Отчет по аудиту ИТ-безопасности

Объект

Оглавление

Инвентаризация ИТ-безопасности — это составление списка систем, т. е. объектов, которые будут подлежать защите и субъектов, которые задействованы в данном информационном пространстве, и будут влиять на информационную защиту системы с указанием критичных сервисов и точек возможного нарушения безопасности.

1. Физический контроль доступа в помещения, наблюдение за помещениями

Анализ сферы физического доступа, наблюдения и контроля помещений на объекте Заказчика

Объект изучения	**Текущее состояние**	**Оптимальная структура**	**Нарушения, замечания и угрозы**	**Меры по исправлению ситуации**
Контроль физического доступа в помещения в рабочее и нерабочее время	**Центральный офис** Два простых аппаратных контроллера электронных ключей, запрограммированы на открытие электронного входного замка каждой двери по карточке доступа, без логической составляющей, в любое время суток **Склад** Закрывается на ключ	СКУД – отдельная интеллектуальная система управления доступом, базированная на собственном сервере, к которой по сети IP подключены контроллеры доступа каждого отдельного помещения: • Серверная • Кабинеты руководителей • Кабинеты изолированных отделов	• Нет системы гибкого управления физическим доступом • Все внутренние отдельные помещения физически защищены обыкновенными замками, некоторые ключи находятся в свободном доступе	• Закупить отдельный сервер • Закупить ПО СКУД • Закупить и установить контроллеры и электронные замки для каждого отдельного помещения • Подключить контроллеры дверей к центральной системе СКУД • Настроить систему СКУД согласно техническому заданию, с учетом разрешенных уровней доступа групп сотрудников и времени суток

				• Зафиксировать группы доступа в регламенте ИТ-безопасности
Визуальный контроль перемещения сотрудников в помещении	**Центральный офис** Четыре IP камеры Axis 207MW – две подключены по Wi-fi, две – по физическому сетевому кабелю 1. У административного директора на локальной рабочей станции находится ПО Axis Camera Station со следующим функционалом: • Запись событий камер, для этого отведено 40Гб на данной рабочей станции • Ручной просмотр визуального изображения с камер 2. У секретаря настроены ярлыки на прямой web-доступ к камерам, по их количеству. Данный функционал позволяет секретарю просматривать визуальное изображение	Выделенный сервер со специальным серверным ПО видеонаблюдения, имеющий функционал: • Наблюдения в режиме онлайн • Хранения и ротации записей с периодом месяц, частотой – ежедневно • Отправки оповещений при нарушении периметра либо другом заданном событии	• Использование рабочей станции в качестве видеосервера грозит потерей видеоархива • Нет постоянного защищенного видеосервера, видеоархив легкодоступен для злоумышленника	• Закупить отдельный сервер либо использовать один из текущих серверов ОС Microsoft под систему видеонаблюдения и видеоархива • Закупить отдельные жесткие диски повышенного объема под видеоархив, при необходимости закупить и установить дисковый контроллер для дополнительных жестких дисков • Закупить и внедрить программное обеспечение ISS SecureOS, настроить видеонаблюдение и видеоархив согласно ТЗ • Настроить мониторинг работоспособности ПО видеонаблюдения Настроить оповещения системы

	с камер в режиме реального времени **Склад** Наблюдения нет			видеонаблюдения при нарушении периметра
Система отчетности и оповещений о доступе и перемещении в офисе Заказчика	**Центральный офис** • Есть видеоархив с буфером хранения 40 Гб • Есть система ручного биометрического учета о посещении офиса у секретаря **Склад** Есть – детекторы движения. Охранная компания Кобра Гарант	1. Должна присутствовать удобная система статистики сервера СКУД с отчетностью • Сотрудник • Время и дата • Действие (вошел\вышел) • Помещение 2. Должна присутствовать удобная панель просмотра и работы с видеоархивом 3. Должна присутствовать система автоматического учета рабочего времени на основе данных СКУД 4. Должна присутствовать функция оповещения ответственного лица о нарушении периметра на основании данных СКУД и видеонаблюдения	• Нет системы учета и статистики о физическом доступе в офисные помещения и кабинеты • Нет системы автоматического учета рабочего времени • Нет системы удобной работы с видеоархивом • Нет системы автоматического оповещения о нарушении физического периметра защиты	• Внедрение СКУД (см пункт 1) • Внедрение профессионального оборудования видеонаблюдения (см пункт 1) • Внедрение системы отчетности и оповещений контроля доступа согласно ТЗ

2. Аппаратное обеспечение информационной системы

Анализ серверной и центральной коммутационной структуры, физической доступности рабочих станций и периферийного оборудования

Объект изучения	Текущее состояние	Оптимальная структура	Нарушения, замечания и угрозы	Меры по исправлению ситуации
Защищенность помещения и наличие специальных защитных монтажных изделий, в которых физически расположена серверная и коммутационная структура	**Центральный офис** • На объекте есть выделенное помещение для работы серверной и центральной коммутационной структуры. • Помещение защищено замком. • Серверная стойка открытая. • Помимо серверного оборудования, помещение служит хранилищем пустой тары от офисной электронной техники **Склад** • На объекте нет никаких защитных помещений либо шкафов, все оборудование размещено в мебельной тумбе • Тумба открывается без ключей	• На объекте должно быть выделенное помещение с четко ограниченным доступом сотрудникам согласно регламента безопасности Или • На объекте должен быть защищенный серверный шкаф, ключи должны находиться у ответственного лица • Должны быть запрещены прямые консольные выводы (типа розеток питания, мониторов, клавиатур, KVM и т.д.) за пределы защищенного серверного шкафа либо полки • Серверная комната не должна использоваться в качестве склада и других	Ключи от серверной комнаты лежат у ИТ-инженера в ящике стола. В принципе есть возможность попасть в серверную любому сотруднику либо гостю Серверная стойка открытая, комната совмещена со складом тары. Есть риск повреждения центральных коммуникаций либо серверного оборудования при проведении хоз. работ	• Внедрить систему СКУД с четким разграничением доступа к серверной комнате (см. пункт 1) • Как бюджетный вариант - организация полностью закрытого монтажного изделия, содержащего серверную и коммуникационную структуры, без возможности намеренного или ненамеренного влияния посторонних лиц

	• Серверное и коммутационное оборудование на видном месте и его легко вывести из строя	вспомогательных ролей • Должна отсутствовать возможность легкого доступа извне (через окно, боковые двери и т.д.)		
Наличие инвентаризационной системы учета и привязки рабочих станций к конкретным пользователям системы	• Маркировок рабочих станций нет • Карточек учета ПК нет • Имена рабочих станций произвольные • Автоматической системы учета оборудования нет	• Электронный либо бумажный каталог рабочих станций, серверов, телефонного и периферийного оборудования объекта с уникальными идентификаторами каждой единицы • Маркировка оборудования и поддержка ее в актуальном состоянии	Отсутствие учета офисного ИТ-оборудования грозит как минимум безнаказанностью виновных в его повреждении, краже и т.д. Также отсутствует инструмент, позволяющий упорядочить структуру, проводить планирование модернизаций ИТ, дающий понимание потенциально узких мест в производительности и безопасности структуры.	• Внедрение маркировки всего ИТ-оборудования • Внедрение электронной системы учета оборудования (на базе 1с либо другого ПО) • Каталогизация и упорядочивание всего ИТ-оборудования • Внедрение специальных программ инвентаризации компьютерной сети, построения интерактивной карты сети и мониторинга ее состояния

3. Сетевое обеспечение информационной системы

Анализ кабельной структуры Организации, доступности и защищенности сетевых розеток и беспроводных соединений

Объект изучения	**Текущее состояние**	**Оптимальная структура**	**Нарушения, замечания и**	**Меры по исправлению**

			угрозы	**ситуации**
Наличие общедоступных участков кабельной системы с возможностью неконтролируемого подключения спец устройств	**Центральный офис** • Сеть сделана по проекту специализированной компании • Проектная документация присутствует • Структурированная документация и схема сети • В сети присутствует защита методом назначения сервером DHCP разных данных в зависимости от подключения к той или иной сетевой розетке. Однако данная схема не контролирует адреса, проставленные злоумышленником вручную. **Склад** • Проектировки сетевой структуры нет • Информационная и электрическая	• Структура должна соответствовать стандартам построения кабельных сетей • Структура должна иметь разделенную физически пользовательскую область и демилитаризированные зоны с контролем обмена траффиком между ними	• Нет фильтрации сетевых портов по MAC-адресам устройств • Есть общественные сетевые розетки • Нет разделения сети на Vlan и демилитаризованные зоны. Злоумышленник, подключившись со статическим адресом к общедоступной сетевой розетке может получить доступ к локальной сети **Склад** Структура полностью не соответствует требованиям безопасности	• Необходимо внедрить привязку сетевых портов к разрешенным MAC-адресам. Оставить только контролируемые порты, например в конференц-зале. • Все неиспользуемые сетевые разъемы должны быть физически отключены, заглушены либо деактивированы на патч-панелях в серверном шкафу • Данные сетевые порты вывести в отдельный Vlan в демилитаризованной гостевой зоне с разграничением доступа через Firewall согласно ТЗ **Склад** • Необходимо рассчитать проект и привести кабельную

	кабельная структура проложена небрежно, полностью открыта и уязвима			структуру к стандартам построения компьютерной сети • Необходимо привести электрическую сеть к стандартам требований по безопасности эксплуатации • Необходимо рассчитать проект по решению проблемы выключения электропитания и зависимости ИТ-структуры от данного форс-мажора. Например, внедрение беспроводного интернет и мощного источника бесперебойного питания
Возможность подключения посторонних лиц по сети Wi-fi	• Шифрование WPA2 • Пароль сложный • Крипто стойкость пароля присутствует • В беспроводной сети присутствует защита	Сеть Wi-fi в центральном офисе должна быть отнесена в демилитаризированную зону с контролем и разделением обмена траффиком	В центральном офисе нет отделения беспроводной сети отдельным Vlan и разграничением доступа между пользовательской и беспроводной сетями	Сеть Wi-fi вывести в отдельный Vlan в демилитаризованной гостевой зоне с разграничением доступа через Firewall согласно ТЗ

	методом назначения сервером DHCP (см. предыдущий пункт) **Склад** Беспроводная сеть вынесена в отдельный Vlan			

4. Системное программное обеспечение

Результаты аудита операционных систем серверов, защиты рабочих станций, коммутационного оборудования, маршрутизаторов, степени защиты паролей и резервных копий
Проведение практических тестов:

- Сканирование локальной сети на открытые ресурсы, поиск общедоступных ресурсов
- Подключение к серверным и периферийным устройствам по сети, возможность вывода их из строя
- Проведение сканирования внешних портов, фиксирование точек успешных атак через найденные уязвимости
- Проверка файлов резервных копий, попытка найти, увидеть, открыть, скачать, удалить их под правами пользователя
- Подключиться к сети, вычислить серверные ресурсы, попробовать выложить документы на внешний ресурс

Объект изучения	**Нарушения, замечания и угрозы**	**Меры по исправлению ситуации**
000.000.000.000 - точка доступа DIR-615	Можно зайти под пользователем User и пустым паролем, просмотреть всю информацию о пробросах, MAC, пользователях, устройствах в сети и т.д.	Необходимо усилить защиту паролем: • Пароль не должен быть слишком коротким, минимум 7 символов • Пароль должен содержать сочетание нескольких цифирных, буквенных символов и одного спец-символа • Пароль не должен быть словарным словом или простым их сочетанием • Пароль не должен состоять только из общедоступной информации
000.000.000.000 - HP LaserJet P1505n	Можно зайти на веб-интерфейс с пустым	Необходимо усилить защиту паролем:

	паролем, перехватить принтер путем смены IP-адреса, сменить либо деактивировать настройки. Тем самым ресурс станет непригодным к использованию	• Пароль не должен быть слишком коротким, минимум 7 символов • Пароль должен содержать сочетание нескольких цифирных, буквенных символов и одного спец-символа • Пароль не должен быть словарным словом или простым их сочетанием • Пароль не должен состоять только из общедоступной информации
000.000.000.000 - Deskjet 6940 series	Можно зайти на веб-интерфейс с пустым паролем, перехватить принтер путем смены IP-адреса, сменить либо деактивировать настройки. Тем самым ресурс станет непригодным к использованию	Необходимо усилить защиту паролем: • Пароль не должен быть слишком коротким, минимум 7 символов • Пароль должен содержать сочетание нескольких цифирных, буквенных символов и одного спец-символа • Пароль не должен быть словарным словом или простым их сочетанием Пароль не должен состоять только из общедоступной информации
000.000.000.000 - Sinology Rack	• Папка restored разрешена для полного редактирования и содержит полную информацию с дисков скорее всего со старого терминального сервера. В данной папке масса старых xls, doc и jpg файлов коммерческого содержания • Base\QB-AO старые архивы с Quick Book • Резервные копии старых виртуальных машин. Доступ гостя к такому ресурсу позволит злоумышленнику выкачать коммерчески	Поскольку данный ресурс служит долгосрочным хранилищем, то необходимо: • Убрать свободный доступ по сети к данному ресурсу • Ввести ограничение по логину и паролю с помощью доменной авторизации (данное хранилище привязано к доменной структуре) • Хранить архивы в зашифрованном виде

	значимые документы	
000.000.000.000 - Sinology	Содержит открытые актуальные резервные копии объекта, снимки дисков tib, виртуальных машин терминального сервера 1c Spider и старый файл-сервер Exchange. Остальные папки закрыты доменным паролем Доступ гостя к такому ресурсу позволит злоумышленнику выкачать незащищенные актуальные резервные копии и после распаковки получить на руки уже актуальные коммерчески значимые документы, что приведет к гораздо более печальным последствиям	Поскольку данный ресурс служит оперативным хранилищем резервных копий, то необходимо: • Убрать свободный доступ по сети к данному ресурсу, оставить ограничение по логину и паролю с помощью доменной авторизации (данное хранилище привязано к доменной структуре) • Хранить файлы резервных в зашифрованном виде с защитой по паролю • По максимуму убрать остальные роли с данного хранилища, оставив только роль хранения резервных копий. Документы переместить в архив либо на защищенный файловый сервер
\\000.000.000.000\cups-pdf	• Полностью открытые коммерчески значимые PDF (счета) и список принтеров, не защищен паролем доступа по сети • Физически располагается на шлюзе, что является нарушением политики безопасности	• Принт-сервер должен быть защищен доменным паролем и правами NTFS • Сетевой ресурс для сканирования должен быть защищен доменным паролем и правами NTFS • На шлюзе не должно располагаться никаких внутренних документ-ресурсов
Рабочие станции пользователей	Открыты порты для: • Smb – доступ к рабочей станции по сети • Remote Desktop – доступ к рабочей станции по удаленному рабочему столу • Не все рабочие станции введены в домен. Такие рабочие станции свободны от всякого контроля и являются главными кандидатами на роль дыр проникновения	• Необходимо закрыть доменными политиками все порты рабочих станций, кроме ICMP • Необходимо ввести все рабочие станции в домен с применением общих доменных политик • Необходимо убрать перекачку файлов по сети с помощью организации удаленного сервера с файловым хранилищем и удаленными рабочими местами (см. пункт 11)

	в структуру • Есть проблемы при закачке по сети больших файлов	
000.000.000.000\1c - Spider1C	Доступна для записи и чтения по сети под правами гостя. Злоумышленник может закачать себе актуальные базы 1с	Сетевая папка конфигураций и файловых баз 1с должна быть защищена доменным паролем и правами NTFS согласно ТЗ
Spider1C	Дисковая подсистема ввода\вывода не справляется с нагрузкой толстых клиентов 1с в терминальном режиме. Это связано с использованием конфигурации RAID5, состоящей только из 3 жестких дисков Sata	Данная проблема может быть решена путем перемещения ресурса 1с на удаленный специализированный сервер
Документы из общих локальных ресурсов	Несмотря на наличие прокси-сервера и довольно неплохой защиты исходящего трафика – злоумышленнику ничего не стоит разместить документы компании на своем ресурсе FTP, подключить изнутри VPN-соединение OpenVPN, передать документы по Skype либо аналогичному интерактивному ПО «клиент-сервер»	Необходимо внедрить простую систему фильтрации входящего и исходящего трафика Все коммерчески значимые данные предлагается вынести на удаленный сервер с файловым хранилищем и удаленными рабочими местами (см. пункт 11), на котором будут настроены политики ограничения работы с ресурсами интернет согласно ТЗ
Внешний адрес ЦО 000.000.000.000 – сканирование извне	Открытые порты: TCP 135 (MS RPC)	Настоятельно рекомендуется заблокировать указанные порты для входящих соединений извне. В сервисах MSRPC и NETBIOS, расположенных по портам 135, 139, могут быть незакрытые уязвимости, которыми может воспользоваться злоумышленник или вредоносная программа. Также атака может произойти через открытый интерфейс сервера печати на складе
Внешний адрес ЦО 000.000.000.000 – сканирование извне	Открытые порты: TCP 80 (HTTP) TCP 135 (MS RPC) TCP 139 (Netbios), TCP 443 (HTTPS, Skype)	
Внешний адрес склада 000.000.000.000 – сканирование извне	TCP 53 (open domain) TCP 631 (CUPS 1.4, сервис печати)	

5. Организационное обеспечение

Анализ состояния субъектов системы - пользователей, их прав доступа, времени работы в ИТ-системе, мониторинга и отчетности об их действиях

Объект изучения	**Текущее состояние**	**Оптимальная структура**	**Нарушения, замечания и угрозы**	**Меры по исправлению ситуации**
Возможность доступа к включенной рабочей станции, периферийному оборудованию посторонним лицом либо другим пользователем при отсутствии сотрудника на рабочем месте (вышел по необходимости, на обед, на перекур и т.д.)	• Рабочие станции выключаются по питанию при долгосрочном отсутствии сотрудника • При краткосрочном отсутствии сотрудника рабочие станции, рабочие столы и открытые документы остаются доступными • Экраны не блокируются (за исключением некоторых лиц)	Доступ к операционной среде должен блокироваться вручную при уходе сотрудника с рабочего места либо автоматически по истечению 5 минут простоя операционной среды	Злоумышленник свободно может получить доступ к незащищенному рабочему месту, оставленному без присмотра	Внедрение политики безопасности рабочих мест при отсутствии сотрудника
Пользовательская операционная система и интерфейс пользователя	• Рабочие станции пользователей представляют собой автономные ПК без контроля со стороны доменных структур • Политики ограничения пользовательских прав и ресурсов рабочих мест нет • Ограничений рабочих	• ОС пользователей должна быть ограничена только нужным функционалом,. Уровень ограничения операционной среды (например, интерфейса Microsoft Windows) должен соответствовать группам доступа пользователей и быть	Свободный круг возможностей, особенно с правами администратора, в операционной среде пользователя дает широкую возможность действия вирусов, троян-инъекций, хакеров, неосторожных действий пользователей в операционной системе и	• Создание и внедрение регламента безопасности с четкими политиками ограничения рабочих мест пользователей, регулированием работы по времени суток с помощью функционала домена

	столов и личных папок нет	закреплен в таблице регламента ИТ-безопасности • Время работы сотрудников в операционной среде должно технически регулироваться, иметь возможность блокировки доступа к ОС в зависимости от времени суток, согласно таблицы регламента ИТ-безопасность • Права пользователей на выполнение операций в ОС, с периферийным оборудованием либо в спец ПО должны быть разделены по ролям, и зафиксированы в таблице регламента ИТ-безопасности. Возможность изменения прав должна быть реализована только с помощью письменного запроса руководителя	т.п. Совокупность этих событий может привести к гарантированному выводу из строя рабочего места пользователя и даже центрального важного ресурса	• По возможности, перенос максимального количества рабочих мест на удаленный сервер (см. пункт 11) и внедрение «тонких терминальных клиентов» с возможностью контроля окружающей среды пользователя через единый центр ОС PXE
Учет, мониторинг и отчетность действий пользователей в серверной структуре и	• Мониторинга действий пользователя в серверной структуре нет	• На ОС серверов и общих ресурсов должно быть реализовано ведение логов, источника и	Любые нарушения периметра безопасности либо неразрешенные действия пользователя	• Внедрение системы полного учета действий пользователей в

система оповещений администратора о нарушениях безопасности в серверной структуре	• Системы оповещения о нарушении периметра серверной безопасности нет	времени логина, времени работы пользователей в разрезе по доменному уникальному логину пользователя. Доступ к лог-файлам имеет сетевой администратор, генеральный директор и руководитель отдела ИТ-безопасности • Должна присутствовать система комплексного мониторинга и оперативного оповещения нарушения нормального состояния всех общедоступных ресурсов, работа которых важна для Компании	(удаление файла, базы, перекачка файла на внешний носитель и т.д.) останутся незаметными для ответственных лиц. Таким образом, незаметно для них со временем отдельные нарушения могут трансформироваться в целую систему автоматического шпионажа и перекачки данных Компании	серверной среде • Внедрение системы мониторинга и оповещения ответственных лиц о нарушении периметра безопасности: серверная структура, локальная сеть, внешние шлюзы, публичные и общие ресурсы и т.д.

6. Нормативное обеспечение

Отчет о состоянии регламентной составляющей ИТ-безопасности

Объект изучения	**Текущее состояние**	**Оптимальная структура**
Документы, регулирующие права и обязанности сотрудников в ИТ-сфере компании	Системных документов нет	1. Работу и обеспечение системы безопасности должен регулировать центральный регламент ИТ-безопасности, в котором содержатся разделы по: • Правам и обязанностям сотрудников • Уровням и возможностям доступа к ресурсам • Физическая безопасность помещений и структуры
Документы,	Системных документов	

регулирующие уровни и возможности доступа к ресурсам	нет	• Безопасность рабочих мест • Безопасность данных, уровни доступа к ним • Ответственность и санкции в случае нарушений 2. В системе должны присутствовать должностные правила по безопасности, оформленные на основе детализации пунктов регламента ИТ-безопасности. Сотрудники должны быть ознакомлены под роспись 3. В системе должны присутствовать инструкции и методики тех или иных действий сотрудников в случае возникновения ситуаций, предусмотренных регламентом ИТ-безопасности 4. В системе должны присутствовать плакаты, напоминания, предупреждения, оформленные в бумажном виде, четкими крупными символами или картинками и размещенные в общественных помещениях и на рабочих местах пользователей
Документы, регулирующие уровни физической безопасность помещений и структуры	Системных документов нет	
Документы, регулирующие ИТ-безопасность рабочих мест	Системных документов нет	
Документы, регулирующие безопасность данных, уровни доступа к ним	Системных документов нет	
Документы, обозначающие уровень ответственности и санкций в случае нарушений	Системных документов нет	

7. Корпоративные данные

Результат аудита защищенности ключевых корпоративных данных, возможности их повреждения или похищения

Роили и ресурсы	**Текущее состояние**	**Меры по исправлению ситуации**
Файл-сервер и документы Компании	• Документы и их копии в многочисленном порядке находятся на рабочих местах (см. таблицу пользователей) • В компании есть несколько сетевых файл-	Корпоративные данные должны быть размещены на специальном удаленном сервере с ограниченным сетевым доступом (см пункт 11)

	серверов и сетевых хранилищ, ни один не защищен разграничением прав NTFS (кроме ресурса «бухгалтерия»)	
Терминальный сервер	Есть локальный терминальный сервер, содержащий интерфейсы и базы 1с. Вход разрешен всем пользователям домена.	• Производственные базы и программы должны быть размещены на специальном удаленном сервере с ограниченным сетевым доступом (см пункт 11) • Нет в списке лицензии для серверной системы Microsoft Server 2003 (имеющаяся лицензия юридически рассчитана на 180 дней)
Клиент-банки и системы отчетности	Находятся на рабочих местах бухгалтерии	• Финансовые программы обмена данными (клиент-банки, торговые площадки и т.д.) рекомендуется разместить на отдельной локальной рабочей станции в виде виртуальной машины • Необходимо вывести это рабочее место в отдельный Vlan без возможности доступа из локальных сетей • Необходимо организовать регулярное выполнение снимков данной виртуальной машины на сервер резервного копирования
Доменная структура	В компании существует сервер, содержащий LDAP-структуру, аналогичную доменной структуре Microsoft. Однако, кроме проведения центральной авторизации, данная структура больше ничего не умеет.	• Внедрение в компании центрального и резервного контроллеров домена с применением групповых политик ограничения прав пользователей и серверов, что позволит держать под контролем безопасность рабочих областей компании • Перевод структуры на удаленный сервер и использование на большинстве рабочих мест «тонких терминальных клиентов» (данный вариант более предпочтителен)
Почтовая система	Базирована на ПО Communigate Pro, на одной из виртуальных машин сервера-носителя. Почтовые базы пользователей находятся локально, на рабочих местах	• Рекомендовано хранить почтовые центральную и личные базы на защищенном ресурсе с центральным администрированием и защитой, таком как удаленный сервер (см. пункт 11) • Нет в списке лицензии на почтовую систему

Дублирование и отказоустойчивость сервисов	• На данный момент резервирования ресурсов нет • Есть система резервного копирования, копии актуальные	Для обеспечения стабильности и полной отказоустойчивости критичных сервисов компании рекомендуем перенос критичных ресурсов и работу с ними на удаленном сервере: • Серверная площадка класса Tier3 • Резервирование питания N+1 • Резервирование интернет • Резервирование системы сервера и данных • Живая миграция • Работа с отказоустойчивым хранилищем Hitachi
Защита серверной структуры от информационных атак	• Централизованная антивирусная система присутствует • Процедура проведения обновлений серверной ОС Microsoft производится вручную • Пароли сложные, но не содержат спецсимволов **Склад** • Пароли несложные	• Нет подтверждения лицензионности антивируса DR. Web. Среди списков лицензий его нет. Необходима закупка лицензий либо перевод максимального количества рабочих станций на вариант «тонкие клиенты» (см. пункт 11) • Необходимо разработать план регламентных операций серверной части. Одним из пунктов будет обязательное плановое обновление серверных систем Microsoft не менее 1 (одного) раза в неделю. Контроль актуальности обновлений осуществляет сетевой администратор и его заместитель с помощью системы автоматического мониторинга • Пароли на серверную структуру должны соответствовать следующим критериям: o Пароль не должен быть слишком коротким, минимум 7 символов o Пароль должен содержать сочетание нескольких цифирных, буквенных символов и одного спец-символа o Пароль не должен быть словарным словом или простым их сочетанием o Пароль не должен состоять только из общедоступной

		информации о пользователе ○ Срок действия пароля администратора должен составлять 6 месяцев

8. Внутренняя IT-структура – СКС, интрасетевые устройства, коммутационные устройства

№	IP адрес	Название устройства	Описание
1			Телевизор Samsung 55 inch conference room
2			Телевизор Samsung 32 inch doccenter
3			Телевизор Samsung 55 inch showroom
4			Медиацентр Iconbit
5			Принтер HPM2037
6			Принтер Kyocera
7			Принтер HP_color
8			Принтер Panasonic
9			Точка доступа WIFI №1
10			Точка доступа WIFI №2
11			Точка доступа WiFi Dlink

9. Серверная IT-структура — сервера и их роли в системе компании

№	IP адрес	Название устройства	Роли	Ресурсы
1			Носитель виртуальных машин XEN	Supermicro 2*CPU XEON E5405 6 Gb Raid5 500 GB
3			Носитель виртуальных машин XEN	Supermicro 2*CPU XEON E5405 6 Gb RAID5 1.8 Tb
4			Носитель виртуальных машин XEN	Supermicro 2*CPU XEON E5335 4 Gb Raid5 500 GB
2			• Сервер терминалов • Базы 1С	Виртуальная машина

			• СУБД SQL 2005 • Сервер антивируса DRWeb • Файл-сервер • Скан-сервер	
5			Цетральный контроллер домена LDAP	Виртуальная машина
6			• Принт-сервер • Сервис DHCP • Резервный DNS сервер	Виртуальная машина
7			Почтовый сервер	Виртуальная машина
8			• Основной DNS сервер • Резервный сервис DHCP • Пользовательский шлюз	Pentium(R) Dual-Core CPU E5300 @ 2.60GHz 2 GB RAM 160 Gb HDD
9			Сервер печати IPCOP	Виртуальная машина
10			Cups для бухгалтерии. Рабочая станция у сотрудницы бухгалтерии	
11			• Хранилище долгосрочных архивов • Техическое хранилище для инженера	Устройство
12			• 1c_backup – хранилище актуальных копий • Local_exchange – файл обменник • Public – старое файл хранилище • Бухгалтерия – неактуальное хранилище	Устройство
13			• Основной шлюз • Основной DNS сервер • Сервис DHCP	Аппаратный сервер

10. Пользовательская структура

	Все в порядке.
	Обратить внимание.
	Проблема. Необходимо принимать меры.

Наименование	Роль Пользователя и используемое ПО	Наличие прав администратора	Установленное ПО (операционная система идентифицируется по OEM-наклейке и последней цифре серийного кода на наклейке)	Рекомендованное ПО и лицензии, достаточные для выполнения функциональных обязанностей	Аппаратное обеспечение	Актуальность антивируса	Актуальность обновлений MS	Есть ли копии рабочих документов локально	Есть ли бумажки с паролями и конф. данными на рабочем месте	Рекламации и пожелания пользователя
	• MS Office • Почтовый клиент • Служебные программы тестирования	Нет	• Microsoft Windows XP Professional (D7PXB) • Microsoft Office, для дома и бизнеса 2010 • Microsoft Office - стандартный выпуск версии 2003 • Total Commander 6.55 PowerPack	• Microsoft Office - стандартный выпуск версии 2003 • Free Commander	• CPU - Intel Celeron CPU 1.70GHz • RAM - 768 (256 + 512) • HDD - ST340014A (40 ГБ)	Не работает	Актуальны	Нет	Нет	Нет
	• Сертификация оборудования • Инструкции для пользователя и ПО	Есть	• Microsoft Windows XP Professional (92M3G) • Microsoft Office - выпуск для малого бизнеса версии 2003 • Adobe Illustrator CS2 • Nero 8 • Total Commander 6.53 • Архиватор WinRAR	• Офис для малого бизнеса 2007 • Free Commander • 7Zip	• CPU - Intel Celeron CPU 2.66GHz • RAM - 2048 (1024 + 1024) • HDD – ST3160815AS (160 ГБ)	Актуален	Актуальны	Есть	Есть	После ввода пароля компьютер долго загружается
	Генеральный директор	Нет	Microsoft Office стандартный 2010 • Microsoft Windows 7	• Microsoft Windows 7 Professional • Free Commander	• CPU - Mobile DualCore	Актуален	Обновлений нет	Нет	Нет	Присутствует торможение системы при открытии

			Professional (наклейки нет) • Corel WinDVD • Total Commander 7.03 • WinRAR 4.10 beta 2	• 7Zip	Intel Core i5-2410M • RAM – 4007 • HDD – HTS545050 B9A300 500 Гб					программ и документов. Судя по всему – проблема в дисковой подсистеме ноубука. Рекомендуется (в порядке последовательности): • Отключить антивирус и проверить работу • Проверить систему сторонним антивирусом, например CureIT • СпецПО отследить, какой процесс наиболее всего нагружает систему, устранить его • Выполнить стрессовое тестирование системы ввода\вывода и жесткого диска • Выполнить переустановку системы
	Административный директор • MS Office • Почта • Видеонаблюдение	Нет	• Microsoft Windows XP Professional (YP89G) • Microsoft Office Professional Edition 2003 • ACDSee 7.0 PowerPack • Adobe Acrobat 7.0.1 • ArcSoft TotalMedia 3.5 • Total Commander 7.03	Microsoft Office Professional Edition 2003 • DoPDF • PDFReader • Free Commander	• CPU - Intel Pentium Dual CPU E2180 @ 2.00GHz • RAM - 2048 (1024 + 1024) • HDD – ST3250310A S (250 ГБ)	Актуален	Актуальны	Есть	Есть	Нет

	• Документация для пользователей • Поддержка клиентов	Нет	Microsoft Windows XP Professional (RVY7J) • Microsoft Office Professional Edition 2003 • Nero BurnRights • Total Commander 7.03 • Архиватор WinRAR	• Microsoft Office Professional Edition 2003 • BurnCD • Free Commander • 7Zip	• CPU - Intel Pentium 4 CPU 2.80GHz • RAM - 512 (256 + 256) • HDD – WDC WD800JD-22JNA0 (80 ГБ)	Актуален	Актуальны	Есть	Нет	Нет
	Менеджеры СОП • 1с • СпецПО QB • Документы • Почта	Нет	• Microsoft Windows XP Professional (9G6JG) (установлено CHM2B) • ABBYY Lingvo 12 Multilingual Edition • Acronis True Image Home • HashTab 2.0.8 • InterBase 6.5 • ScrewDrivers Client v4 • Total Commander 7.03	Microsoft Windows 7 Professional Free Commander	• CPU - Intel Atom CPU N270 @ 1.60GHz • RAM - 1024 • HDD – WD1600BEVT-22ZCT0 (160 ГБ)	Актуален	Отключены	Есть	Нет	Некомфортно работать с удаленной папкой Exchange по сети (связано с удаленностью папки Exchange, она не предназначена для работы по сети)
	• Организация производства • Курирование сборочного участка производства • Подмена СОП по индустриальной части	Нет	Microsoft Windows XP Professional (8MC36) • Microsoft Office Professional Edition 2003 • Adobe Acrobat 5.0 • AutoCAD 2002 • AutoCAD 2008 • MechaniCS 6.0 • PdfFactory Pro • ScrewDrivers Client v4 • Total Commander 7.03	• Microsoft Office Professional Edition 2003 • AutoCAD 2008 либо аналог nanoCAD • DoPDF • PDFReader • Free Commander	• CPU - Intel Celeron CPU 2.53GHz • RAM - 512 (256 + 256) • HDD – WDC WD800JD-08LSA0 (80 ГБ)	Агент не видит сервера	Актуальны	Есть	Нет	Нет
	Заместитель коммерческого директора • Продажи • Оформление рекламы • Работа с удаленным	Нет	• Microsoft Windows 7 Professional (нет) • Acronis Disk Director Suite • Acronis True Image Home • Microsoft Office Standard 2010 • ScrewDrivers Client v4 • Total Commander 7.03 • WinRAR 4.01	• Microsoft Windows 7 Professional • Microsoft Office Standard 2010 • Free Commander • 7Zip	• CPU - Mobile DualCore Intel Core i3-330M • RAM - 3760 • HDD – WD3200BEVT-	Актуален	Актуальны	Нет	Есть	• Тормозит оболочка Проводник, беспокоят обновления от ПО, которые нельзя поставить с ограниченными правами,

	сервером • Почта				26A23T0 (320 Гб)					выскакивают, мешают работать. • Общее торможение системы, симптомы как у ноутбука генерального директора, рекомендации те же
	• Разработка технического ПО • Тестирование технического ПО • Почта • Документы	Нет Находится не в домене	Microsoft Windows XP Professional (RPBXJ) • Adobe Acrobat 5.0 • Advanced Serial Port Monitor • PICkit 2 v2.40 • SiSoftware Sandra 2002 Standard • Sowedoo Easy PDF Converter 6.0 • Total Commander 6.53 • WinRAR archiver	• Advanced Serial Port Monitor • PICkit 2 v2.40 • Free Commander • 7Zip	• CPU - Intel Pentium 4, 1818 MHz • RAM - 512 • HDD - IC35L060AVVA07-0 (60 Гб	Актуален	Актуальны	Есть	Нет	• Медленный запуск системы (минут 20-30 с утра) • Долго работает почта
	СОП, техническая поддержка клиентов • Почта • Документы • MS Access	Нет	• Microsoft Windows 7 (нет) • Microsoft Office 2010 • Множество ПО и полные пакеты драйверов работы с аудио, сетью и камерой • Total Commander 7.03 • WinRAR	• Microsoft Windows 7 Professional • Microsoft Office 2010 • Необходимо совместно выбрать нужно СпецПО • Free Commander • 7Zip	• CPU - Intel Core i3-2310M CPU @ 2.10GHz • RAM – 4096 (2048 + 2048) • HDD – HTS723232A7A364 (320 ГБ) • HDD2 - HTS542512K9SA00 USB Device (120 ГБ) (внешний USB-диск не	Актуален	Не актуальны	Есть	Есть	• Диск Q – нет места • Скорость обмена с локальным хранилищем Exchange очень слабая • Поиск MS Outlook зависает и появляется ошибка от 5 до 20 раз подряд «сбой операции. Объект не найден» • Техническая поддержка компании – не устраивает организация

					безопасен)					работы по задачам. Нет формирования ожидания пользователя по его задаче, отсутствие решения проблемы по истечению времени, забываются задачи пользователя
	Менеджеры СОП • 1с • СпецПО QB • Документы • Почта	Нет	Microsoft Office, для дома и бизнеса 2010 • Microsoft Windows 7 (нет) • Corel WinDVD • EasyClients - База клиентов • McAfee Security Scan Plus • Total Commander 7.03	Microsoft Windows 7 Professional Free Commander	• CPU - DualCore Intel Core i3-2310M, 2100 MHz • RAM – 1959 • HDD – WDC WD3200BEVT-08A23T1 (320 Гб	Актуален	Не актуальны	Есть	Нет	• Есть пожелание почту перенести с Windows Live • Есть зависания системы, 91% ОЗУ использовано ничем • Не обновляется офис (ошибка 0000057E WindowsUpdate DT00)
	Менеджеры СОП • 1с • СпецПО QB • Документы • Почта	Нет	• Microsoft Windows XP (Наклейка полностью испорчена и нечитаема) • Acronis Disk Director Suite • Acronis True Image Home • Remote Administrator • SLP-V • Total Commander 7.03 • КриптоПро CSP	Microsoft Windows XP Professional Free Commander	• CPU - Intel Pentium 4, 3000 MHz • RAM – 496 • HDD – IC35L060AVVA07-0 (60 Гб)	Актуален	Актуальны	Есть	Нет	Нет
	Свободная рабочая станция	Нет	Microsoft Windows XP Professional (DBHF8) • Microsoft Office Small Business 2007 • ACDSee 5.0 PowerPack • PdfFactory Pro		• CPU - Intel Core 2 Duo, 2333 MHz • RAM – 2038 • HDD – WD1600AA	Актуален	Актуальны	Есть	Есть	Свободная рабочая станция

			• SlovoEd 3.x for PocketPC • Total Commander 6.53 • WinRAR		JS-22WAA0 (160 Гб)					
	Менеджеры СОП • 1с • СпецПО QB • Документы • Почта	Нет	Microsoft Windows XP Professional (HW9PW) • Adobe Acrobat 7.0.1 • Microsoft Office Professional Edition 2003 • Remote Administrator v2.1 • SiSoftware Sandra Professional Business XI • Total Commander 6.53 • WinRAR	Microsoft Office Professional Edition 2003 • Free Commander • 7Zip	• CPU - Core2 Duo CPU E4600 @ 2.40GHz • RAM – 1024 • HDD – HDP725025 GLA380 (250 ГБ)	Актуален	Отключены	Есть	Есть	• Наблюдаются зависания при работе с 1с на терминальном сервере Spider, скорее всего не справляется дисковая подсистема • При закрытии внутреннего окошка QB – иногда он закрывается весь. Поставлена задача ответственным инженерам
	Менеджеры СОП • 1с • СпецПО QB • Документы • Почта	Нет	Microsoft Windows XP Professional (PTVT6) • ACDSee 6.0 PowerPack • AllSubmitter • Diskeeper Server Enterprise Edition • Inpaint • InterVideo WinDVD Creator 2 • iSpring Pro • McAfee Security Scan Plus • Nero 6 Ultra Edition • Photo Frames PRO 1.50 • Remote Administrator • Total Commander 7.03 • UltraISO 8.0 Premium Edition • WinRAR	Free Commander	• CPU - Intel Pentium 4, 3000 MHz • RAM – 2048 • HDD – ST3120026AS (120 Гб)	Актуален	Отключены	Есть	Есть	Нет

	Менеджеры СОП • 1с • СпецПО QB • Документы • Почта	Нет	• Microsoft Windows Vista Business (39K9W) • 2007 Microsoft Office system • Adobe Photoshop CS2 • Adobe Photoshop CS3 • Firebird (СУБД, зачем СОП) • InterBase 6.5 (СУБД, зачем СОП) • Remote Administrator • Total Commander 7.03 • WinRAR	• Free Commander • 7Zip	• CPU - Intel Pentium 4 CPU 3.00GHz • RAM – 1024 • HDD – ST380211AS ATA Device (80 ГБ) (ATA интерфейс может приводить к торможению диска)	Актуален	Есть неустановленные	Есть	Есть	Иногда зависает терминальное подключение, выбрасывает из сеанса
	ИТ инженер Есть Virtual PC с win XP Prof Adobe Photoshop		ОС Linux Есть виртуальная платформа Virtual PC с установленной ОС XP Prof Adobe Photoshop	ОС XP Prof для тестирования и работы	Не применимо	Не применимо	Не применимо	Нет	Нет	Нет
	Менеджеры СОП • 1с • СпецПО QB • Документы • Почта	Нет	• Microsoft Windows XP Professional (Нет наклейки) • HashTab (вычисление хэш, зачем СОП) • Total Commander 7.03	Microsoft Windows XP Professional Free Commander	• CPU - Intel Pentium 4 CPU 2.80GHz • RAM – 512 • HDD – ST3802110A (80 ГБ)	1 день просрочен	Отключены	Есть	Нет	Сотрудник в отпуске
	Коммерческий директор	Нет	• Microsoft Windows 7 Профессиональная (39HKW) (установлен TYJDP) • Microsoft Office стандартный 2010 • Total Commander 7.03	• Microsoft Windows 7 Профессиональная • Microsoft Office стандартный 2010 Free Commander	• CPU - Core i3 CPU M 380 @ 2.53GHz • RAM – 3072 (2048 + 1024) • HDD – ST9320325AS (320 ГБ)	Отсутствует вообще, инженер обещал исправить на месте	Актуальны	Есть	Нет	Нет

	Офис-менеджер • Интернет-броузер • 1с • Icq и месседжеры • Почта	Нет	Microsoft Windows XP Professional (BTMCJ) • PostgreSQL 8.3 (СУБД, зачем офис-менеджеру) • Radmin Server 3.3 • Radmin Viewer • Total Commander 7.03	Free Commander	• CPU - Pentium Dual CPU E2140 @ 1.60GHz • RAM – 1024 (512 + 512) • HDD – ST380815AS (80 ГБ)	Актуален	Не актуальны	Есть дистрибутивы	Нет	• Постоянный спам на anikina@cas.ru • Общее торможение и подвисание системы
	Юрист • Почта • Документы • Интернет-броузер	Есть	Microsoft Windows XP Professional (HWJH6) • "ГАРАНТ Платформа F1 ЭКСПЕРТ" (не предоставлена лицензия) • Stamp v0.85 (ПО для редактирования штампов) • Total Commander 6.55 • VMware Infrastructure Update	"ГАРАНТ Платформа F1 ЭКСПЕРТ" Free Commander	• CPU - DualCore Intel Pentium, 2000 MHz • RAM – 1015 • HDD – ST3250310AS (250 Гб)	Актуален	Актуальны	Есть	Нет	Нет
	Таможня Упаковка	Есть	Microsoft Windows XP Professional (T6TQB) • Microsoft Office - выпуск для малого бизнеса версии 2003 • Total Commander 7.03	Microsoft Office - выпуск для малого бизнеса версии 2003 Free Commander	• CPU - Intel Celeron D, 2666 MHz • RAM – 1024 • HDD – ST380011A (80 Гб)	Актуален	Отключены	Есть, архивы *.tib	Нет	Сотрудник в отпуске
	Бухгалтерия • 1с • Клиент-банки локально • Документы • Документы в терминале	Нет	• Microsoft Windows XP Professional (наклейки нет) • "ГАРАНТ Платформа F1 ЭКСПЕРТ" (не предоставлена лицензия) • ConsultantPlus – RUNA (не предоставлена лицензия) • Norton PartitionMagic 8.0 • Remote Administrator • Total Commander 6.55 • WinRAR • X-Lite 3.0 (sip-телефон, зачем)	• Microsoft Windows 7 Professional • "ГАРАНТ Платформа F1 ЭКСПЕРТ" • ConsultantPlus – RUNA • Free Commander • 7Zip	• CPU - Pentium Dual CPU E2200 @ 2.20GHz • RAM – 1024 (512 + 512) • HDD – ST3160215AS (160 ГБ)	Актуален	Актуальны	Есть, бухгалтерские документы	Есть	Сложно работать и в терминале с 1с и по сети с документами одновременно
	Главный бухгалтер	Нет	• Microsoft Windows XP	• Microsoft Windows	• CPU - Dual-	Актуал	Актуа	Есть	Нет	Нет

	• 1с • Консультант		Professional (наклейки нет) • "ГАРАНТ Платформа F1 ЭКСПЕРТ" (не предоставлена лицензия) • Total Commander 7.03 • КриптоПро CSP	7 Professional • "ГАРАНТ Платформа F1 ЭКСПЕРТ" Free Commander	Core CPU E5300 @ 2.60GHz • RAM – 1024 • HDD – WD1600AAJS-00L7A0 (160 ГБ)	ен	льны			
	• 1с • Почта • Документы	Нет	Microsoft Windows XP Professional (MTHK6) • "ГАРАНТ Платформа F1 ЭКСПЕРТ" (не предоставлена лицензия) • Adobe Acrobat 5.0 • Microsoft Office Professional Edition 2003 • Total Commander 7.03 • WinRAR	• Microsoft Office Professional Edition 2003 • "ГАРАНТ Платформа F1 ЭКСПЕРТ" • DoPDF • PDFreader • Free Commander • 7Zip	• CPU - Pentium 4 CPU 2.40GHz • RAM – 768 (512 + 256) • HDD – ST380011A (80 ГБ)	Актуален	Актуальны	Есть	Нет	• Медленно печатается документ из терминального сервера Spider • Медленно работает сохранение с терминального сервера Spider • Медленно работает сетевой диск Exchange
	Бухгалтерия Linux в качестве тонкого клиента	нет	Linux в качестве тонкого клиента для работы только в терминальном режиме	Не применимо	Не применимо	Не применимо	Не применимо	Нет	Нет	Нет
	Разработка и тестирование спецПО	• Есть • Находится не в домене	Microsoft Windows XP Professional (VVDYD) • Microsoft Office - профессиональный выпуск версии 2003 • Microsoft Office SharePoint Designer 2007 • 1С:Предприятие 8.1 • 1С:Предприятие 8.2 • Acronis Disk Director Suite • Acronis True Image Home • Active@ File Recovery 7.3 • AllFusion ERwin Data Modeler • CA AllFusion Process Modeler • Microsoft Office 2007 Service	• Microsoft Office - профессиональный выпуск версии 2003 • Необходимо совместно выбрать нужно СпецПО • Free Commander • 7Zip	• CPU - DualCore Intel Pentium E2180, 2000 MHz • RAM – 2039 • HDD – ST3250410AS (250 Гб)	Нет в службах	Актуально	Есть, в основном технические	Нет	Нет

			Pack 3 • Microsoft SQL Server 2005 • Microsoft SQL Server 2008 • Microsoft Visual Studio 6.0 Enterprise Edition • NOD32 FiX v1.9 • SiSoftware Sandra 2002 Standard • Total Commander • Ultra Image Printer 2.0 • VMware Workstation • WinRAR • Множество спецПО для работы с техническими конфигурациями драйверов и аппаратных частей весов, принтеров этикеток							
	Разработка и тестирование спецПО	• Есть • Находится не в домене	Microsoft Windows XP Professional (наклейки нет) • Microsoft Office SharePoint Designer 2007 • Microsoft Office 2007 Service Pack 2 • ABBYY Lingvo • Ability Photopaint Studio 2002 • ACDSee 32 • Acronis True Image Home • Adobe Acrobat 5.0 • avast! Free Antivirus • AXIS Camera Management (разработчик ПО, зачем видеонаблюдение) • CDBF - DBF Viewer and Editor • HauteCapture 1.1 • Microsoft SQL Server 2008 • Microsoft Visual Studio 6.0 Enterprise Edition • Nero 6 Ultra Edition • NOD32 FiX v1.9	• Microsoft Windows XP Professional • Microsoft Office 2007 Service Pack 2 • Необходимо совместно выбрать нужно СпецПО • Free Commander • 7Zip	• CPU - DualCore Intel Pentium E2180, 2000 MHz • RAM – 2039 • HDD – ST3250310AS (250 Гб)	Avast	Отключены	Технические	Нет	Нет

			• NVR Workstation v2.2.56 • Pervasive.SQL V8 Workgroup • RAD Studio • ScrewDrivers Client v4 • The Bat! • Total Commander 6.53 • WinRAR • Множество спецПО для работы с техническими конфигурациями							
	Техническая документация, чертежи, монтаж и установка весов	Нет	Microsoft Windows XP Professional (86B3D) • AutoCAD 2008 • DWG TrueConvert™ • Microsoft Visual Studio 2005 • T-FLEX CAD • WinRAR	• AutoCAD 2008 либо аналог NanoCAD • DWG TrueConvert™ • T-FLEX CAD • 7Zip	• CPU - Celeron CPU 2.66GHz • RAM – 1024 (512 + 512) • HDD – STM3160215AS (160 ГБ)	Актуален	Актуальны	Нет	Нет	Нет
	Офис-менеджер • Учет времени прихода сотрудников • Просмотр камер наблюдения через броузер	Нет	Microsoft Windows XP Professional (FC89J) • BioTime (не предоставлена лицензия) • Microsoft SQL Server Desktop Engine • ScrewDrivers Client v4 • Total Commander 7.03	BioTime Free Commander	• CPU - Celeron CPU E1200 • RAM – 512 • HDD – WD800AAJS-00WAA0 (80 ГБ)	Актуален	Актуальны	Офисные документы	Нет	Нет
	Сергей Опанасюк • Интернет-броузер • Переводчик multilex • Офисные приложения • Roxio Easymedia • Банк-клиент • Adobe digital edition • Total commander (необходимо	Нет Находится не в домене	• Microsoft Windows 7 Professional (YYJYD) • Microsoft Office Standard 2010 • Acronis Disk Director Suite • Acronis True Image Home • Microsoft SQL Server 2005 • MultiScreen • ScrewDrivers Client v4 • Total Commander 7.03	Free Commander	• CPU - Mobile DualCore Intel Core i3-330M • RAM – 3760 • HDD – WDC WD3200BEVT-26A23T0 (320 Гб)	Антивируса нет	Актуальны	Нет	Нет	Нет

	заменить на Free Commander)									
	Президент компании	• Есть • Находится не в домене	Microsoft Windows 7 Home Premium Microsoft Office Professional Plus 2007	Microsoft Office Professional Plus 2007	• CPU - Mobile Intel Core 2 Duo P8700, 2533 MHz • RAM – 2042 • HDD – WD3200BEVT-22ZCT0 (320 GB)	Антивируса нет	Обновлений нет	Есть документы (на корейском языке)	Нет	Нет
Сервер MS Windows Spider 1c										
	-	-	• Microsoft Windows Server 2003 R2 Standard Edition (лицензия только на trial ent 180 day) • 1С:Предприятие 7.7 для SQL (не предоставлена лицензия) • Acronis Backup & Recovery 10 • Acronis Universal Restore • Adobe Illustrator CS3 • AVRStudio4 • Microsoft Office Enterprise 2007 • Microsoft SQL Server 2000 • Proteus 6 Professional • Readiris Pro 7.0 • R-Studio 5.2 • Total Commander 7.03	• Microsoft Windows Server 2003 R2 Standard Edition • 1С:Предприятие 7.7 • Acronis Backup & Recovery 10 • Microsoft Office Enterprise 2007 • Microsoft SQL Server 2000 Free Commander	• CPU - 4 x Intel Xeon CPU E5405 @ 2.00GHz • RAM – 3996 • HDD – XENSRC PVDISK SCSI Disk Device (43 ГБ), HDD XENSRC PVDISK SCSI Disk Device (54 ГБ)	Актуален	Актуальны	-	-	-
Склад										
	Работает на локальном сервере терминалов занимается ПО для весов. Локальным ПО не пользуется	Нет. Но на рабочей станции есть администраторы паролей к которым	Microsoft Windows XP Total Commander 7.03	Microsoft Windows XP	• CPU – Celeron 1.7GHz • RAM – 256 • HDD – 30 Гб	Антивирус не актуален	Актуальны	Нет	Нет	Старая и слабая рабочая станция

		никто не знает								
	Компьютер настроен как тонкий клиент. Работает с 1С на удаленном сервере, печать документов на локальный принтер.	Нет	Linux в качестве тонкого клиента	-	Не применимо	Не применимо	Не применимо	Не применимо	Нет	Вылетает 1с на терминальном сервере Spider
	Работает в 1С на удаленном сервере. Компьютер используеться как тонкий клиент	Нет	Linux в качестве тонкого клиента	-	Не применимо	Не применимо	Не применимо	Не применимо	Нет	Нет
	Отвечает за склад Отправляет фотографии по почте личной через веб-интерфейс	Нет	Linux в качестве рабочей системы	Все ПО свободное	Не работает с сервером	Не применимо	Не применимо	Нет	Нет	Иногда интернет работает медленно

11. Стратегические рекомендации по организации серверной структуры

- Исходя из результатов аудита, можно видеть, что множество открытых ресурсов Компании являются стандартными и уязвимости в них существуют из-за разрастания структуры по горизонтали. В данных случаях оптимальным является централизация структуры стандартных ресурсов в одном едином узле, который гораздо легче и надежнее защитить от любых форс-мажоров. Предлагается реализовать центральный терминальный сервер для организации работы со следующими ресурсами:

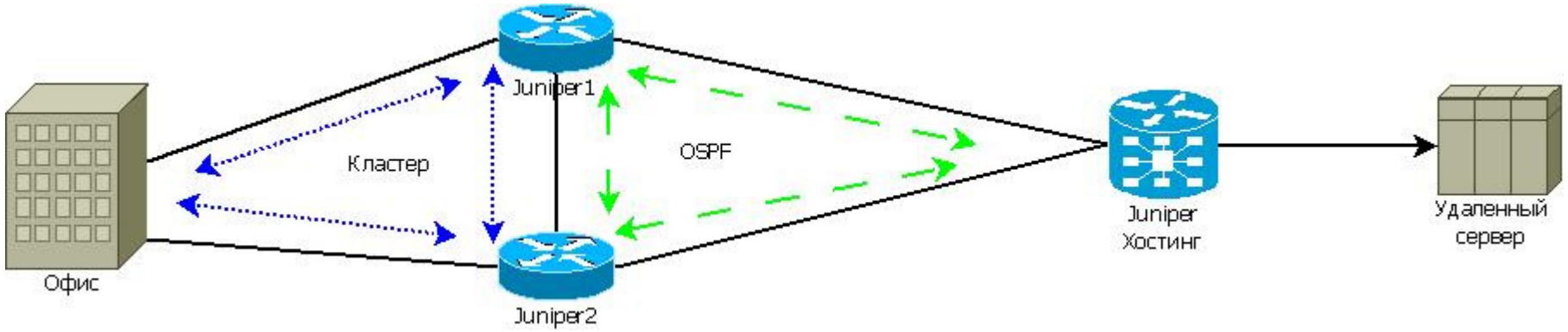
- Документы Компании с распределением прав доступа
- Базы и клиенты 1с
- Почтовые клиенты
- Почтовый сервер
- Офисные приложения

- Для выполнения данной задачи предлагается аренда удаленной серверной структуры в рамках услуги «Бизнес сервер». Это аренда эксклюзивного мощного серверного оборудования с лицензионным программным обеспечением, стабильными каналами связи и электропитания, защитой баз данных и полным спектром сопутствующих услуг.

Преимущества услуги для Вашей компании:

- ✓ **Выделенный для Вас сервер**, построенный на профессиональном оборудовании;
- ✓ Сервер расположен на закрытой и **защищенной площадке класса Tier3 с обеспечением качества услуги 99,999%**;
- ✓ Сервер **обеспечен бесперебойным питанием** и резервированием канала Интернет;
- ✓ Информационную защиту обеспечивает **аппаратный кластер Juniper Network®**;
- ✓ Настроенное **автоматическое копирование** данных;
- ✓ **Кнопка экстренного выключения** сервера;
- ✓ Сервисный контракт на оборудование, заключенный с производителем, что позволяет произвести **экстренную замену** вышедшего из строя аппаратного обеспечения **в режиме 24/7/4**.
- ✓ Сервер подключен к промышленной **Системе Хранения Данных Hitachi** AMS2100. Преимущества данной системы:
  - высокая надёжность и отказоустойчивость
  - высокая доступность данных
  - мощные средства управления и контроля
  - высокая производительность
  - высокая масштабируемость
  - сервисная поддержка производителя NBD (Next Business Day).

- ➢ Предлагается реорганизовать структуру интернет-шлюзов в ЦО. Необходимо убрать лишние шлюзы, оставив только надежные аппаратные устройства профессионального уровня. Для этого необходима закупка дополнительного устройства Juniper. При внедрении каждый канал интернет будет подключен к каждому Juniper, организуя, таким образом кластерное соединение. Это позволит достичь следующих преимуществ:
  - ✓ Отказоустойчивость шлюзов – при падении одного канала интернет или выхода из строя шлюза – пользователи переключаются на резервную систему практически незаметно
  - ✓ Технология OSPF – может быть применена в данной схеме для удаленных серверов. Организуется внутри шифрованных туннелей, образуя «треугольник». В случае выхода из строя одного из каналов интернет – сотрудники, работающие на удаленном сервере, не прерывают работу ни на секунду. Таким образом нет простаивания бизнес-задач из-за нестабильных провайдеров интернет



- Предлагается внедрить доменную структуру Microsoft, убрав текущую систему Linux LDAP. В данную доменную структуру войдут те рабочие станции, которые требуют полноценного интерфейса пользователя для выполнения бизнес-задач и не могут быть превращены в «тонкие» терминальные клиенты (например, компьютеры разработчиков, дизайнеров и т.д.). Внедрение полноценной доменной структуры потребует закупку двух серверных лицензий, 35 лицензий CAL Microsoft. Данная структура позволит:
  - ✓ Вести контроль за рабочими станциями, иметь полную картину действий пользователя
  - ✓ Гибко назначать права на рабочих местах, ограничивать возможности доступа и интерфейс пользователя
  - ✓ Централизованно управлять обновлениями, установкой ПО, авторизацией пользователей
  - ✓ Распределять новые периферийные устройства в автоматическом режиме
  - ✓ Резервный контроллер домена можно разместить рядом с удаленным сервером, что позволить страховать доменную структуру и интегрировать удаленный сервер в нее, используя те учетные данные и политики, которые распространены в центральном офисе

- При переводе максимального количества пользователей на удаленный сервер, их рабочие места можно превратить в специализированные «тонкие» терминальные клиенты. Например, взять для этой цели компьютеры, отмеченные при аудите как «не имеющие лицензии Windows». Для централизованного управления данными «тонкими» клиентами оптимальнее всего внедрить централизованный сервер Unix, который будет предоставлять загрузку ОС по технологии PXE. Это позволит собрать единую шаблонную операционную систему и автоматически запускать ее на «тонких» клиентах. Таким образом администратор имеет единый центр управления «тонкими» клиентами.

12. Распределение прав на удаленном файловом сервере

Предложение по структуре защищенного файлового сетевого хранилища с разграничением по правам доступа

Соответствие пользователей группам							
			Принадлежность к группе				
		Группы пользователей					
Отдел	**Пользователь (логин)**	**Группа1**	**Группа2**	**Группа3**	**Группа4**	**Группа5**	**Группа6**
Дирекция							
Технический персонал и разработка							
Бухгалтерия							
Сотрудники отдела продаж							
Склад							
Офис-менеджер							

Права групп на папки файл-сервера						
		Нет доступа				
		чтение				
		чтение + запись				
Ресурсы	**Доступ для групп**					
	Группа1	**Группа2**	**Группа3**	**Группа4**	**Группа5**	**Группа6**
Data						
Users (персональные папки пользователей)		Владелец – полный доступ Остальные – нет доступа				
User1						
User2						
User3						
User4						
User5 и т.д.						
Дирекция						
Технические данные						
Бухгалтерия						
СОП						
Склад						
Офис						
Exchange						