности можно планировать заранее с уведомлением, либо проводить их в форме имитации нештатных ситуаций для моделирования определенных событий. При проверке сети и связанной с ней инфраструктуры следует учесть несколько моментов. Наиболее важным из них является определение того, к чему есть доверие, и к чему доверия нет. Системы и службы, рассматриваемые как доверенные, представляют собой наиболее вероятные объекты незаконного проникновения и использования, так как объекты, не пользующиеся доверием, блокируются согласно установленным категориям. Если посмотреть на все в общем плане и понять, каким образом относятся друг к другу различные службы, можно предугадать вероятные пути атак. Аудитору приходится мыслить как хакеру, в то же время думая о стратегии

обеспечения безопасности. Это довольно трудная задача — вроде игры в шахматы с самим собой. Аудит безопасности — это детальная проверка состояния безопасности сети в сравнении с целями и задачами, определенными в политике безопасности. Его цель — проверить, что в информационной системе компании используются методы, соответствующие авторитетным рекомендациям, а также определить методы ведения бизнеса и технические уязвимости, подвергающие сеть опасности простоя, разглашения, потери конфиденциальной информации или повреждения данных. Полномасштабный аудит безопасности предусматривает проверку следующих факторов:

- **Избыточность.** Вся сеть может выйти из строя, если один из ее центральных компонентов даст сбой. Надежность сети повышается посредством установки избыточных каналов связи и оборудования.
- **Многоуровневая защита.** Сеть необходимо защищать от внешних атак одним уровнем защиты — межсетевым экраном, на котором установлено новейшее ПО. Второй уровень защиты от нецелевого использования или сетевых атак реализуется посредством установки ПО обнаружения вторжений как на межсетевом экране, так и на системах электронной коммерции.
- **Физическая безопасность.** Сетевые устройства и жизненно важные серверы должны размещаться в запираемых помещениях, и доступ к ним должен строго контролироваться.
- **Удаленный доступ.** Соединения виртуальных частных сетей (VPN) гораздо эффективнее с точки зрения стоимости и безопасности, чем доступ через телефонные линии и даже чем подключения к удаленным офисам. Они также позволяют дистанционным пользователям и специалистам по эксплуатации осуществлять доступ к сети через защищенный канал, обеспечивающий безопасность их паролей и полномочий доступа.
- **Корпоративная политика безопасности.** Корпоративная политика безопасности должна удовлетворять деловым целям компании, должны быть назначены руководящие сотрудники, ответственные за реализацию и доведение этой

политики до всех сотрудников. Она обновляется по мере изменения деловой среды. Также может быть назначен сотрудник, ответственный за отношения с партнерами по бизнесу, производителями и поставщиками с полными правами и ответственностью, а также с правом принятия решений по управлению объектами, связанными с информационными ресурсами компании. Оценка безопасности может проводится в семи пересекающихся областях.

- **Интернет-безопасность.** Каким образом осуществляется управление и мониторинг внешних соединений?
- **Безопасность взаимоотношений между компаниями.** Каким образом осуществляется управление взаимоотношениями с клиентами и партнерами?
- **Безопасность внутренней сети.** Каким образом контролируется доступ внутри организации?
- **Предотвращение внештатных ситуаций и восстановление системы безопасности.** Какие шаги предпринимаются для предотвращения прерывания обслуживания жизненно важных систем?
- **Управление информационной безопасностью.** Каким образом осуществляется управление внутренними политиками и процедурами для обеспечения эффективности безопасности?
- **Управление персоналом в рамках обеспечения безопасности.** Каким образом осуществляется управление персоналом для обеспечения эффективности безопасности?
- **Средства контроля физического доступа.** Защищены ли жизненно важные информационные системы с физической точки зрения так же хорошо, как и с электронной?

Аудит безопасности помогает лучше понять угрозы и выявить уровень эффективности текущей защиты информационной системы. Результаты аудита должны быть представлены в подробном виде, чтобы руководство могло принять решения по улучшению контроля над рисками без дополнительных финансовых расходов. Успешный аудит безопасности предусматривает выполнение следующих задач:

- Определяется подверженность системы внешним атакам (например действиям хакеров из Интернета или несанкционированному доступу к модемам, факсимильным аппаратам и голосовой почте).
- Определяется подверженность внутренним угрозам, включая случайное и умышленное нецелевое использование.
- Проводится сопоставление политики безопасности с реально применяемыми в организации подходами к ее обеспечению. Если политика безопасности отсутствует, аудит поможет определить области, которым необходимо уделить внимание. В данном случае аудит называется оценкой.

В большинстве случаев тщательный аудит обнаруживает области, для которых теоретические положения и реальное состояние не совпадают. Для объектов, в которых наблюдается такое соответствие и которые удовлетворяют авторитетным рекомендациям, аудит обеспечивает проверку инфраструктуры безопасности компании и используемых подходов к ее обеспечению. Аудит безопасности сначала определяет, каково должно быть положение дел согласно используемым в данный момент подходам и рекомендациям, затем раскрывает непосредственное практическое положение дел, после чего сравнивает полученные данные с авторитетными рекомендациями. Процесс аудита состоит из трех этапов:

- Обзор имеющихся политик информационной безопасности и процедур в сравнении с авторитетными рекомендациями.
- Исследование применяемых на практике операционных процедур, включая диалоги с сотрудниками, инспекцию сайтов, а также сканирование внутренней и внешней сетей.
- Выявление уязвимостей и предоставление рекомендаций по их устранению.

Результаты правильно проведенного аудита безопасности должны включать:

- Отчет исполнительного директора, содержащий оценку безопасности организации и акцентирующий внимание на проблемах.
- Технический отчет, содержащий схему сети, результаты детализированного анализа уязвимостей, сгруппированные по серьезности, включая описание каждой уязвимости и конкретные инструкции по их устранению, а также сравнение

с авторитетными рекомендациями политик и процедур организации для рассмотрения этих вопросов в свете целей и задач бизнеса.
- Сопоставление текущих методов и подходов к работе с официальными политиками и авторитетными рекомендациями с рекомендациями по совершенствованию, распределенными по категориям согласно степени серьезности и потенциального ущерба.

Аудит безопасности может обнаружить уязвимые места системы:

- Межсетевые экраны, на которых установлены разные версии ПО или уровни обновления.
- Проблемы с ресурсами для межсетевых экранов.
- Сотрудники, устанавливающие личные веб-сайты.
- Внутренние узлы, открытые для воздействия из Интернета.
- Соединения с внешней сетью без аутентификации или контроля доступа.
- Проблемы, связанные с действием вирусов.
- Риски, связанные с резервным копированием, и вопросы контроля над изменениями.
- Администрирование и управление безопасностью.
- Удаленные мошеннические действия.
- Опасности нарушения физической защиты.
- Пиратское или нелегальное ПО.
- Программы по обмену мгновенными сообщениями.
- Клиенты распределенных сетей (P2P) и нарушения авторских прав.

Методы аудита включают беседы с сотрудниками, изучение файлов журналов и анализ уязвимостей посредством соответствующих программ, не использующих какие-либо средства взлома или атаки на отказ в обслуживании (DoS). Кто проводит аудит? Без участия независимой стороны есть риск ложного чувства защищенности в некоторых областях, умышленного игнорирования уязвимостей или негласных допущений, о которых может не знать руководство. С помощью стороннего аудитора можно получить большую пользу. Чтобы подготовиться к аудиту, можно выделить время для взаимодействия с ключевым персоналом, посоветоваться с аудитором и получить у сетевых администраторов схемы сети и данные о конфигурации устройств. В небольших компаниях аудит безопасности может

занять всего пять дней (два дня на исследования информационной среды, один — на проведение сканирования и анализа уязвимостей, и еще два — на экспертный анализ и составление отчетов). В более крупных компаниях он занимает больше времени. Аудит должен проводиться настолько часто, насколько это установлено правилами, так как с модификацией конфигурации изменяется инфраструктура. По прошествии недель или месяцев аудит может быть недействителен из-за изменений в информационной среде. В небольших компаниях достаточно проводить аудит раз в год, в то время как в более крупных организациях он необходим аудит раз в месяц. Также важно, чтобы результаты аудита принимались в расчет в периоды между проведением аудитов. Можно ли назвать аудит тестом на проникновение? Нет. Тест проникновения подразумевает использование хакерских утилит для проведения попыток получения доступа к системам через их известные уязвимости. Аудит — это процесс, сфокусированный на деловой среде предприятия, окружающей компьютерные системы; он включает сканирование сети, не предусматривающее попыток получения доступа к системам. При этом не должна нарушаться работа служб и данные не должны подвергаться риску. Тест проникновения может проводиться отдельно, но только после получения результатов аудита и выявления и исправления всех возникших неполадок. В результате аудита безопасности следует представить результаты в удобочитаемом формате, а также план действий, направленный на упрощение разработки новых проектов по устранению обнаруженных неполадок [1].

## 2. Постановка задачи

Цели и задачи аудита ИТ:

- Обследование существующей IT-инфраструктуры.
- Формальное описание существующей IT-инфраструктуры.
- Составление перечня аппаратного и программного обеспечения.
- Объединение имеющейся в наличии документации.
- Проведение анкетирования сотрудников.
- Обследование информационной структуры.
- Составление списка отсутствующего оборудования.
- Выявление проблемных мест в информационной сети.

- Сбор информации, жалоб и пожеланий от конечных пользователей по работе компьютеров, сети, оргтехники и программного обеспечения.
- Описание выявленных проблем в виде списка возможных рисков для бизнеса и предложение по их предупреждению.

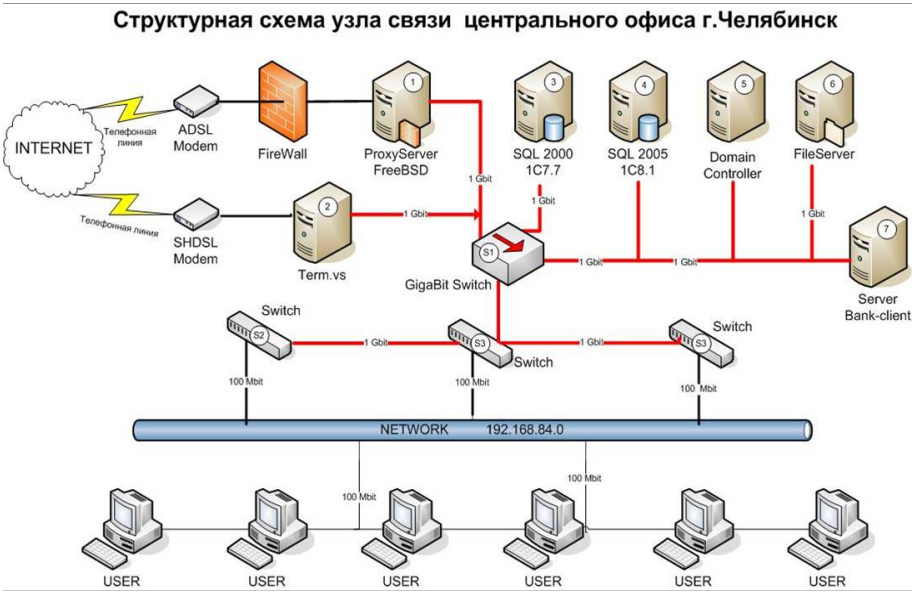


Рис. 1. Структурная схема узла связи центрального офиса г. Челябинск

## 3. Методы

### 3.1. Текущее положение системы ИТ. Обзор системы

Аудит информационной системы компании был проведен в период с 19.02.2008 по 22.02.2008. В результате проведенного осмотра информационной системы компании ЗАО «Челябинск-Восток-Сервис» были выявлены следующие структурные особенности:

- Распределенная сеть филиалов в городах Челябинской области.

- Распределенные информационные базы данных 1С v.7.7 и v.8.1.
- Центральный офис в г. Челябинске. Структурная схема узла связи представлена на рис. 1.
- Обособленное подразделение в г. Москве.
- Центральный склад г. Челябинске.
- Магазины в г. Челябинске.
- Использование технологий Microsoft Active Directory.
- Использование Интернет-технологий для информационного обмена.

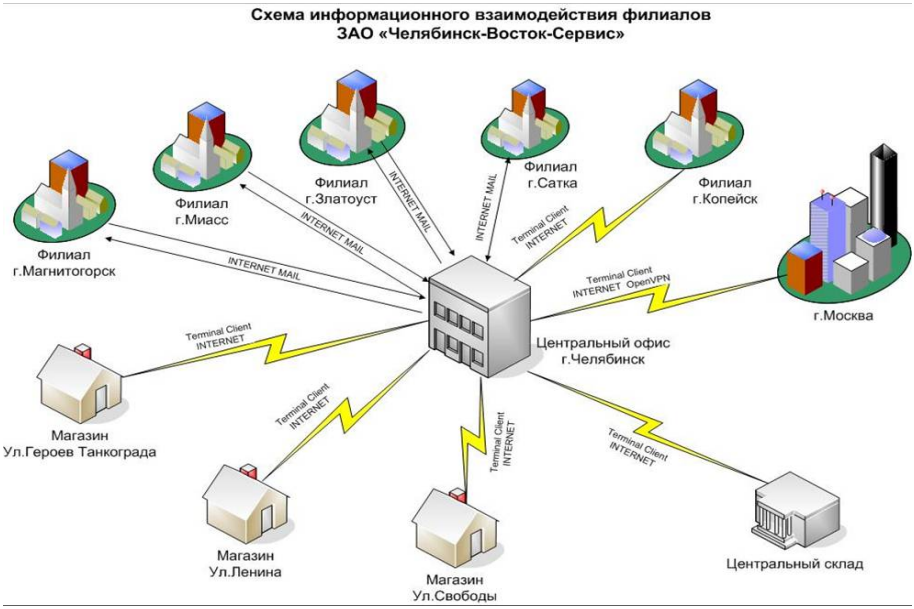


Рис. 2. Информационное взаимодействие филиалов ЗАО «Челябинск-Восток-Сервис»

## 3.2. Информационная структура компании

- **Центральный офис** — г. Челябинск ул. Потемкина 34-а.
- **Магазины** в г. Челябинске:
  (1) ул. Героев Танкограда 55;

(2) пр. Ленина 23;
(3) ул. Свободы 88.

- **Центральный склад** в г. Челябинске.
- **Филиалы в городах** (схема информационного взаимодействия представлена на рис. 2):
  (1) г. Магнитогорск;
  (2) г. Миасс;
  (3) г. Златоуст;
  (4) г. Сатка;
  (5) г. Копейск.
- **Обособленное подразделение** в г. Москва.

### 3.3. Описание серверной комнаты

- Серверная комната находится на 2 этаже центрального офиса.
- Общая площадь комнаты 8 кв.м.
- Количество рабочих мест — 2 (ведущий системный администратор, помощник системного администратора).
- На правой стене от входа установлена миниАТС Panasonic.
- В комнате находится 7 серверов и две рабочии станции.
- Коммуникационное оборудование расположено в навесном шкафу 8U на высоте 1 метр от поверхности пола.
- Каждый сервер подключен к отдельному бесперебойному источнику питания. Общее число BackUPS фирмы APC–7 шт. Мощность от 300 до 500 Ватт.
- В комнате расположен один основной ввод 220 Вольт. Также проведен дополнительный ввод 220 Вольт, который не задействован.
- В комнате имеется окно и кондиционер.
- Напольное покрытие — линолеум.
- В комнате присутствует неорганизованный склад оборудования.

### 3.4. Описание организации доменной структуры предприятия

Информационная сеть компании построена на основе технологии Microsoft Active Directory. Название домена — VS. Основной контроллер домена — PDC.VS - на основе Microsoft Windows Server 2003. PDC.VS является держателем пяти основных ролей Active Directory:

- PDC Master.
- Domain Name Master.
- Global Catalog.
- Schema Master.
- Infrastructure Master.

Домен находится в режиме Mixed Mode для обеспечения совместимости с серверами Windows 2000. Реплики AD присутствуют на 7 серверах, членах домена. В каталоге Active Directory, на текущий момент:

- 89 пользователей;
- 45 групп безопасности;
- 20 организационных контейнеров.

| Сервер | Операционная система | Доменное Имя IP адрес | Назначение | Основные Службы | Установленные программы |
|---|---|---|---|---|---|
| 1 | FreeBSD 6.0 | Не в домене<br>192.168.84.1 | 1. Основной сетевой шлюз<br>2. Прокси-сервер доступа в Интернет<br>3. FTP сервер, SSH | Squid, OpenVPN natd, ipwf, ftpd SSH | MC, OpenVPN |
| 2 | Windows 2003 Server Ent Eng SP2 | Term.vs<br>192.168.84.6 | 1.Основной терминальный сервер<br>2. Система ГАРАНТ | Terminal service HASP driver | 1C7.7<br>1C8.1<br>The BAT<br>HASP |
| 3 | Windows 2003 Server Ent Eng | Server2.vs<br>192.168.84.8 | 1.SQL 2000 Server для 1C7.7<br>2. Файловый сервер 1C7.7<br>3. Antivirus Server<br>4. Почтовый сервер | SQL 2000 Kaspersky Antivirus | 1C8.0<br>1C8.1<br>HASP, Kaspersky Server |
| 4 | Windows 2003 Server Ent Eng SP2 | SQL.vs<br>192.168.84.7 | 1. SQL 2005 Server для 1C8.1 | SQL 2005 HASP 1C8.1 агент | 1C8.1<br>Net.FrameWork 2.0 |
| 5 | Windows 2003 Server Ent Eng SP2 | PDC.vs<br>192.168.84.2 | 1.Основной контроллер домена VS<br>2. DNS<br>3. DHCP<br>4. WINS | Kerberos key DNS DHCP HASP | HASP driver |
| 6 | Windows 2003 Server Ent Eng SP2 | File.vs<br>192.168.84.5 | 1.Файловый сервер для профилей пользователей<br>2. Файловый сервер архивации | FileShare | HASP driver |
| 7 | Windows 2000 Server ENG SP4 | Server.vs<br>192.168.84.9 | 1. Сервер клиент-банк | MySQL КриптоПРО | Клиент-Банк MySQL |

Рис. 3. Функциональное назначение серверов

Задействованы групповые политики безопасности. Доверительные отношения с другими доменами отсутствуют. Функциональное назначение серверов представлено на рис. 3.

### 3.5. Описание типовой рабочей станции центрального офиса компании

- Операционная система Windows XP PRO Russian.
- Рабочая станция является членом домена VS.
- Компьютер, при подключении к сети, автоматически получает IP, DNS и Gateway с сервера DCHP PDC.VS, срок аренды 2 недели.
- Пользователь имеет ограниченные права на использование компьютера.
- Установлено следующее программное обеспечение:
  - 1С Предприятие 7.7 , 8.0, 8.1.
  - Open Office 2.3.
  - 7zip 4.58.
  - Антивирус Kaspersky 6.0.
  - Adobe Acrobat Reader 7.0.
  - FAR manager v.1.75.
- В бухгалтерии, при входе в домен, на компьютер применяется доменная групповая политика безопасности. Папки «Мои Документы» и «Рабочий стол» пользователя являются «перемещаемыми» и хранятся на файловом сервере File.VS.
- В соответствии с групповой политикой безопасности, через 42 дня пользователь обязан поменять пароль входа в домен, причем пароль должен быть сложным (7 символов минимум, заглавные и прописные буквы, спецсимволы).

## 4. Результаты

### 4.1. Достоинства системы ИТ и положительные моменты

(1) Использование технологий Microsoft Active Directory.
(2) Применение доменных групповых политик безопасности (перенаправление пользовательских папок, смена пароля).
(3) Ежедневное архивирование состояние системы на серверах Term.vs, SQL.vs, File.vs.
(4) Администраторы при выполнении административных функций используют личные учетные записи с соответствующими правами.
(5) Центральный склад, магазины и филиал в г. Копейске работают с базой 1С в оперативном режиме используя терминальный доступ.

(6) Использование гигабитных линий связи между всеми серверами и коммутаторами.
(7) Ограниченные учетные записи пользователей. Стандартизированное программное обеспечение рабочих станций с использованием бесплатных программ.
(8) Использование технологии зеркалирования RAID 1 на серверах Server.vs и Server2.vs для обеспечения сохранности данных.
(9) SQL 2000 Server установлен на специализированном сервере. Это повышает быстродействие и время отклика базы данных 1С7.7 [2].
(10) Для филиалов в г. Магнитогорск, Златоуст, Сатка, Миасс задействована технология информационного обмена УРБД фирмы 1С. Данная технология обмена не зависит от скорости канала обмена информацией.
(11) Функциональное распределение ролей серверов. Выделение терминального сервера, серверов баз данных, файловые сервера.
(12) Использование в качестве защитного барьера между локальной сетью и Интернет операционной системы FreeBSD v.6.0. Данная система отличается повышенной стабильность работы и устойчивость к взломам извне [3].
(13) На серверах Windows 2003 Server установлены последние обновления в виде Service Pack 2.
(14) Доступ к ресурсам Интернет ограничен и возможен только по выданному администратором имени и паролю. Имя и пароль отличаются от доменного.
(15) Архивированием баз данных 1С занимается администратор баз данных. Так же на него возложены обязанности информационного обмена между базами 1С 7.7 и 8.1.

## 4.2. Недостатки системы ИТ

(1) Отсутствие коммуникационного шкафа для оборудования. Отсутствие кроссовых панелей. Сервера расположены на полу. Силовые провода расположены хаотично с проводами линии связи.
(2) В комнате недостаточно свободного места. Рабочие места не соответствуют нормам СНИП.

(3) Все сервера запитаны от одной розетки 220 Вольт (!). Источники Бесперебойного питания стоят на полу. Каждый сервер подключен к своему источнику.
(4) Отсутствует в розетке заземление (!). Это может привести к выходу оборудования из строя, поражение электрическим током персонала.
(5) Модем SHDSL висит (!) на входящей линии связи. Это может привести к обрыву связи с центральным складом в любой момент времени.
(6) В качестве основных серверов используются офисные компьютеры. Это снижает надежность системы в целом, т.к. офисные компьютеры не обладают необходимым запасом прочности и надежности.
(7) Напольное покрытие в серверной комнате — линолеум — источник образования статического электричества, опасного для компьютерной техники.
(8) Провода компьютерной связи, проложенные до конечных пользователей не соответствуют стандарту СКС (Структурированные Кабельные Системы). В серверной комнате наблюдается огромное количество проводов сращенных методом «скрутки»(!). Такая же ситуация наблюдается и во многих кабинетах пользователей. «Скрутка» линий цифровых сигналов — источник помех, ошибок в приеме и передаче сигнала. Особенно это не допустимо на линиях 1000 Mbit.
(9) Отсутствие резервных каналов связи с удаленными офисами, магазинами и центральным складом. Обрыв телефонных линий (вне здания) может прервать информационный обмен на неопределенное время. Так же будет отсутствовать интернет и электронная почта.
(10) УРБД 1с технология обмена не позволяет в реальном времени отслеживать изменения в базах данных.
(11) Отсутствие антивирусной защиты на сервере FreeBSD. Для вирусной атаки данный сервер абсолютно прозрачен и вредоносный код достигнет конечного пользователя.
(12) Антивирус установлен только на одном сервере (!). Для установленного антивируса истек срок лицензии. Антивирусные базы не пополняются.

(13) Антивирус Касперского 6 установлен на MS SLQ 2000 Server. Данный продукт антивируса замедляет быстродействие работы 1С продуктов. Отсутствует либо закончилась лицензия антивируса Касперского у пользователей. В данной ситуации компьютер открыт для любого вредоносного кода. Ситуацию спасают только ограниченные пользовательские права.

(14) Наличие у пользователей с доступом в Интернет — ICQ или QIP пейджера. Данная программа является источником повышенного риска для вирусной атаки из Интернет.

(15) Отсутствует корпоративная почта компании. Пользователи и филиалы пользуются бесплатными почтовыми сервисами mail.ru, yandex.ru и др.

(16) У пользовательских компьютеров нет политики по распределению дискового пространства. В основном локальный диск C отформатирован в формате FAT32, что является большим недостатком по сравнению с файловой системой NTFS.

(17) На сервере Server2.vs системный раздел диска C в формате FAT32 (!). Необходимо установить обновление Service Pack 2. Крайне желательно установить Service Pack 4 на MS SQL 2000 Server.

(18) На серверах установлены программы ICQ чат.

(19) На серверах SQL.vs и Term.vs «разогнаны»(!) центральные процессоры на 500 MHz каждый. Это недокументированная возможность повышения быстродействия компьютера. Повышенное тепловыделение и нестабильная работа — побочные эффекты такого «разгона».

(20) На сервере Server.vs запущен сервис DHCP Server(!), DNS Server, и NNTPSVC. Данные сервисы вносят дезорганизацию в работу всей сети.

(21) На всех серверах «открыты» порты 25 и 110. Данные порты необходимо закрыть остановкой соответствующих сервисов SMTP и POP. Это предотвратит рассылку и распространение спама и вирусов.

(22) Отрыт анонимный (!) полный доступ (!) по FTP на внешний адрес центрального офиса 217.115.81.86. На данном FTP сервере находятся инструкции и файлы выгрузки-загрузки 1С в формате XML.

(23) Нерациональное распределение ролей серверов. Более эффективно использовать для сервера баз данных специализированный сервер. SCSI-диски значительно ускорят время реакции на пользовательский SQL запрос.

(24) SHDSL модем подключен непосредственно к терминальному серверу TERM.vs. Это способствует проникновению во всю локальную сеть со стороны провайдера.

(25) Неоднородные операционные системы у пользователей. У большинства пользователей установлена Windows XP PRO RUS + SP2. Пакет обновления SP2 установлен у 50% пользователей Windows. У 3-х пользователей установлена Windows 2000.

(26) Не задействованы все возможности использования доменных групповых политик безопасности. Это значительно повысит эффективность работы системных администраторов в управлении пользователями и компьютерами. Нет удаленного администрирования пользователей и филиалов.

(27) У 70% пользователей офиса оперативной памяти 256 Мбайт. Учитывая, что пользователи в основном работают с базами 1С 7.7 и 1С8.1 — то для комфортной работы данное значение необходимо поднять хотя бы до 512 Мбайт.

(28) В 2-3 комнатах пользователей расположены активные сетевые концентраторы. Это вносит дополнительную задержку в информационном обмене.

(29) Не оптимально расположены базы 1С8.1 на SQL2005 Server. Вследствие этого — постоянно не хватает свободного дискового пространства. Не рационально настроены транзакционные логи баз данных SQL.

(30) Нестандартная конфигурация терминальных серверов. Задействованы нерегламентированные возможности системы Microsoft Windows. Это может привести к полному отказу в обслуживании пользователей.

(31) Парк пользовательских компьютеров по техническим характеристикам отстает от требований используемого программного обеспечения как по скорости процессора, так и по объему жесткого диска и оперативной памяти.

(32) Отсутствует единый источник бесперебойного питания с достаточным запасом по мощности.

(33) Не установлены необходимые последние обновления на SQL 2005 Server.

## 5. Выводы

На данный момент система ИТ компании находится в нестабильном положении. Любой фактор риска может надолго дестабилизировать работу компании и нанести материальный и моральный ущерб. На данный момент ситуацию усугубляет и полная кадровая смена системных администраторов. Любая система ИТ строится с фундамента. Правильно заложенные основы — залог успешного развития информационного обмена компании и ее филиалов. И как следствие — успешный бизнес. В данном случае видны правильные движения, однако соответствующая основа не подготовлена.

- Первое, на что необходимо обратить внимание — это линии связи, линии коммуникации. Эти линии можно сравнить с артериями и кровеносными сосудами. Если они работают с ошибками и не стабильно — то система не работоспособна, какие бы мощные сервера не были. Следовательно, необходимо уделить должное внимание на устранение проблем в кабельной системе:
  (1) Маркировать провода.
  (2) Устранить «скрутки» путем прокладки кабеля вновь — либо вилка-розетка.
  (3) Сделать коммутационную кросс-панель в шкафу.
  (4) Разместить активное оборудование Switch в шкафу.
  (5) Устранить HUB в комнатах пользователей.
  (6) Установить в кабинетах розетки кат.5е.
  (7) От каждого рабочего места необходимо провести отдельный провод в серверную.

  Выполнение перечисленных выше условий, гарантирует высокую скорость и стабильность обмена информацией с серверами.
- Второе - это функциональные роли серверов, оптимальное распределение нагрузки, дальнейшая масштабируемость системы серверов. В данной ситуации видно не рациональное распределение ролей серверов и управление серверами. Такое положение дел уже отчетливо сказывается на работе пользователей с системой 1С7.7 и 1С8.1. По объективным причинам размеры баз данных постоянно увеличиваются в

объеме. Растет соответственно объем данных пересылаемый от сервера к пользователю (в варианте DBF) и обратно. Единственный правильный выход в данной ситуации это перевод базы данных из формата DBF в SQL. Рекомендуется это сделать при числе активных пользователей от 15-20 человек и размере базы от 1 Гбайт. Данный перевод даст положительный эффект прироста производительности только при условии размещения SQL базы на дисках типа SCSI, SAS или SATA RAID 0+1 и выше. В нашем случае мы видим, что сервер SQL.vs не соответствует условиям. Сам по себе факт перевода базы из DBF в SQL дает только эффект стабильности работы. Прирост скорости можно получить используя только высокоскоростные дисковые массивы. Тот факт, что системы 1С7.7 и 1С8.1 разделены по разным серверам SQL 2000 и SQL 2005 соответственно — это правильно. Система 1С7.7 конечно работает на SQL 2005 — но не рекомендуется из-за не стабильности в работе 1С7.7.

- Третье, на что необходимо обратить внимание — это информационное взаимодействие с филиалами. В компании используется ADSL и SHDSL технология связи, которые обеспечивает на данный момент все потребности. Однако необходимо рассмотреть вариант расширения каналов связи для обеспечения растущих потребностей в информационном обмене в связи с увеличение филиалов и количества пользователей в центральном офисе. Критичность отсутствия связи для интерактивной работы с базой данных удаленных филиалов обуславливает создание резервных каналов связи. Здесь возможны варианты — либо оптоволоконные линии связи, либо использовать беспроводные каналы. Оптоволоконная связь характеризуется повышенным быстродействием, емкостью канала и не подвержена внешним помехам. Обратная сторона данного решения — высокая стоимость. Беспроводные каналы связи — более дешевое решение, однако скорость обмена гораздо меньше. Беспроводной канал связи можно использовать только как резервный канал. Частный случай беспроводного решения - спутниковая

ассиметричная связь. Характеризуется стабильностью, надежностью, высокой скоростью, дешевая стоимость обслуживания. Недостатки — организация запросного канала связи, проблемы с получением постоянного IP адреса (не все провайдеры предоставляют данную услугу) [4].

- Четвертое, важное замечание. Организация серверного помещения. Комнату необходимо переоборудовать только для размещения серверов и коммуникационного оборудования. В идеале все оборудование должно быть смонтировано в специальном шкафу. Помещение должно быть оснащено круглосуточным кондиционированием с автоматическим поддержанием заданной температуры. В помещение необходимо сделать силовой ввод с заземлением 220 Вольт через отдельный пакетный предохранитель. Рекомендуется иметь подъемный пол или систему кабельнесущих лотков. Покрытие пола — ковролин.

В заключение, оценивая работу администраторов компании по 10 бальной шкале можно выставить оценку 4, за допущенные стратегические просчеты в создании инфраструктуры и управление пользователями и серверами.

## Список литературы

[1] Брэгг Р., Родс-Оусли М., Страссберг К. Безопасность сетей. Полное руководство. — М.: Издательство «ЭКОМ», 2006. — 912 с. ↑1

[2] Microsoft I. Администрирование Microsoft SQL Server 2000. — М.: Русская редакция, 2004. — 640 с. ↑9

[3] Эбен М., Таймэн Б. FreeBSD. Энциклопедия пользователя: ООО ДиаСофтЮП, 2003. — 768 с. ↑12

[4] Олифер В., Олифер Н. Компьютерный сети. — СПб.: БИНОМ. Лаборатория знаний, 2001. — 672 с. ↑5

Levinson Dmitriy Mikhaylovich. *Audit of information system of Joint-Stock Company "Chelyabinsk-vostok-service"* // Proceedings of Junior research and development conference of Ailamazyan Pereslavl university. — Pereslavl, 2009. — p. 302–319. (*in Russian*).

Abstract. Audit research of information system of ZAO "Chelyabinsk-Vostok-Service" is presented. Review, conclusions and recommendations are of structure of this company are provided.