Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ЛЕСОСИБИРСКИЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ -
филиал Сибирского федерального университета

Высшей математики, информатики и естествознания
кафедра

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

09.03.02 Информационные системы и технологии
код и наименование направления

ПРОЕКТИРОВАНИЕ АВТОМАТИЗАРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ РЕСУРСАМИ КОМПЬЮТЕРНЫХ СЕТЕЙ

тем а

Руководитель Е.В. Киргизова
инициалы, фамилия

Выпускник А.В. Кононов
инициалы, фамилия

Лесосибирск 2019

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ЛЕСОСИБИРСКИЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ -
филиал Сибирского федерального университета

Высшей математики, информатики и естествознания
кафедра

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

09.03.02 Информационные системы и технологии
код и наименование направления

ПРОЕКТИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ РЕСУРСАМИ КОМПЬЮТЕРНЫХ СЕТЕЙ
тема

Работа защищена « 24 » июня 2019 г. с оценкой « хорошо »

Председатель ГЭК _____ (подпись) Е.Г. Кучумов (инициалы, фамилия)

Члены ГЭК

_____ (подпись) Т.В. Захарова (инициалы, фамилия)

_____ (подпись) Е.В. Киргизова (инициалы, фамилия)

_____ (подпись) А.А. Степанов (инициалы, фамилия)

_____ (подпись) В.В. Фирер (инициалы, фамилия)

Руководитель _____ (подпись) Е.В. Киргизова (инициалы, фамилия)

Выпускник _____ (подпись) А.В. Кононов (инициалы, фамилия)

Лесосибирск 2019

РЕФЕРАТ

Ключевые слова: информационная система, база данных, информационные ресурсы, программное обеспечение, аппаратное обеспечение.

Цель: разработка системы управления ресурсами компьютерных сетей.

Объект исследования: информационная система ООО «Монитор».

Предмет исследования: системы мониторинга программно-аппаратной среды.

Работа содержит 3 главы, введение, заключение, список использованных источников. В практической части работы проведена разработка информационная система учета компьютерной техники и программного обеспечения в локальной сети предприятия.

64 стр., 36 рис., 12 табл., 20 источников, 1 приложение.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность

Специфика использования информационных систем в настоящее время связана с одновременным функционированием разнородных устройств и систем, обеспечивающих работу системных и прикладных программных комплексов. Задача учета ресурсов компьютерных сетей является актуальной в связи с необходимостью мониторинга нагрузки на сетевые ресурсы, анализа их производительности, изучения возможностей оптимизации и распределения нагрузки на ИТ-оборудование. Оптимально распределенная нагрузка на сетевые ресурсы позволит обеспечить производительность работы информационных систем, повысить эффективность работы всех подразделений организации.

Цель данной работы заключается в разработке системы управления ресурсами компьютерных сетей.

Задачи работы:

- анализ технологий учета компьютеров и программного обеспечения в доменной сети;

- определение области применимости для мониторинга программно-аппаратной среды в условиях исследуемого предприятия;

- рассмотрение возможных решений в области автоматизации мониторинга программно-аппаратной среды;

- разработка программного обеспечения для управления ресурсами компьютерных сетей.

Объект исследования: информационная система ООО «Монитор».

Предмет исследования: системы мониторинга программно-аппаратной среды.

Методы исследования: изучение литературных источников, нормативно-правовой базы, изучение технической документации средств

защиты информации, анализ состояния работы с персональными данными, сравнения, включенного наблюдения.

Работа состоит из трех глав, заключения, списка использованных источников и приложений. В первой главе проведен анализ теоретических аспектов автоматизации мониторинга программно-аппаратной среды, определены задачи мониторинга программно-аппаратной среды. В главе 2 проведен анализ существующих методов мониторинга программно-аппаратной среды. В главе 3 проведено описание процесса проектирования информационной системы программно-аппаратной среды. Далее проведена оценка экономической эффективности проекта.

1. Теоретические обоснование необходимости мониторинга программно-аппаратной среды

1.1 Актуальность задач учета компьютеров и программного обеспечения в доменной сети

Задачи по инвентаризации состояния информационной системы обусловлены необходимостью анализа активности пользователей, наличия на рабочих станциях программного обеспечения, не разрешенного к использованию в условиях предприятий, анализа состояния аппаратного комплекса и его соответствия системным требованиям для работы прикладных программных систем. Также данная задача может использоваться для анализа угроз нарушения функциональности.

Угрозы нарушения функциональности информационно-программного обеспечения компьютера можно сгруппировать по нарушаемым свойствам безопасности, к которым относятся [18]:

- угроза конфиденциальности;
- угроза целостности;
- угроза доступности.

Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой.

К угрозам, создающим опасность конфиденциальности информации, относится утечка информации, под которой понимается неконтролируемое распространение защищаемой информации в результате её разглашения, несанкционированного доступа к ней или получения защищаемой информации заинтересованными субъектами (заинтересованными

субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо) [8].

Проведем классификацию угроз конфиденциальности информации.

1. Разглашение информации
   1.1. Преднамеренное разглашение (прямой умысел).
   1.2. Непреднамеренное разглашение (по неосторожности).
2. Несанкционированный доступ к информации
   2.1. Физический доступ.
   2.2. Программно-аппаратный доступ.
   2.3. Программный доступ.
3. Перехват информации (утечка информации по техническим каналам)
   3.1. Перехват информации, обрабатываемой техническими средствами.
   3.2. Перехват разговоров, ведущихся в выделенных (защищаемых) помещениях.
   3.3. Перехват информации, передаваемой по каналам связи.
4. Хищение носителей информации.

Угрозы целостности - угрозы, при реализации которых информация теряет заранее определенные системой вид и качество.

Самым ценным ресурсом являются документы. Это объясняется содержанием в них конфиденциальной информации, для безопасности которой организована вся система политики безопасности.

Вторым по важности объектом становится сервер баз данных, то есть среда хранения документов.

Третий сектор – это сервер операционной системы и электронного документооборота. К нему относятся операционная система, оболочка информационного пространства (интерфейс), протоколы передачи данных и т.д. Стоит отметить, что при выходе из строя данных компонентов целостность данных не нарушается.

Четвертый, самый некритичный сектор - аппаратная система (каналы связи между компонентами, аппаратный межсетевой экран), выход из строя

которой не приведет к разрушению хранимых документов, а неисправные комплектующие и провода можно заменить на новые.

Угрозы доступности характеризуют возможность доступа к хранимой и обрабатываемой информации в любой момент. Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих компоненты информационной среды.

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования).

Все атаки на информационно-программное обеспечение компьютера предприятия можно условно разделить на три вида: локальные, удаленные и атаки на потоки данных [11].

В случае локальной атаки злоумышленник имеет физический доступ к информационным ресурсам компьютера. Подобные атаки характерны внутренних преднамеренных угроз. К ним относятся получение доступа на этапе загрузки операционной системы, атаки на средства аутентификации и т.п.

Удаленная атака осуществляется пользователем, не имеющего прямого доступа к интересующим его средствам вычислительной техники. Здесь стоит говорить и о внешних преднамеренных угрозах, к которым могут относиться атаки на маршрутизатор, сбор сведений о системе, заражение вредоносными программами и т.д.

Под атакой на поток данных подразумевается событие, когда между двумя компьютерами идет активный обмен данными по сети, и злоумышленник атакует сегмент сети или ее узел, находящийся между двумя взаимодействующими компьютерами. Такой вид атак реализует как внутренние преднамеренные угрозы, так и внешние. Специалисты разделяют атаки на поток данных на пассивные (злоумышленник, никак не выдавая свое

присутствие, перехватывает все электронные документы для последующего изучения, но не имеет возможности модифицировать передаваемые сообщения) и активные (злоумышленник предпринимает ряд активных действий, направленных на перехват передаваемых электронных документов, то есть получает возможность модификации сообщений или передачи собственных данных).

Подводя итог, отметим, что возможные угрозы эталонного состояния информационно-программного обеспечения компьютера классифицируются в соответствии с главными характеристиками информации – доступность, целостность, конфиденциальность. Кроме того, возможно разделение атак на локальные, удаленные, атаки на поток данных.

Для реализации надежной системы защиты информационно-программного обеспечения компьютера необходимо определить требования к данной системе:

– необходимо обеспечивать защиту на всех этапах сбора, хранения, обработки, передачи и использования информации;

– система защиты должна быть привязана к целям и задачам защиты информации для конкретного состава и структуры информационно-программного обеспечения компьютера;

– обязательное обеспечение целостности системы защиты, подразумевающей содержание всех необходимых составляющих; наличие логических связей между компонентами, направленных на реализацию эффективного функционирования системы;

– система защиты информационно-программного обеспечения компьютера должна быть логически, технически и экономически обоснованной.

– принципы функционирования системы защиты информационно-программного обеспечения компьютера должны быть понятны; сама системы – удобной в эксплуатации и управлении.

– система защиты информации должна быть эффективной и достаточно гибкой, способной к настройке при изменении компонентов ее составных частей, технологии обработки информации и условий защиты.

1.2 Анализ организационной структуры предприятия

В качестве предметной области в рамках данной работы рассматривается деятельность ИТ-специалистов в части сервисного обслуживания компьютерной техники, мониторинга заявок на проведение данных работ, выявление основных нарушений в ходе выполнения операций сервисного обслуживания техники, выявление нарушений правил эксплуатации техники.

Бесперебойное функционирование информационной системы предприятия в настоящее время определяет эффективность его деятельности в целом, так как большинство бизнес-процессов в настоящее время автоматизировано и перебои в работе какого-либо из сегментов вычислительной техники приведут к задержкам значительного количества бизнес-процессов.

Основными направлениями использования информационных технологий в ИТ-отделах в рамках оказания технической поддержки пользователям являются:

- оказание технической поддержки пользователям;
- мониторинг состояния ИТ-инфраструктуры предприятия;
- мониторинг функционирования прикладного программного обеспечения;
- мониторинг отработки заявок пользователей.

Рассмотрим общие требования к функционалу данного типа программного обеспечения, проведем анализ его характеристик.

К основным задачам служб технической поддержки специалистами ИТ-подразделений относят [2]:

- вопросы ремонта и обслуживания компьютерной техники отдельных подразделений и служб предприятия;

- вопросы установки, настройки программного обеспечения на рабочих станциях специалистов отдельных подразделений и служб предприятий

- вопросы функционирования локальной сети предприятия;

- вопросы обеспечения информационной безопасности;

- вопросы функционирования прикладного ПО.

Рассмотрим порядок обращения сотрудников в службу технической поддержки ИТ-подразделения предприятия.

При неисправности оборудования, прежде всего, необходимо проверить правильность его подключения и наличие электропитания.Далее необходимо позвонить в сервисную службу ИТ-отдела предприятия и описать проблему, либо составить служебную записку на имя начальника ИТ-подразделения, в которой указать:

1. причину обращения;
2. номер помещения, где находится рабочая станция;
3. фамилия контактного лица и телефон;
4. дату составления;
5. подпись руководителя подразделения или его заместителя.

Специалисты службы технической поддержки, выяснив проблему, определяют пути решения (либо дистанционно – с использованием средств удалённого доступа, либо непосредственно на рабочем месте пользователя или путем направления технического средства в сервисный центр.

Рассмотрим документооборот в процессе направления техники в ремонт.

Специалист ИТ-подразделения определяет характер и причины неисправностей, составляет акт о выходе из строя оборудования и направляет

его в сервисный центр. При получении его из ремонта проводит диагностику и в случае устранения неисправности, вводит в эксплуатацию.

В случае, если проблема неустранима, производится подготовка документов для списания оборудования согласно принятым стандартам бухгалтерского учета на предприятии.

Поддержка функционирования программного обеспечения предполагает следующие направления:

- поддержка системного ПО (в рамках которой решаются вопросы , связанные с функционированием операционных систем, драйверов оборудования, системных утилит и др.);

- поддержка функционирования прикладного ПОв части прикладного функционала (в случае возникновения проблем, например, с некорректными результатами расчетов или других ошибок пользовательского функционала);

- поддержка ПО общего назначения (вопросы, связанные с работой офисного, почтового ПО);

- вопросы, связанные с обеспечением информационной безопасности (вопросы разграничения доступа к системе, файловым ресурсам, системы антивирусной защиты).

Таким образом, основными этапами работы службы технической поддержки являются:

- предварительный прием обращения;

- определение профиля обращения;

- направление обращения к специалистам согласно профилю проблемы;

- устранение проблемы;

- оформление документации.

Сервисное обслуживание компьютерной техники может проводиться как по заявкам пользователей, так и в случае возникновения неисправности.

Принципиальная схема локальной вычислительной сети ООО «Монитор» приведена на рис.2 На рисунке 2 показано, что с сервера баз

данных, по каналам связи передается информация на рабочие места, где в свою очередь сотрудники формируют отчет и распечатывают его на принтере.

На рис. 2 приведена схема технической архитектуры автоматизированной системы ООО «Монитор».

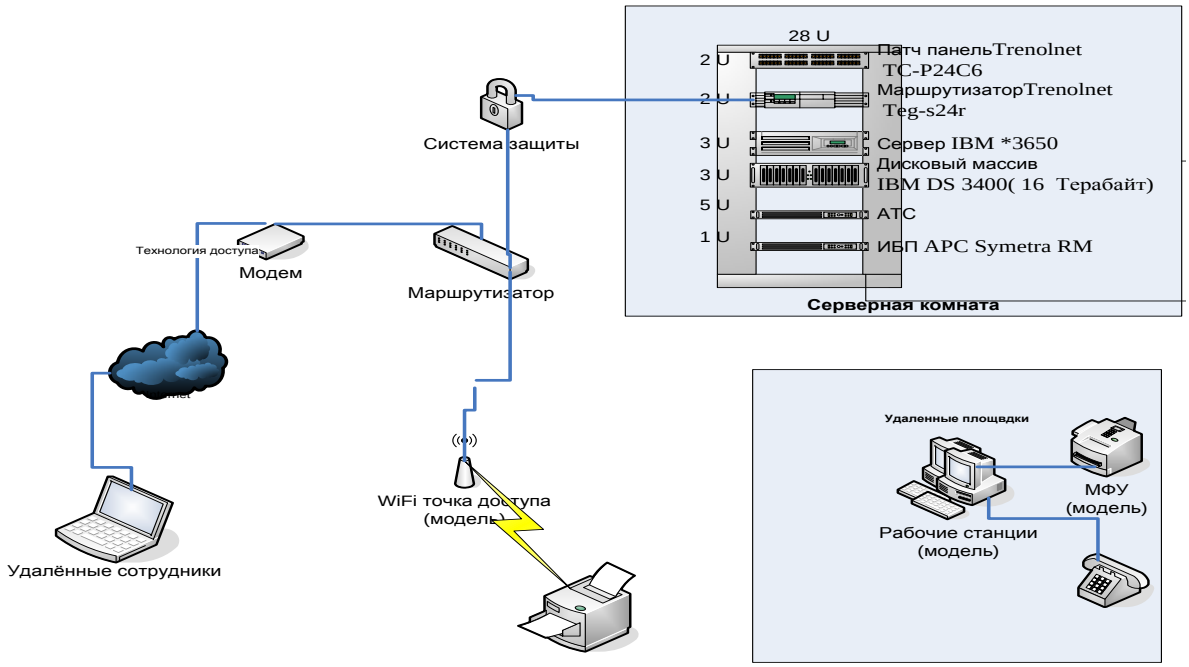


Рисунок 1 - Принципиальная схема компонент локальной сети ООО «Монитор»

Рассмотрим более подробно состав технической архитектуры:

Основной сервер компании состоит из:

1. Патч -панель:Trenolnet TC-P24C6
2. Маршрутизатор: Trenolnet Teg-s24r
3. Сервер: IBM 3650
4. Дисковый массив IBM DS 3400(объем 16 Терабайт)
5. ИБП APC Symetra RM
6. Модем ADSL D-Link DSL-2500U
7. Wi-Fi- точка доступа D-Link DFL-900AP+
8. Система защиты ProxyServer UserGate

Основные параметры локальной ООО «Монитор» приведены в таблице 1. Технические характеристики сервера IBM x3550, используемого в работе специалистов, приведена в таблице 2, характеристики рабочей станции специалиста приведены в таблице 3.

Таблица 1 - Основные параметры локальной сети ООО «Монитор»

№	Наименование параметра	Значение
1	Общее количество портов локальной сети	96
2	Общее количество активных подключений локальной сети	54
3	Количество коммутаторов (48 портов)	2
4	Наличие АТС (внешних/внутренних линий)	14/48
5	Количество рабочих станций пользователей	38
6	Количество технологических подключений к сети (сетевые принтеры, сканеры, МФУ, система видеонаблюдения и др. устройства, не являющиеся компьютерами, но использующие локальную сеть)	16
7	Источник бесперебойного питания Smart UPS 2000 (используются для подключения коммутаторов и серверов)	2
8	Телекоммуникационная стойка	2
9	Кондиционер	1

Таблица 2 - Технические характеристики сервера IBM x226

Характеристика	Значение
Процессор	4 x Intel Xeon-2.67GHz (667MHz,2x2MB L2 Cache),
Оперативная память	4 x 2048MB PC2-5300 667MHz DDR2 ECC DIMM Fully Buffered
HDD	4 x 1024 GB SATA
Дополнительно	DVD/ RW

Таблица 3 - Технические характеристики рабочей станции специалиста

Характеристика	Значение
Периферия	Есть
Монитор	Acer G226HQLHbd, 21,5’, 1920x1080 (16:9), 8мс, LED, 250 кд/м^2
Описание	Офисный ПК
Процессор	Intel (TM) Core i5 G6600
ОЗУ	4GB
HDD	500ГБ SATA3

Видеосистема	ATI Radeon X1200
Сеть	1GB/c
Габариты	~ 420 x 195 x 530мм

В локальную сеть ООО «Монитор» входят компоненты:

- серверы;

- рабочие станции пользователей;

- сетевые принтеры.

Таблица 4 - Перечень прикладных задач, требующих использования сетевых технологий

Наименование задачи	Технологическое решение	Расположение
АИС Бухгалтерского учета	1С: Предприятие 8.2 (для удаленных офисов – тонкий клиент)	Сервер 1С:Предприятие, локальная сеть ООО «Монитор»
1С 8.2: Зарплата и Управление Персоналом	1С: Предприятие 8.2 (для удаленных офисов – тонкий клиент)	Сервер 1С:Предприятие, локальная сеть ООО «Монитор»
Работа системы антивирусной защиты	Средства администрирования Kaspersky	Сервер АВЗ
АРМ Экономиста	1С: Предприятие	Windows 2008 Server
Файловый обмен	Файловый сервер	Windows 2008 Server
АРМ Управление СКУД	СКУД «Орион»	Windows 2008 Server
Система электронного документооборота	Lotus Domino	Lotus Domino Server на сервере Windows 2008
Сдача отчетности в государственные органы	MS SQL Server	Сервер, локальная сеть ООО «Монитор»
Сервер лицензий 1С	1С: Предприятие Hasp	Сервер лицензий 1С:Предприятие
Web-сервер предприятия	Apache + MySQl	Web-сервер, локальная сеть ООО «Монитор»
АРМ Учет техники	MS SQL Server	Сервер, локальная сеть ООО «Монитор»

Схема программной архитектуры ООО «Монитор» приведена на рисунке 2.

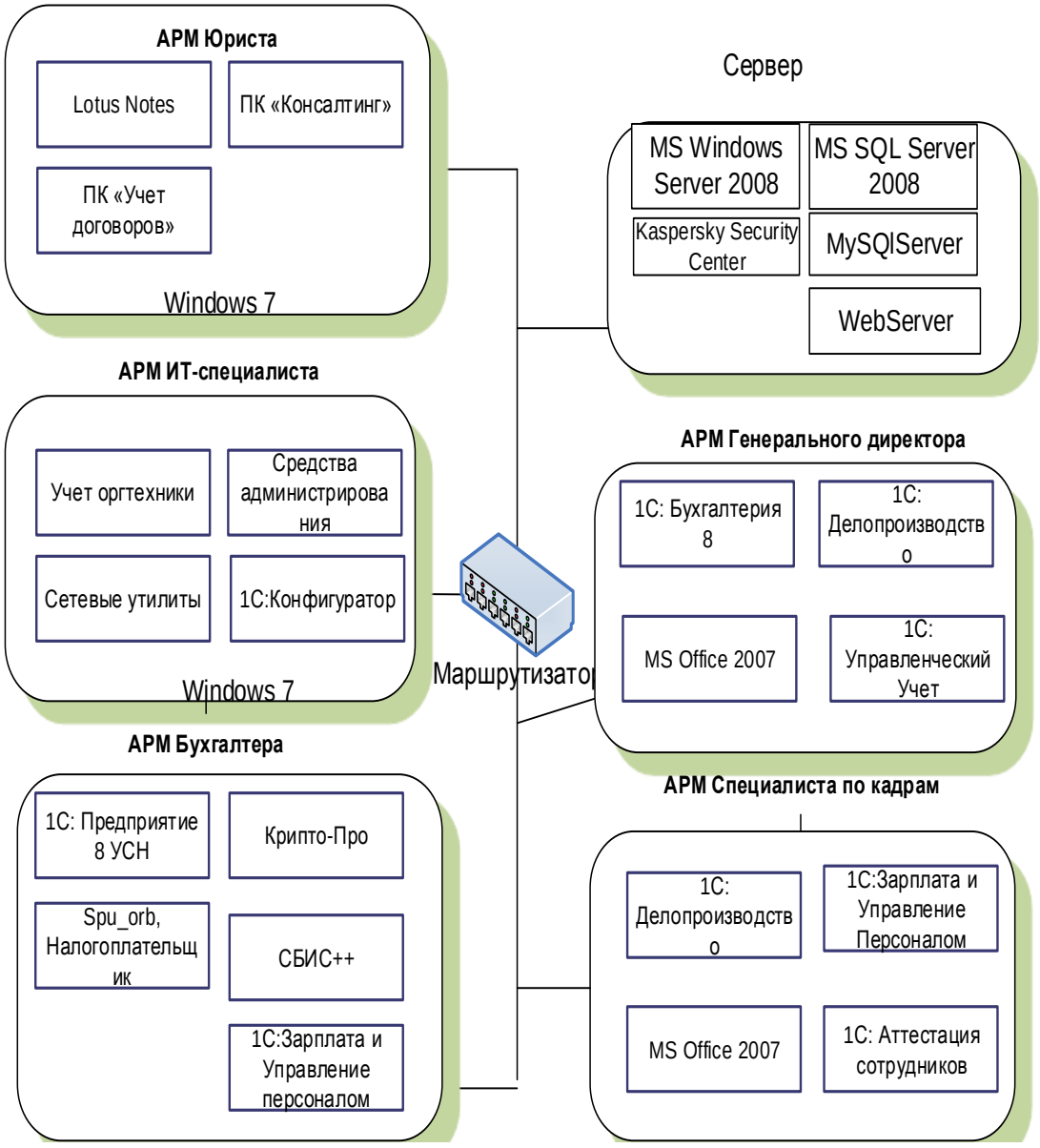


Рисунок 2 - Схема программной архитектуры локальной сети ООО «Монитор»

Обеспечение полноценного функционирования такого набора программных комплексов возможно на основе построения сети, в которой одновременно реализовано несколько серверных решений. Таким образом, программная архитектура сети ООО «Монитор» предполагает одновременно

несколько серверных решений, рабочие станции пользователей одновременно включены в несколько подсетей с использованием различных протоколов.

Перечень серверов, используемых в локальной сети ООО «Монитор», приведен в таблице 5.

Таблица 5 - Перечень серверов, используемых в сети ООО «Монитор»

Наименование сервера	Аппаратная платформа	Операционная система
Контроллер домена	IBM x3550	Windows 2008 Server
Файловый сервер	IBM x3550, виртуальная среда	Windows 2008 Server
Сервер АВЗ	IBM x3550, виртуальная среда	Windows 2008 Server

В рамках данной работы проведено исследование задачи учета компьютеров и программного обеспечения в доменной сети для ООО «Монитор».

Задачи учета компьютеров и программного обеспечения в доменной сети в условиях информационной системы ООО «Монитор» предполагают необходимость решения задач:

- контроль устанавливаемого программного обеспечения;

- контроль отработки политик, связанных с установкой программных решений;

- контроль производительности компьютеров;

- инвентаризация программных продуктов с целью контроля лицензий.

Таким образом, программный продукт по автоматизации учета компьютеров и программного обеспечения в доменной сети должен выполнять задачи:

- мониторинг состояния программной и аппаратной среды;

- получение оперативной информации по аппаратному и программному обеспечению;

- формирование отчетной информации.

В компетенцию отдела информационных технологий входят вопросы, связанные с обеспечением деятельности ИТ-инфраструктуры предприятия. Далее рассмотрим вопросы деятельности ИТ-отдела более подробно.

ИТ-отдел ООО "МОНИТОР" находится в подчинении технического директора. Спецификой деятельности специалистов по информационным технологиям является то, что в их функции входит не только поддержка функционирования стандартных ИТ-объектов (системная инфраструктура, прикладное ПО), но и обеспечение функционирования программной части и системы информационной безопасности специализированного производственного оборудования, что требует специальной квалификации и повышает уровень ответственности.

Основными задачами отдела являются:

- Формирование, использование и защита информационных ресурсов, а также организация доступа к ним специалистов ООО "МОНИТОР".

- Обеспечение бесперебойного функционирования ИТ-инфраструктуры предприятия;

- Обеспечение функционирования программного обеспечения специального производственного оборудования;

- Обеспечение функционирования онлайн сервисов и поддержка функционирования сайта ООО "МОНИТОР".

Структура ИТ-отдела приведена на рис.6. Как показано на рисунке 6, начальник ИТ-отдела находится в подчинении технического директора, в структуре отдела выделены 2 группы (ТО и ТС – технических, общесистемных и телекоммуникационных систем, ППО, в состав которой входят специалисты, работающие с прикладным программным обеспечением).

В таблице 6 приведен перечень функциональных обязанностей специалистов ИТ-отдела ООО "МОНИТОР".

Таблица 6 - Перечень функциональных обязанностей специалистов ИТ-отдела ООО "МОНИТОР"

Наименование подразделения	Кол – во единиц	Функциональные обязанности
Начальник ИТ-отдела	1	Координация деятельности отдела, документооборот со сторонними организациями по вопросам работы ИТ-отдела
Специалист по защите информации	4	Документооборот в области защиты информации, подготовка документов в области информационной безопасности, взаимодействие с руководством Администрации по вопросам соблюдения требований защиты информации, технологические сопровождение аппаратных средств информационной безопасности, сопровождение технологии ЭДО, обеспечение защиты программной части специализированного оборудования
Администратор баз данных	4	Администрирование баз данных программных комплексов, определение ролей пользователей в программных комплексах, учет заявок на предоставление прав доступа к информационным ресурсам
Специалист по обслуживанию технических средств	7	Техническое обслуживание СВТ, закупка запчастей, составление отчетности по обеспеченности средствами вычислительной техники специалистов
Системный администратор	3	Обслуживание серверного оборудования, администрирование ресурсов ЛВС
Специалисты по сопровождению ПО	4	Установка, настройка прикладного ПО и его обновлений, консультирование пользователей по работе с прикладным ПО, взаимодействие с разработчиками
Специалисты по сопровождения спецоборудования	4	Сопровождение программной части работы оборудования, связанного с обеспечением перевозок

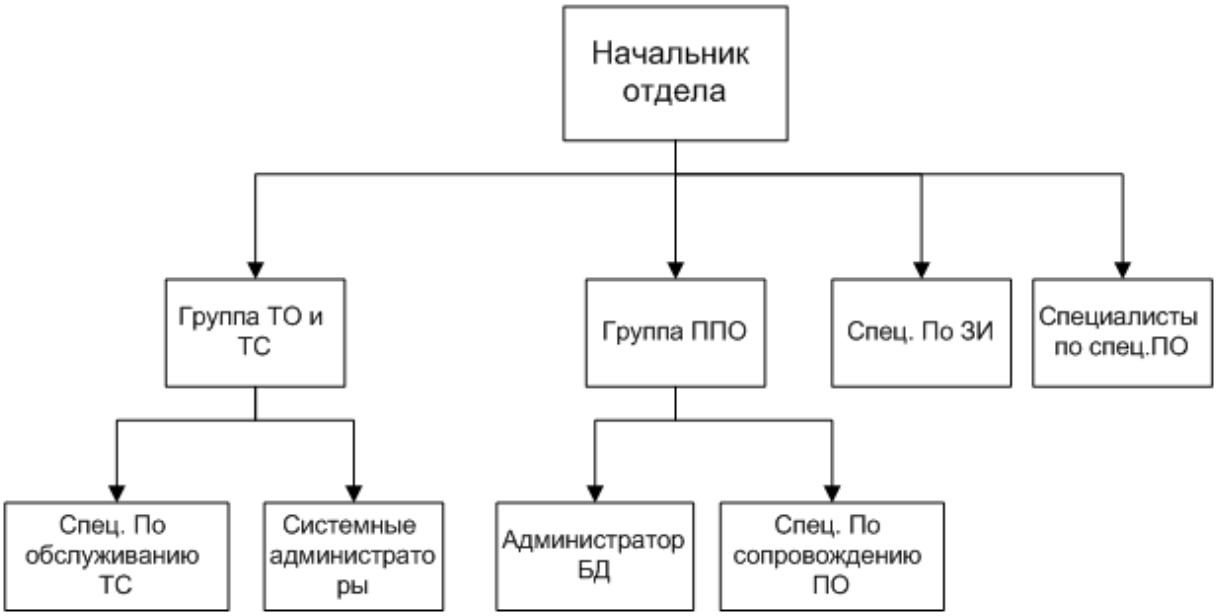


Рисунок 3 - Организационная структура ИТ-отдела ООО «Монитор»

Таким образом, в компетенцию ИТ-отдела входят вопросы поддержки функционирования аппаратных и программных комплексов предприятия, что предполагает необходимость оперативного реагирования на возникающие проблемы. Специфика ИТ-инфраструктуры предприятия такова, что ее компонентами являются достаточно разнородные решения и для исправления проблем необходимо оперативное привлечение профильных специалистов.

Как показано на рисунке 3, в структуру ИТ-отдела ООО «Монитор» входят специалисты:

- Группы ремонта, в функции которых входят вопросы системного администрирования, ремонта техники и обеспечение функций работы систем связи;

- Группы по работе с программным обеспечением, в функции которой входят вопросы сопровождения и разработки прикладного РО, включая установки обновлений, администрирования баз данных, взаимодействия с разработчиками;

- Группы по защите информации, в функции которой входят вопросы организационного и технологического сопровождения информационной безопасности.

2.Проектная часть

В настоящее время в связи с введением стандартизации на состав программного и аппаратного обеспечения в информационных системах предприятий специалистами ИТ-отдела, а также сотрудниками профильных отделов создаются стандарты наличия установленного программного и аппаратного обеспечения на компьютерах пользователей, что может быть связано со следующими моментами:

- мониторинг количества имеющихся лицензий и фактически установленных программ;

- мониторинг наличия посторонних программных продуктов;

- мониторинг качественных характеристик аппаратного комплекса рабочих станций;

- мониторинг системы безопасности;

- мониторинг процесса отработки административных политик.

Учет аппаратных средств на рабочих станциях пользователей в ручном режиме представляет собой сложную задачу, так как затруднен сбор данных. Таким образом, для учета устройств, установленных на компьютерах пользователей необходимо применять специализированные средства диагностики.

В организациях, имеющих сложную филиальную структуру, сложную задачу представляет контроль состояния информационной системы, что предполагает необходимость использования специализированных программных решений.

В настоящее время задача удаленного мониторинга программно-аппаратной среды реализована в программных продуктах различных типов:

- специально предназначенном для этого программном обеспечении;

- программном обеспечении, предназначенном для системных администраторов;

- антивирусных программных решениях;

- средствах защиты данных.

Рассмотрим функционал программных решений по мониторингу программно-аппаратной среды.

2.1. Реализация задач мониторинга программно-аппаратной среды с использованием средств антивирусной защиты

Современные корпоративные антивирусные решения обладают дополнительным функционалом, который может быть использован и для рассматриваемой в рамках данной работы задачи. Достоинство использования решения подобного типа для задач мониторинга в том, что не требуется приобретать дополнительные решения для удаленного мониторинга системы, так как они реализованы в пакете антивирусной системы.

Далее приведем примеры получения информации с использованием средств администрирования антивирусной системы. На рисунке 4 приведено окно с информацией об удаленной рабочей станции.

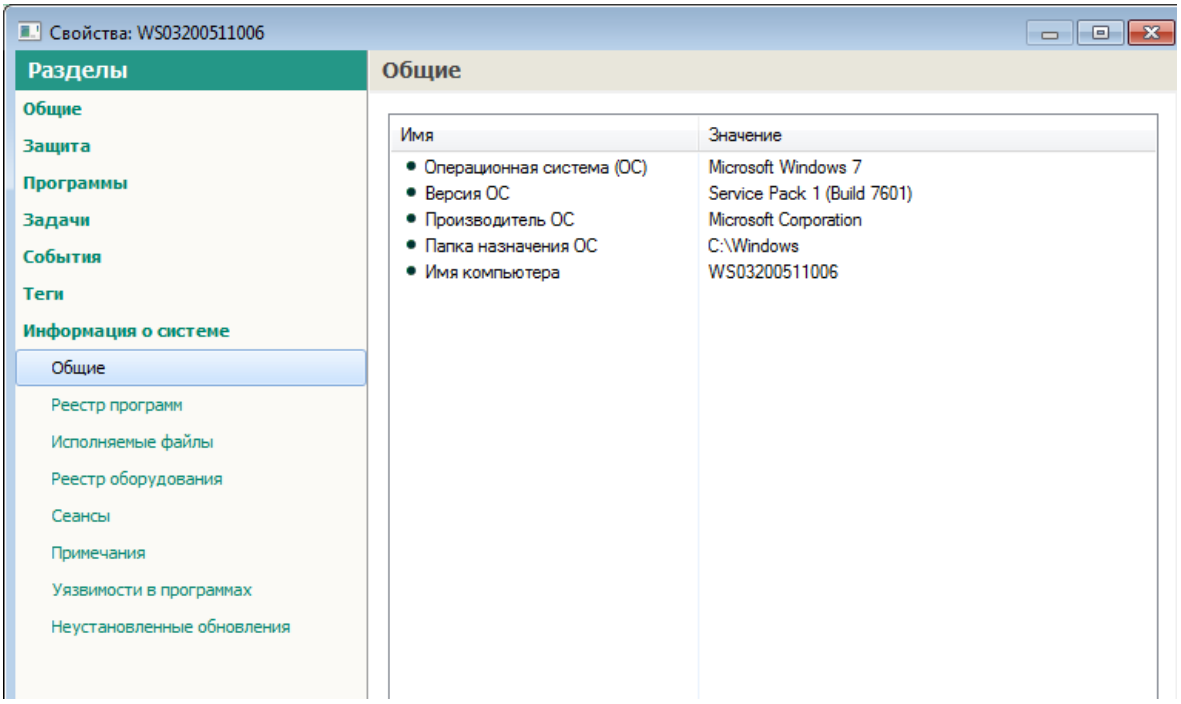


Рисунок 4 - Информация об удаленной рабочей станции

На рисунке 5 показан пример сформированного реестра установленных программ на удаленной рабочей станции. На рисунке 6 показан реестр оборудования удаленной рабочей станции, полученный средствами администрирования АВЗ. На рис.7 показаны режимы сетевых настроек удаленной рабочей станции. При необходимости запуска задачи на рабочей станции в удаленном режиме средства администрирования АВЗ также предоставляют такую возможность (рисунок 8).

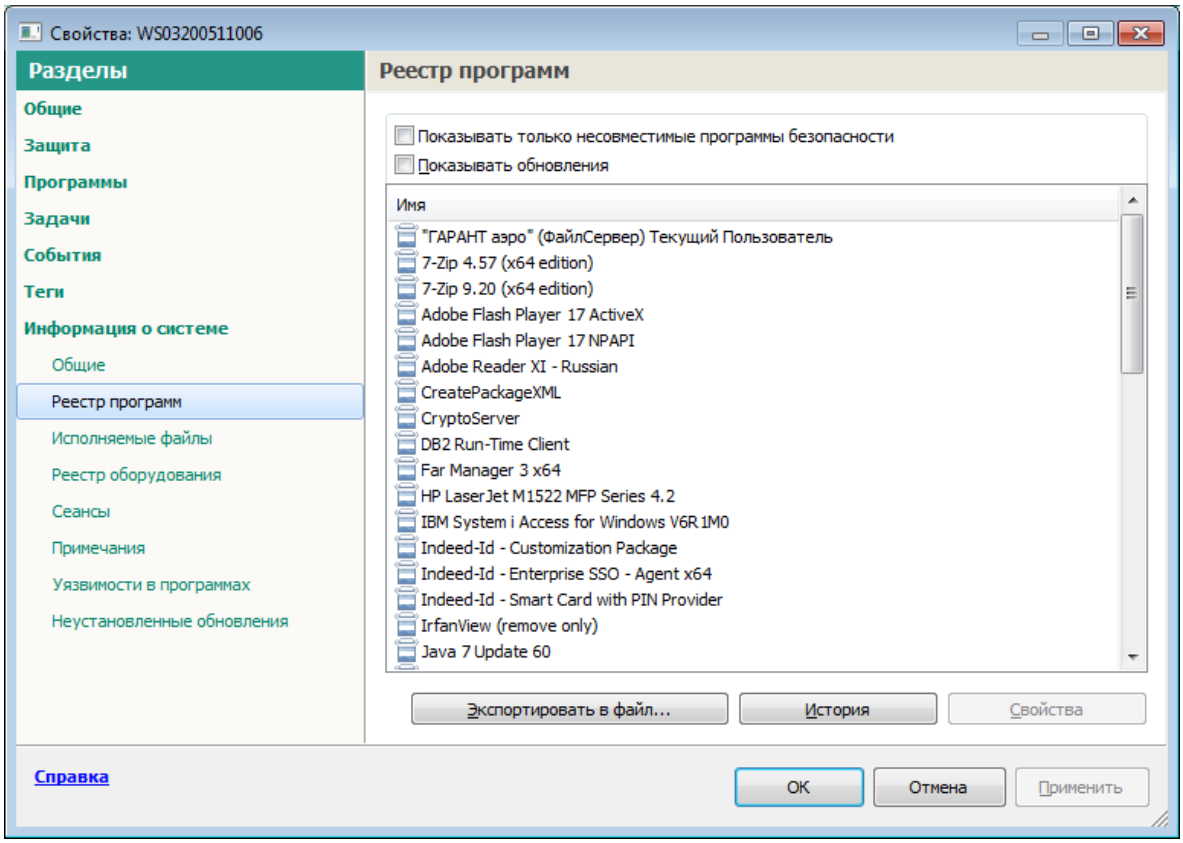


Рисунок 5 - Реестр установленных программ

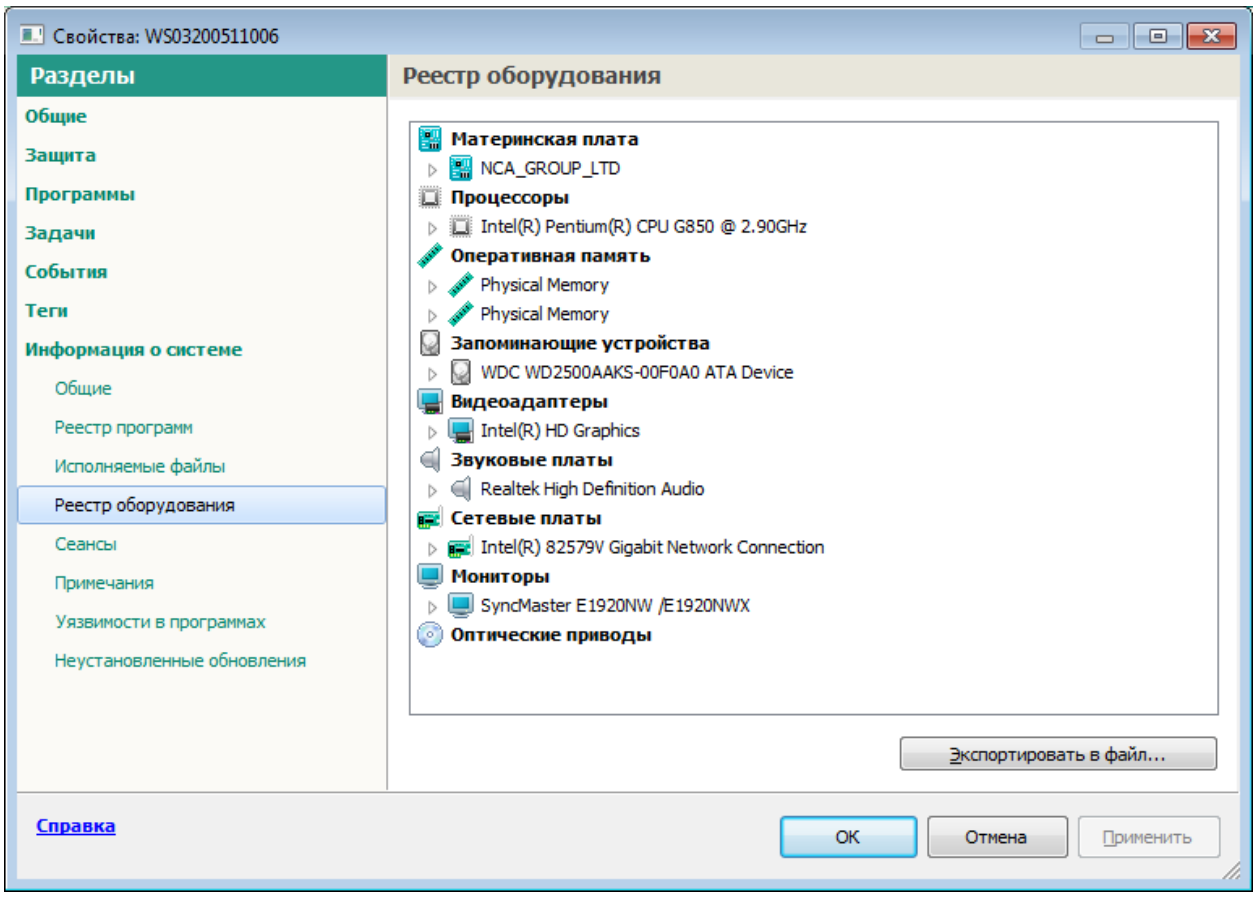


Рисунок 6 - Реестр оборудования

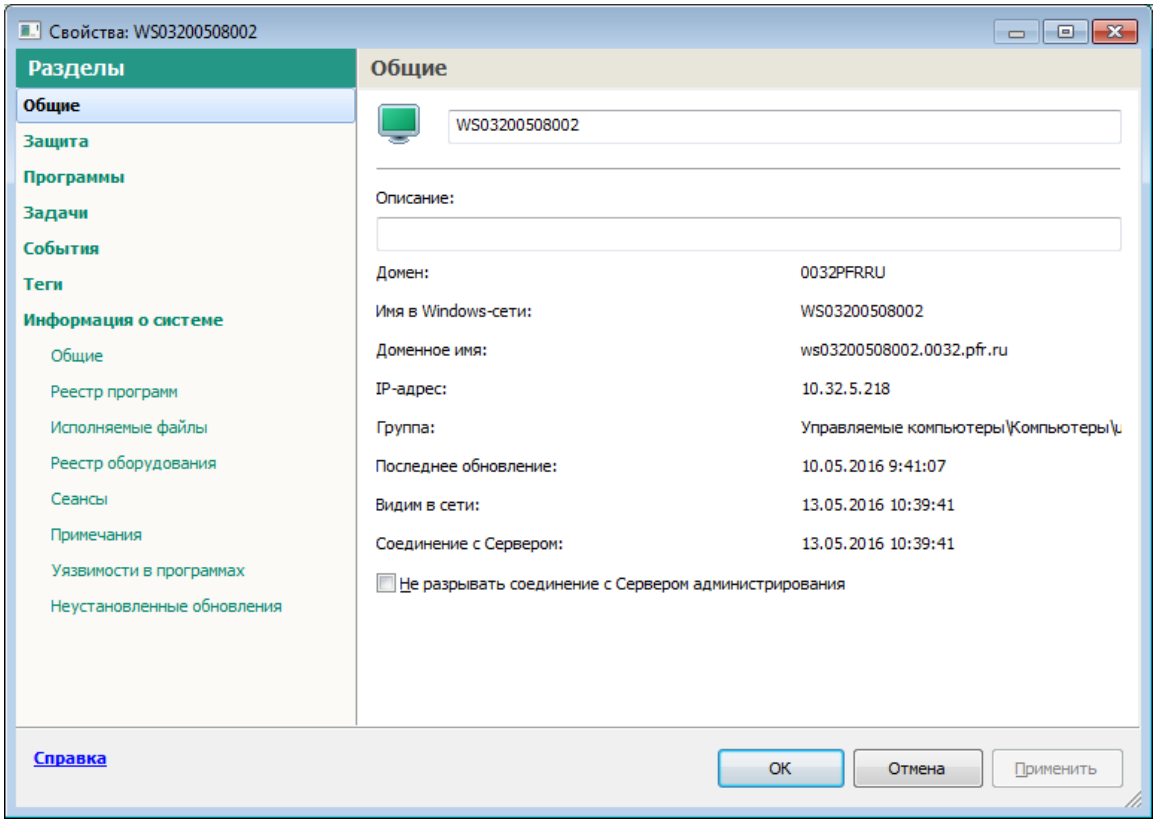


Рисунок 7 - Сетевые настройки удаленной рабочей станции

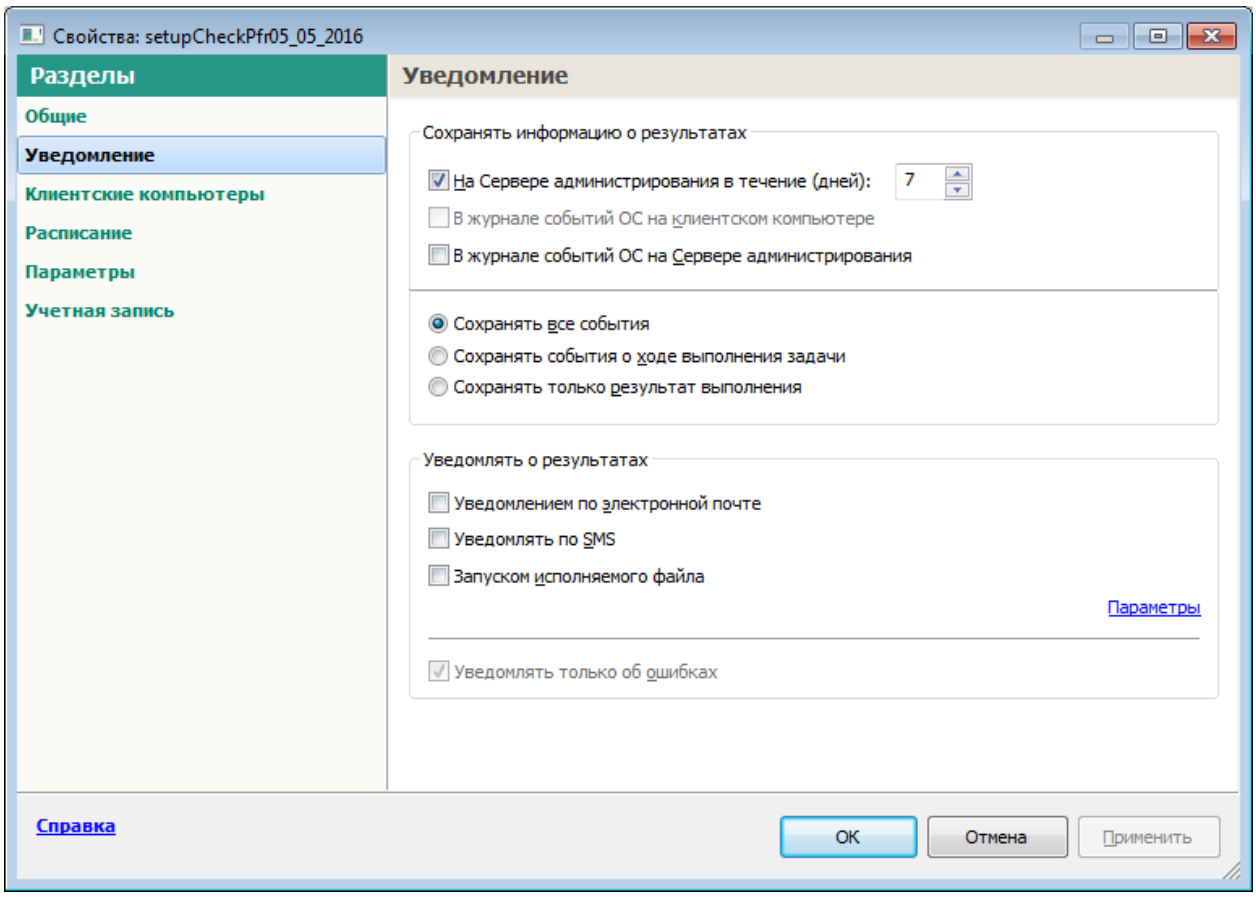


Рисунок 8 - Настройка запуска задачи с использованием средств администрирования АВЗ

Таким образом, рассмотрев возможности антивирусного корпоративного пакета в технологии мониторинга программно-аппаратной среды предприятия, можно сделать следующие выводы:

- корпоративные средства АВЗ предполагают возможности мониторинга состояния программного и аппаратного обеспечения, уровнях доступа к системе, пользователях рабочей станции, активности ПО;

- основным недостатком данного типа решений для решения задач мониторинга является невозможность формирования сводной отчетности о параметрах установленного ПО и устройств на рабочих станциях (так как данная задача не является для производителей антивирусного ПО профильной – разработчики не предусмотрели такой возможности);

- отсутствуют возможности фиксации факта изменения аппаратной среды (при переустановке оборудования в базе отмечается только наличие новых устройств, а факта переустановки не отмечается, что делает систему уязвимой перед угрозой хищения аппаратной части с рабочих станций);

- в случае использования подобного решения для мониторинга программно-аппаратной среды функционирование системы не будет полноценным, так как оно будет жестко связано с антивирусной системой. Мониторинг устройств, не входящих в архитектуру АВЗ, производиться не будет.

Таким образом, для небольших систем и для задач, связанных с мониторингом единичных компьютеров, данные решения являются оптимальными.

2.2. Использование специализированного ПО для учета компьютеров и программного обеспечения в доменной сети

В настоящее время создано большое количество программных продуктов, созданных для решения задач учета компьютеров и программного обеспечения в доменной сети удаленных рабочих станций. В качестве примера можно рассмотреть работу утилиты checkcfg.exe, которая может запускаться автоматически с использованием административных политик и формировать протоколы о состоянии программно-аппаратной среды, пример которого приведен в Приложении.

К основным возможностям данного ПО относится периодический сбор данных об аппаратном обеспечении и установленных программах в сети предприятия [1]:

- Тип и частота процессора, объём памяти, жестких дисков
- Сбор S.M.A.R.T.-данных жестких жисков
- Установленная операционная система, драйверы устройств, системное ПО

- Установленные подключения к сетям, в т.ч. сетевым дискам

Также реализована система слежения за критическими изменениями в конфигурациях:

- Изменение параметров аппаратных устройств.
- Критические снижения объема жестких дисков.
- Подключение / отключение внешних устройств
- Установка / удаление программ.
- Установка обновлений Windows.
- Изменение параметров загрузки Windows.
- Установление внешних модемных соединений.
- Предоставление доступа к локальным каталогам

Возможность ведения учета (с простановкой инвентарных номеров) оргтехники;

- Удобный древовидный интерфейс с персональным (пофамильным) учетом оргтехники.
- Возможность удаленного присваивания инвентарных номеров компьютерам.
- Генерация отчетов о состоянии ИТ-инфраструктуры в RTF-формате

Таким образом, данная система обладает рядом преимуществ перед функционалом средств АВЗ, так как предполагает возможность формирования протоколов сканирования компьютеров, протоколов изменения их конфигурации, а также получения сводной отчетности по параметрам программно-аппаратной среды.

Схема архитектуры данного приложения приведена на рисунке 9.

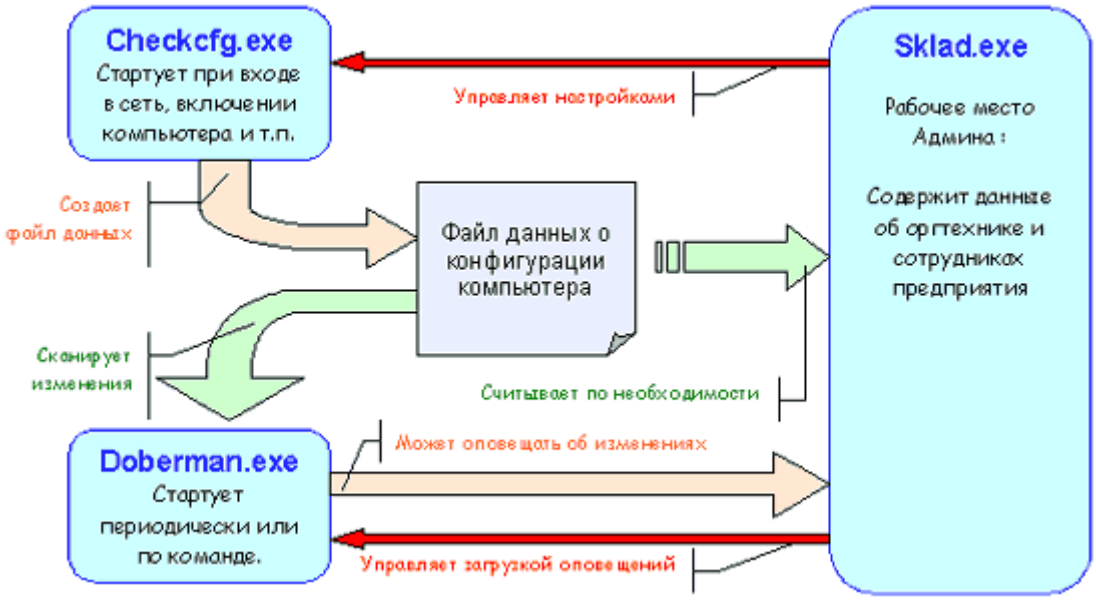


Рисунок 9 - Схема архитектуры системы checkcfg

Также достоинством данного ПО является возможность самостоятельной разработки программного обеспечения на основе анализа протоколов сканирования параметров компьютеров. Самостоятельно разработанное ПО на основе протоколов checkcfg позволит формировать необходимую отчетность в соответствии со спецификой работы организации.

Также данная система обладает существенным недостатком – процесс сканирования, запущенный административно, может быть принудительно остановлен пользователем на удаленной рабочей станции, что не даст возможности передачи протоколов сканирования программно-аппаратной среды на уровень администратора.

2.3. Использование средств защиты данных для учета компьютеров и программного обеспечения в доменной сети

В некоторых случаях задачи учета компьютеров и программного обеспечения в доменной сети сопряжены с более глубоким анализом работы системы, когда необходимо протоколировать не только факты установки программ и устройств, но и процесс работы пользователя за компьютером.

Такие задачи могут быть актуальны при работе с информацией, содержащей государственную или коммерческую тайну, персональные данные определенного уровня защищенности, работу с банковскими расчетными счетами при определенном уровне сумм проводимых операций, работе с криптографическими системами. В данном случае для защиты от потенциальных угроз утечки информации необходимо подробное протоколирование действий пользователей путем организации хранения снимков с экрана на данных рабочих станциях, а также протоколов работы с клавиатурой.

В таком случае к задачам мониторинга программно-аппаратной среды добавляются следующие:

- ведение архива снимков с экрана;
- ведение мониторинга запущенных процессов;
- ведение учета ввода данных с клавиатуры;
- ведение учета активности встроенных учетных записей, а также блокировка активности учетных записей, не допущенных к работе на данном рабочем месте.

Расширение функционала мониторинга в соответствии с указанными дополнительными требованиям возможно с использованием КСЗИ «Панцирь-К».

На рисунке 10 приведено окно запуска системы КСЗИ «Панцирь-К». Данное ПО позволяет производить контроль целостности системных файлов. В случае, когда определена активность запрещенного к запуску ПО, его активность может быть заблокирована с использованием административных политик. Для разбора событий, связанных с несанкционированной активностью ПО существует возможность протоколировать ввод данных с клавиатуры, а также снимков с экрана (Рисунок 11).

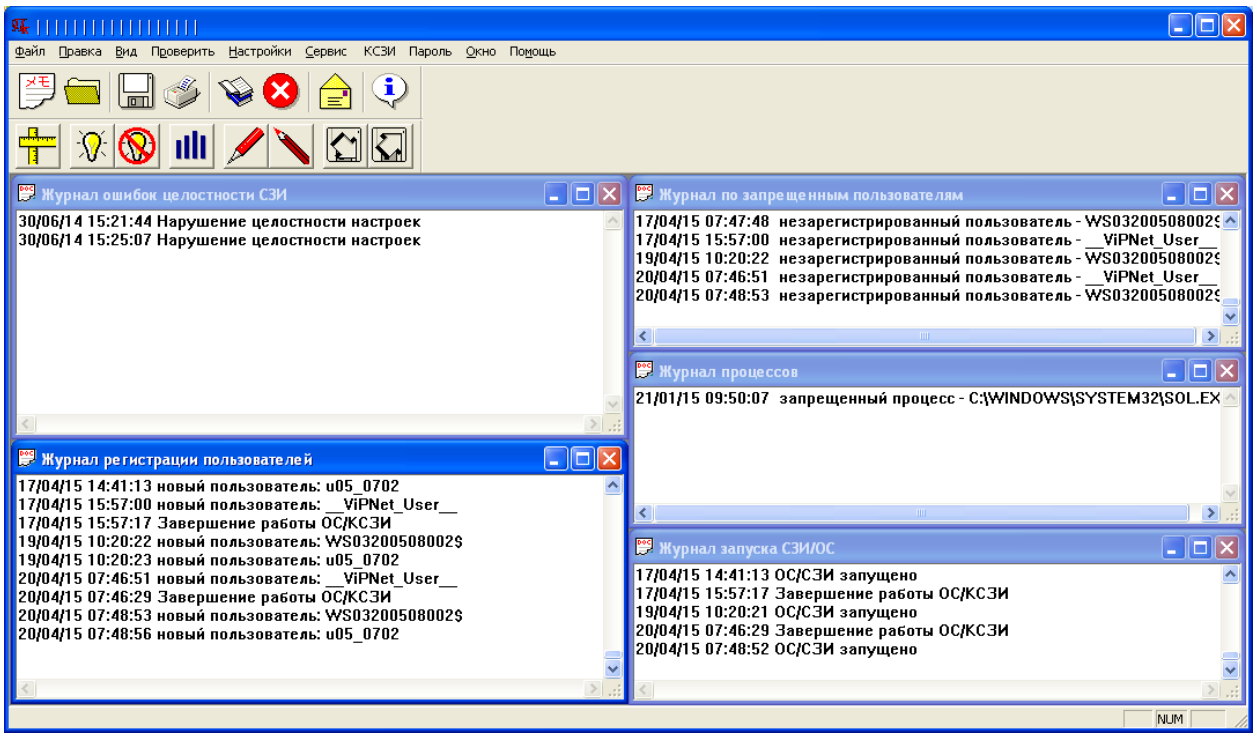
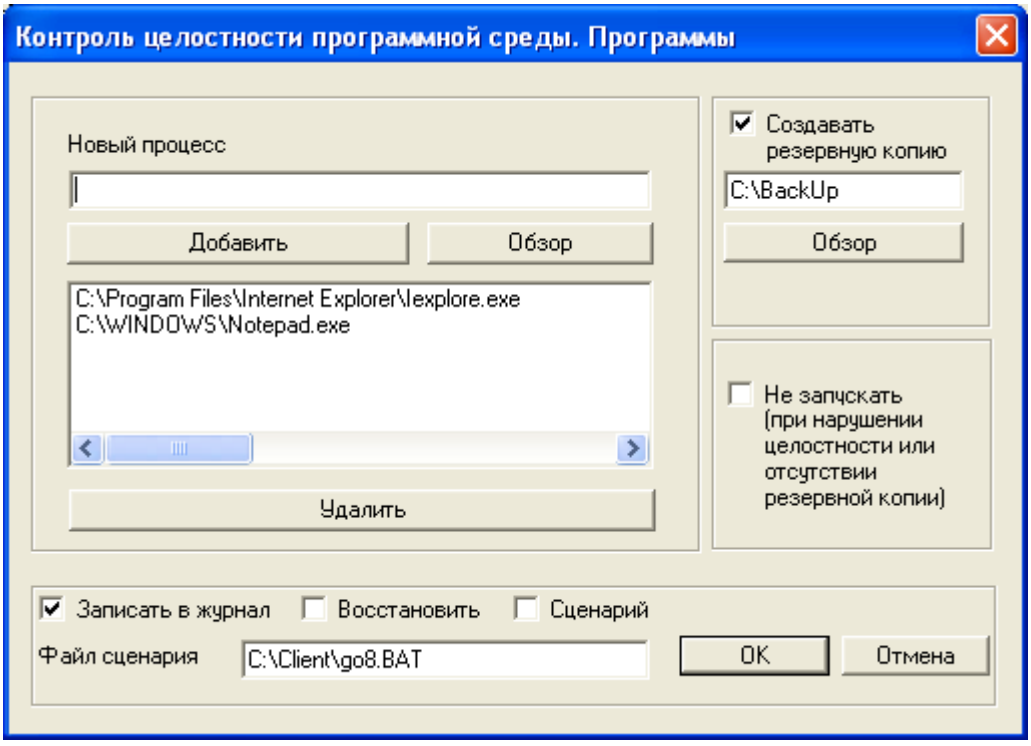


Рисунок 10 - Окно запуска КСЗИ «Панцирь-К»



1

Рисунок 11 - Настройки контроля целостности

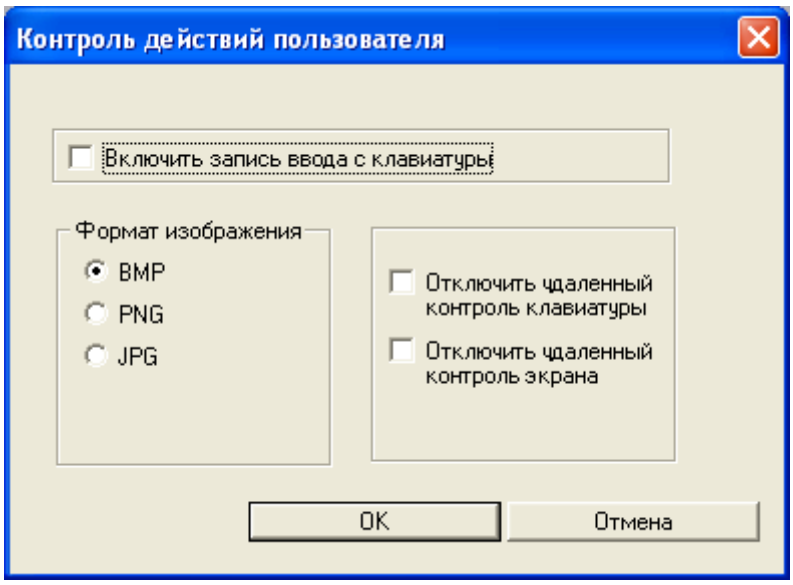


Рисунок 12 - Настройка аудита действий пользователя

Таким образом, в случае возникновения инцидентов, связанных с вирусным заражением по вине пользователя, а также запрещенных действий пользователей, существует возможность протоколирования.

Настройка контроля учетных записей пользователей приведена на рисунке 14. В данном режиме есть возможность контроля типов авторизации – с использованием вода пароля с консоли или использования смарт-карт, контролировать активность встроенных учетных записей, которые зачастую используются вредоносным ПО.

Таким образом, даже в случае вирусного заражения или несанкционированных запусков ПО со стороны пользователя, активность вредоносного ПО, использующего учетные записи локального администратора или гостя, блокируется.

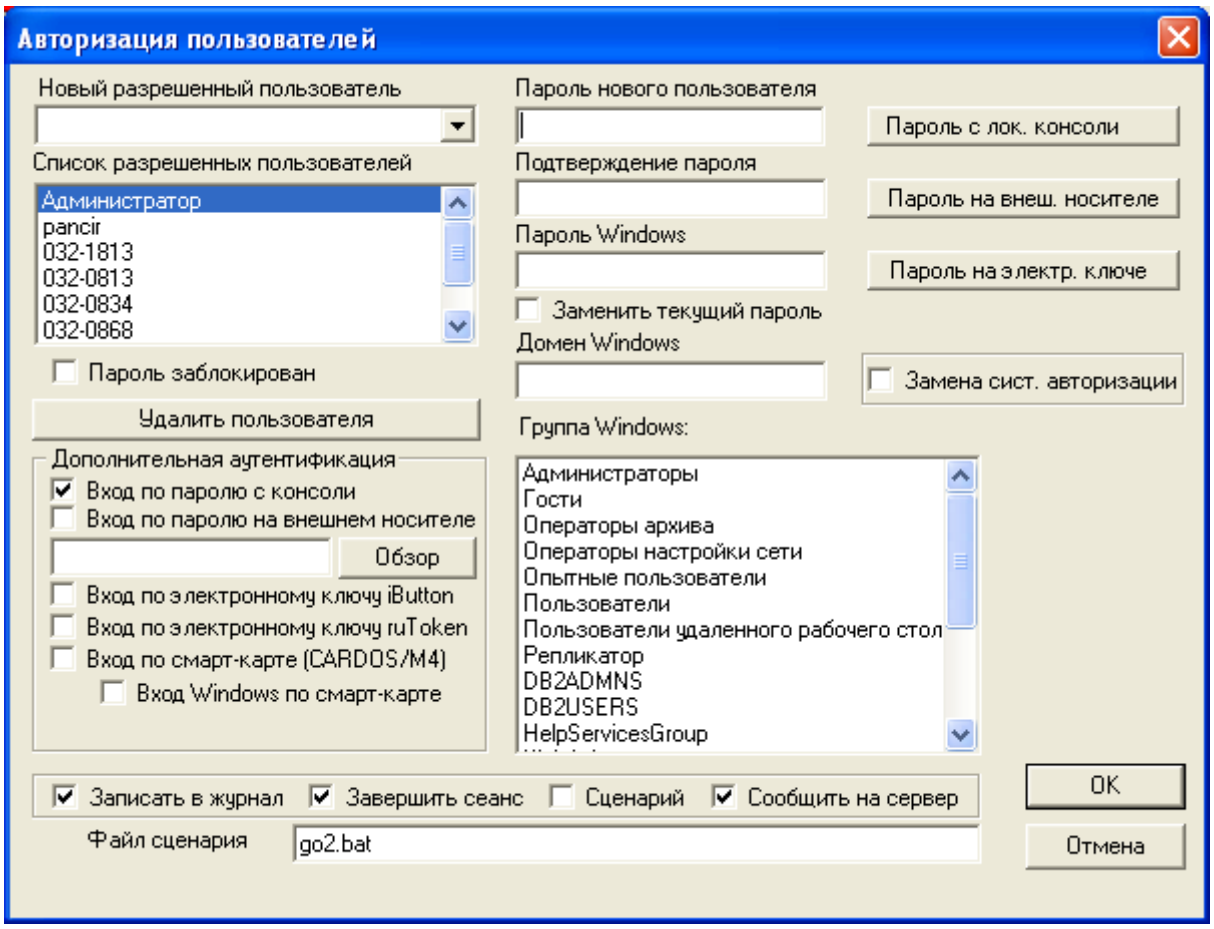


Рисунок 13 - Настройка контроля учетных записей пользователей

Также использование данного ПО позволяет в удаленном режиме управлять доступом:

- к сетевым ресурсам;
- к буферу обмена;
- к подключенным устройствам;
- к файловой системе;
- другим ресурсам.

Данные сервисы позволяют блокировать активность вредоносного ПО, функционал которого связан с указанными ресурсами.

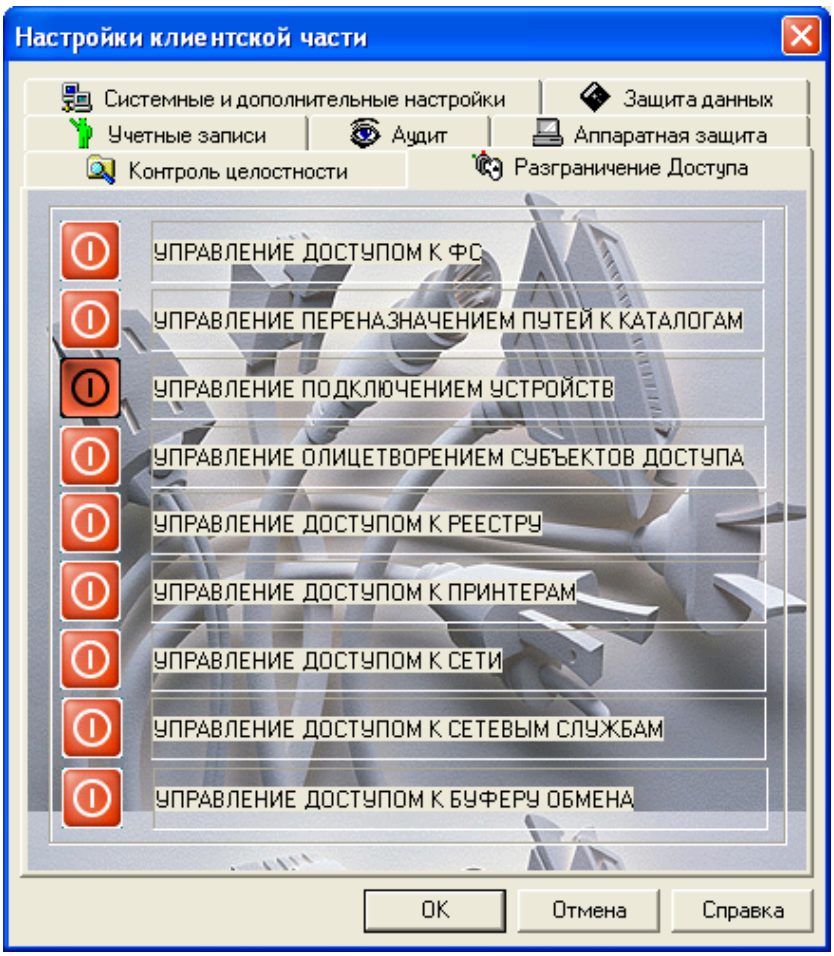


Рисунок 14 - Настройка управления доступом

Также использование данного КСЗИ позволяет контролировать использование файла подкачки, который также может использоваться вредоносным ПО (рисунок 15).

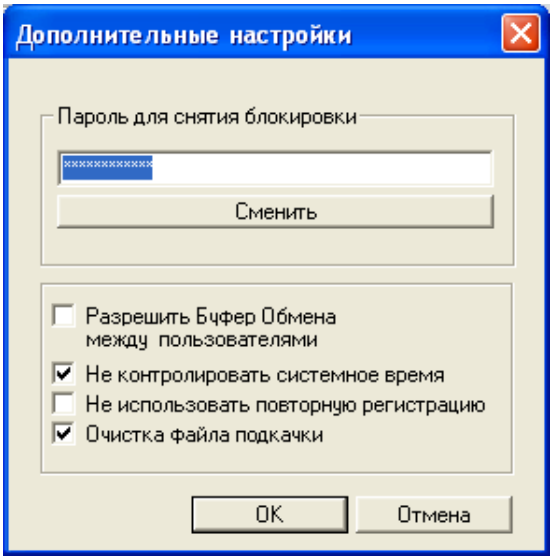


Рисунок 15 - Дополнительные настройки

Таким образом, наиболее полным функционалом мониторинга удаленной программно-аппаратной среды обладает КСЗИ «Панцирь-К», но его использование не всегда оправдано вследствие высокой требовательности к серверным ресурсам и каналам передачи данных для хранения протоколов работы удаленных рабочих станций.

2.4. Обзор существующих программных решений для мониторинга программно-аппаратной среды

Таким образом, рассмотрев функционал программных систем для удаленного мониторинга программно-аппаратной среды выберем оптимальные решения для подразделений исследуемого предприятия. Результаты приведем в таблице 7.

Таблица 7 - Выбор решений для удаленного мониторинга программно-аппаратной среды

Подразделение	Основное решение	Дополнительное решение
Руководство	Checkcfg	Kaspersky Security Center
Отдел инвестирования	Checkcfg	Kaspersky Security Center
HR-отдел	КСЗИ «Панцирь-К»	Checkcfg, Kaspersky Security Center
ИТ-отдел	КСЗИ «Панцирь-К»	Checkcfg, Kaspersky Security Center
Экономический отдел	КСЗИ «Панцирь-К»	Checkcfg, Kaspersky Security Center
Ревизионный отдел	Checkcfg	Kaspersky Security Center
Отдел налогового консультирования	Checkcfg	Kaspersky Security Center
Отдел маркетинга	Checkcfg	Kaspersky Security Center
Юридический отдел	Checkcfg	Kaspersky Security Center

Как показано в таблице 8, в ряде подразделений целесообразно использовать усиленные системы мониторинга программно-аппаратной среды, так как в экономическом отделе производится отработка данных, содержащих коммерческую тайну и производится работа с банковскими

системами, HR-отдел работает с персональными данными сотрудников, ИТ-отдел имеет доступ к администрированию системой.

Для остальных подразделений достаточно использования решений checkcfg как основной программы для мониторинга состояния программно-аппаратной среды, а решения на базе антивирусной системы – как дополнительной.

Задачи мониторинга программного и аппаратного обеспечения в условиях информационной системы предприятий предполагают необходимость функционала, не реализованного в рассмотренных программных средствах, что предполагает необходимость решения задач:

- контроль устанавливаемого программного обеспечения;

- контроль отработки политик, связанных с установкой программных решений;

- контроль производительности компьютеров;

- инвентаризация программных продуктов с целью контроля лицензий.

Проведем анализ бизнес-процессов мониторинга программного и аппаратного обеспечения в условиях рассматриваемого предприятия.

Контекстная диаграмма приведена на рисунке 16. Как показано на рисунке 16, входящими информационными потоками являются:

- Стандарты автоматизированной информационной системы предприятия;

- Данные протоколов анализа автоматизированной информационной системы.

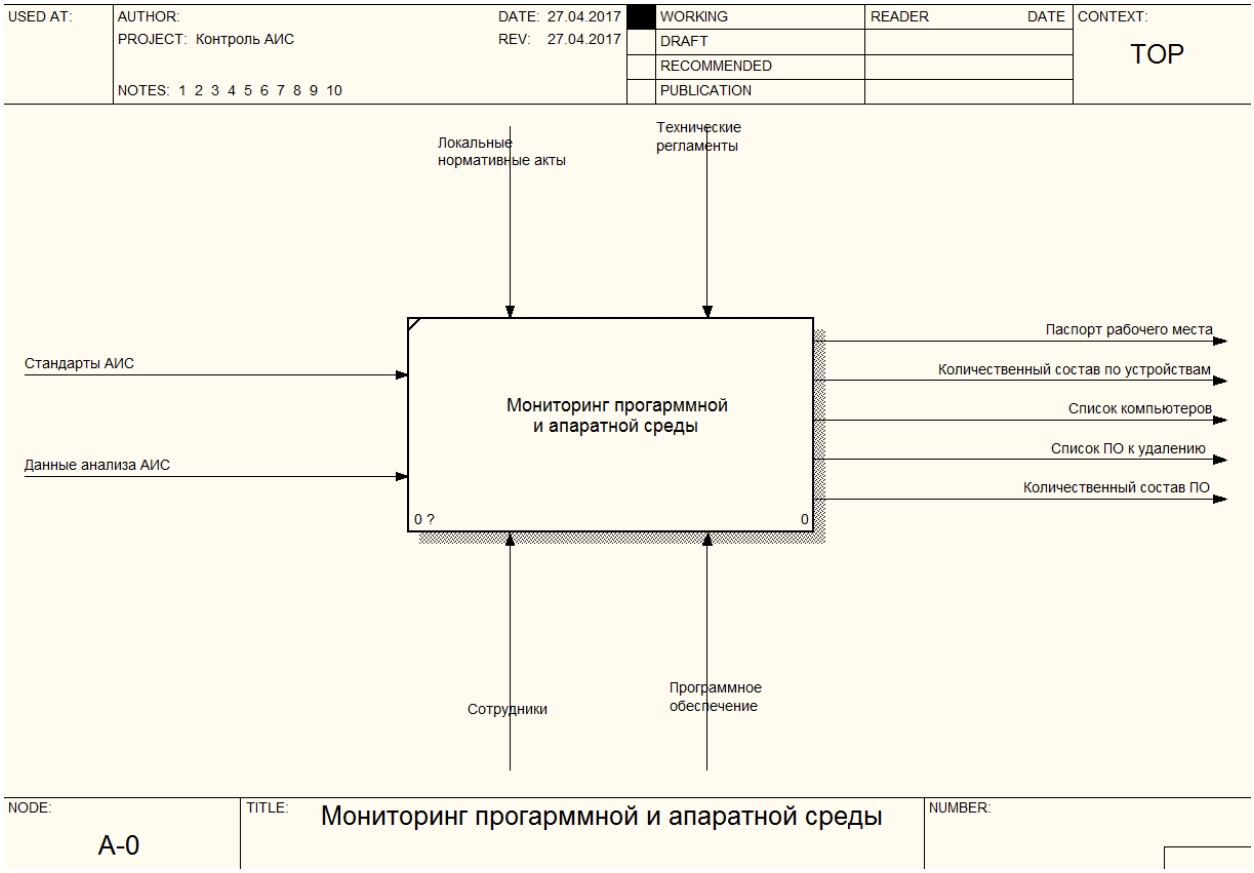


Рисунок 16 - Контекстная диаграмма

Результатная информация включает в себя сформированные отчеты:

- Паспорт рабочего места;
- Количественный состав по устройствам;
- Список ПО к удалению;
- Количественный состав ПО;
- Список обнаруженных компьютеров в локальной сети.

На рисунке 17 приведена диаграмма основного бизнес-процесса

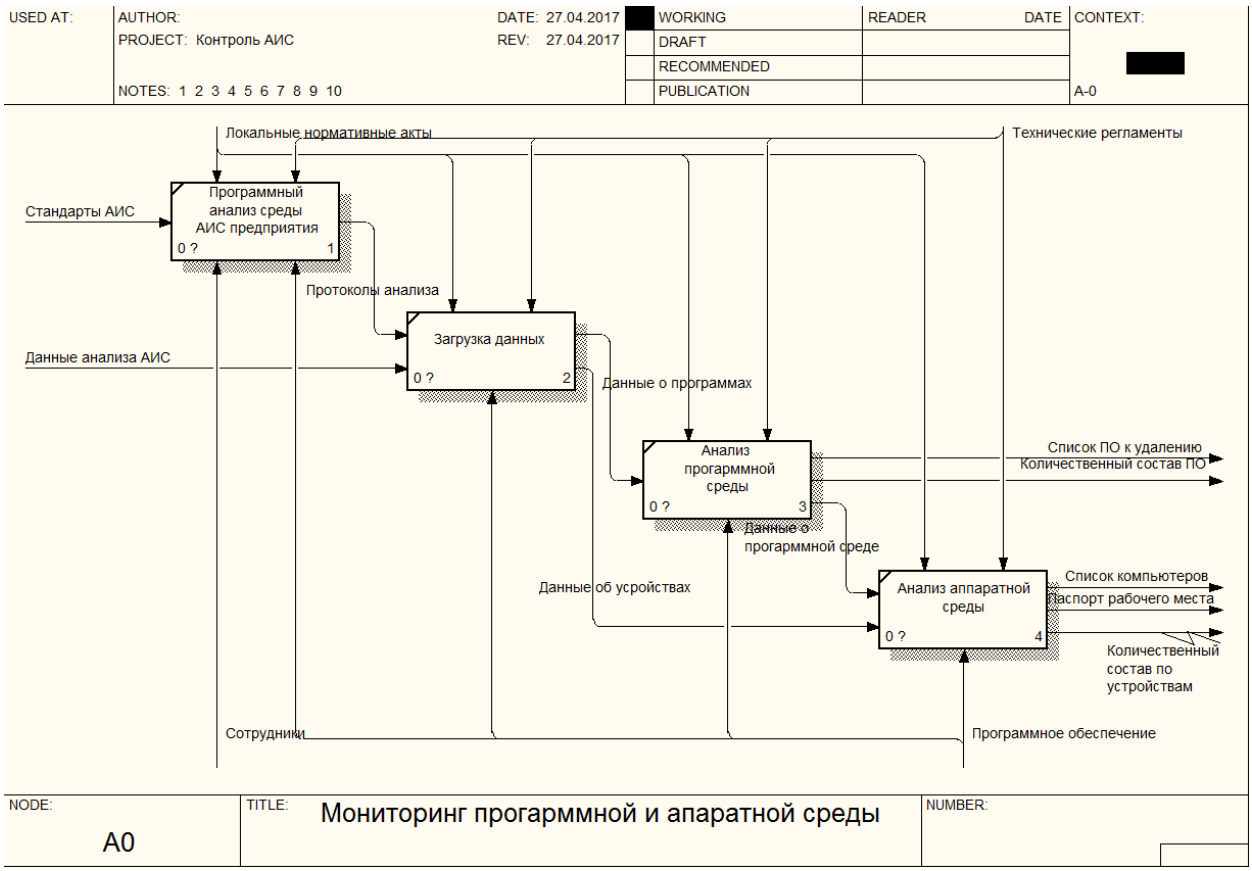


Рисунок 17 - Диаграмма декомпозиции мониторинга программной и аппаратной среды

Таким образом, программный продукт по автоматизации мониторинга программной а аппаратной среды должен выполнять задачи:

- мониторинг состояния программной и аппаратной среды;

- получение оперативной информации по аппаратному и программному обеспечению;

- формирование отчетной информации.

3. Проектирование ПО мониторинга программно-аппаратной среды

3.1 Информационная модель

Диаграмма потоков данных разрабатываемой системы приведена на рисунке 18.

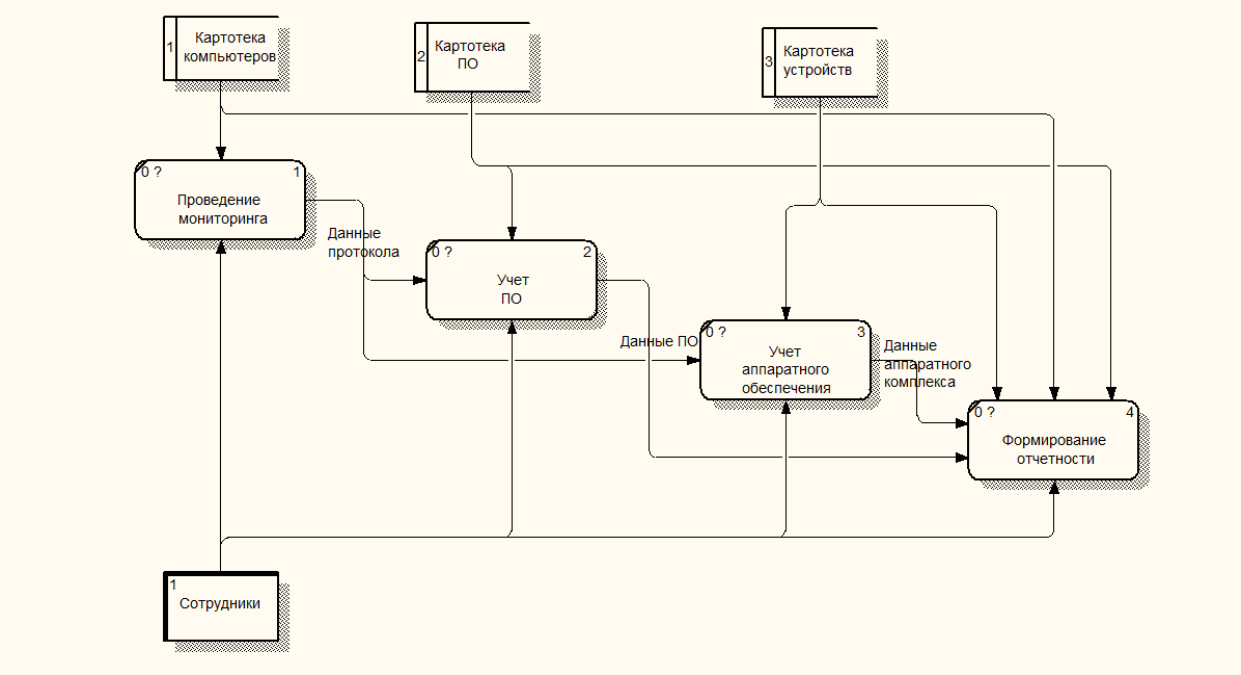


Рисунок 18 - Диаграмма потоков данных

На рисунке 20 приведена диаграмма «Сущность - Связь» разрабатываемой системы.

Рисунок 19 - Диаграмма «Сущность - Связь»

На рисунке 20 приведена диаграмма классов.

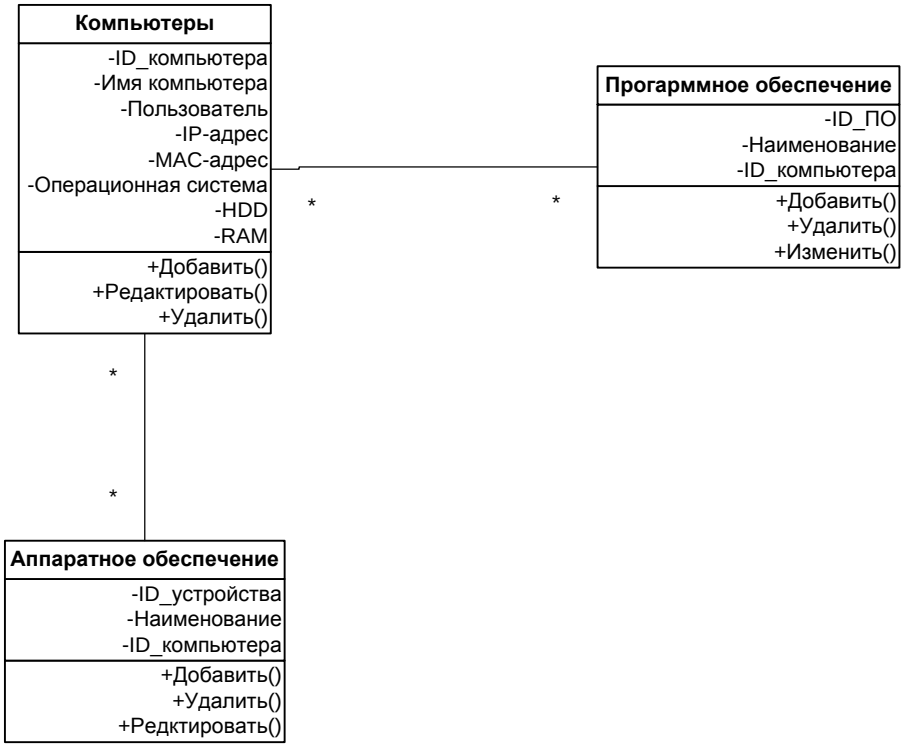


Рисунок 20 – Диаграмма классов

Далее определим атрибуты сущностей разрабатываемой системы.

В таблице 8 приведены атрибуты сущности «Компьютер».

Таблица 8 - Атрибуты сущности «Компьютер»

Наименование атрибута	Тип данных	Примечание
Код компьютера	Числовой	Первичный ключ
IP-адрес	Текстовый	
Имя компьютера	Текстовый	
Операционная система	Текстовый	
Наименование процессора	Текстовый	
Емкость жесткого диска	Числовой	
Оперативная память	Числовой	
ФИО пользователя	Текстовый	
Логин пользователя	Текстовый	
MAC-адрес	Текстовый	

В таблице 9 приведены атрибуты сущности «Программное обеспечение».

Таблица 9 - Атрибуты сущности «Программное обеспечение»

Наименование атрибута	Тип данных	Примечание
Код ПО	Числовой	Первичный ключ
Код компьютера	Числовой	Вторичный ключ
Наименование ПО	Текстовый	
Признак удаления	Логический	

В таблице 10 приведены атрибуты сущности «Аппаратное обеспечение».

Таблица 10 - Атрибуты сущности «Аппаратное обеспечение»

Наименование атрибута	Тип данных	Примечание
Код устройства	Числовой	Первичный ключ
Код компьютера	Числовой	Вторичный ключ
Наименование устройства	Текстовый	

На рисунке 21 приведена схема логической модели.

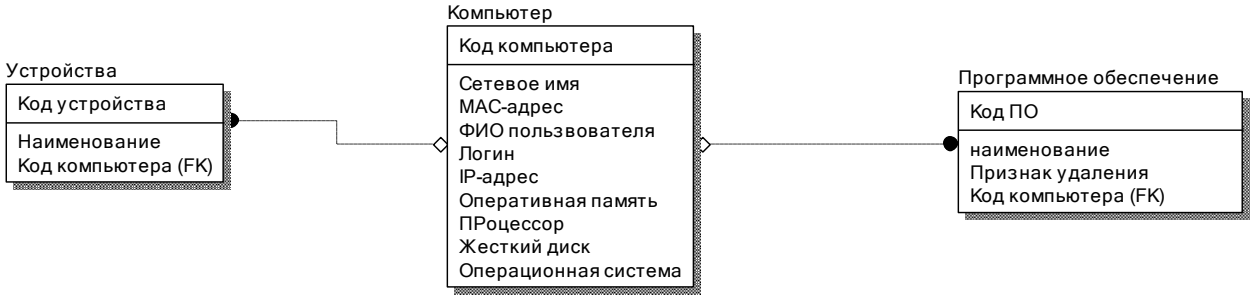


Рисунок 21 - Логическая модель данных

В соответствии с построенной логической моделью проведем построение физической модели.

В таблице 11 приведены атрибуты сущности «Программное обеспечение».

Таблица 11 - Структура таблицы «cm_sft»

Поле	Тип данных	Примечание
Code_sf	Int	Первичный ключ
Code_cm	Int	Вторичный ключ
Nam_po	Char	
Udal	Bool	

В таблице 12 приведено описание структуры таблицы, содержащей данные справочника компьютеров.

Таблица 12 - Структура таблицы «cmp»

Поле	Тип данных	Примечание
Code	int	Первичный ключ
Ipadr	Char	
Hostname	Char	
Syst	Char	
Cpu	Char	
Hdd	Int	
Ram	Int	
Fio	Char	
Login	Char	
MAC	Char	

В таблице 13 приведены атрибуты сущности «Аппаратное обеспечение».

Таблица 13 - Структура таблицы «dvs»

Поле	Тип данных	Примечание
Code_dvs	Int	Первичный ключ
Code_cm	Int	Вторичный ключ
Nam_dvs	Char	

Схема данных приведена на рисунке 22.

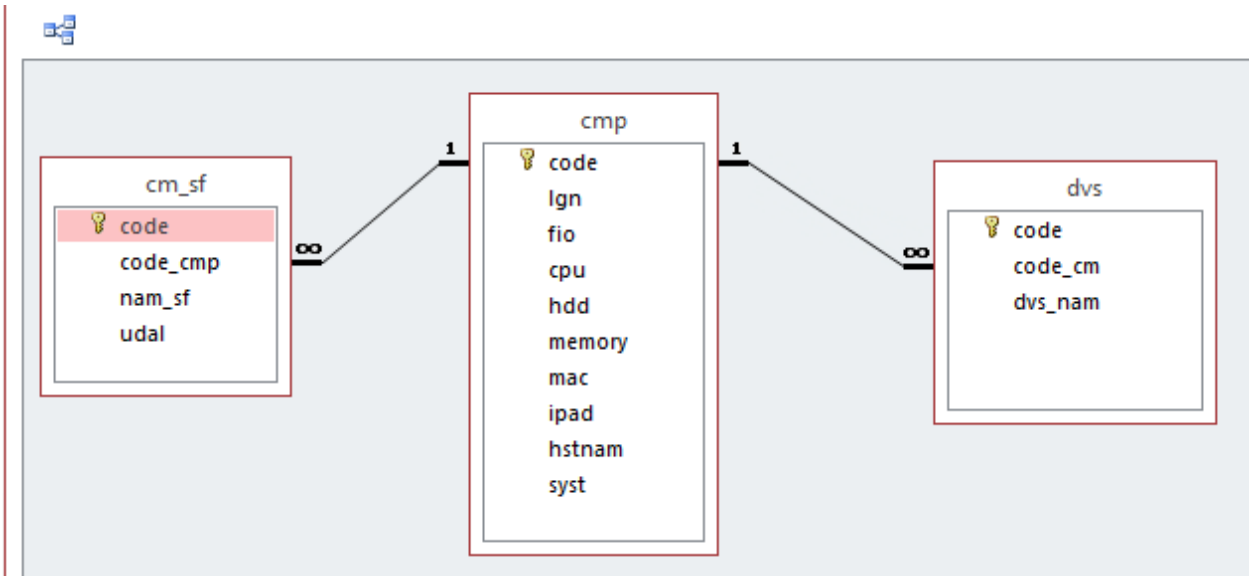


Рисунок 22 - Схема данных

На рисунке 23 показана схема архитектуры разрабатываемой системы мониторинга программно-аппаратной среды.

Как показано на рисунке 23, в функционировании разрабатываемого ПО присутствует вспомогательное решение, формирующее протоколы о состоянии программно-аппаратной среды и запускаемое в режиме автозагрузки с использованием административных политик.

Далее производится анализ сформированных протоколов, загрузка их в базу данных с последующим формированием сводной отчетности и выборок по запросу пользователя.

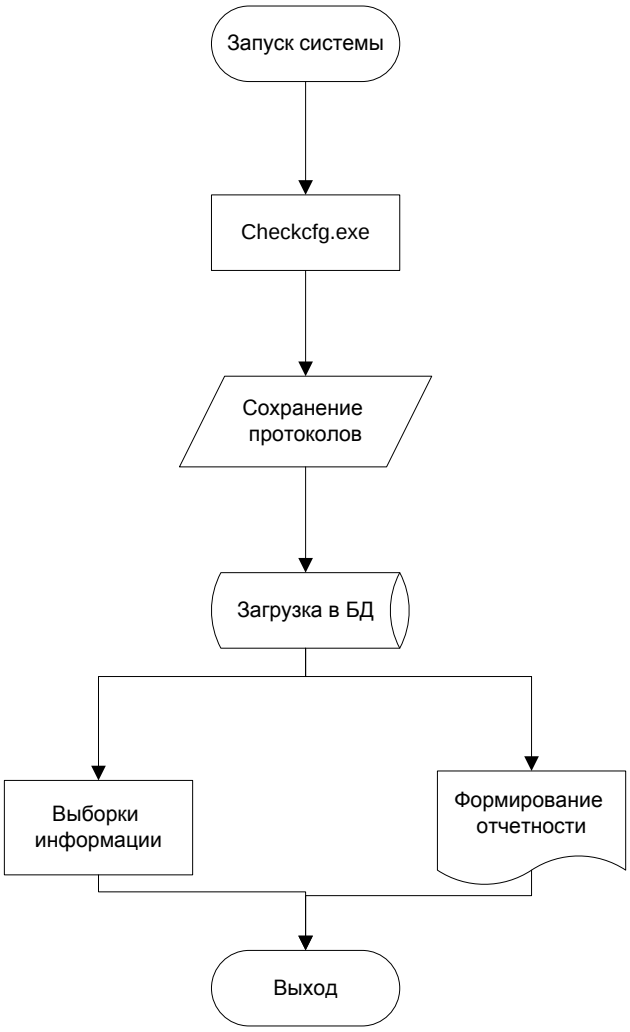


Рисунок 23 - Блок-схема работы ПО

3.2 Описание разработанного ПО

Схема работы программы:

- С помощью доменных политик в автозагрузку загружается модель анализа программной и аппаратной среды checkcfg.exe;

- Протоколы работы программы, образец которых приведен в Приложении 1, копируются в каталог C:\diag\in;

- Данные протоколов загружаются в систему;

- Разработанное ПО проводит формирование протоколов анализа состояния программной и аппаратной среды.

Разработка программы проведена на языке Delphi.

Главная форма приложения приведена на рисунке 24. На рисунке 25 приведен режим загрузки данных.

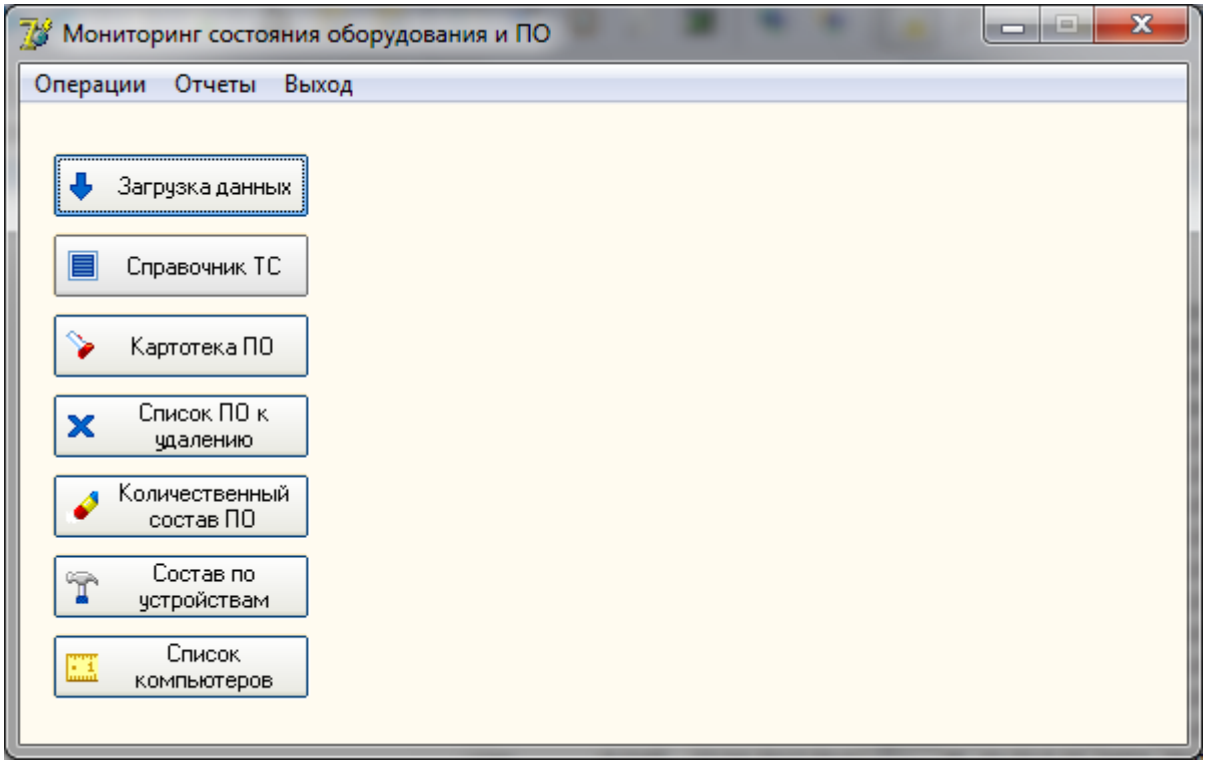


Рисунок 24 - Главная форма приложения

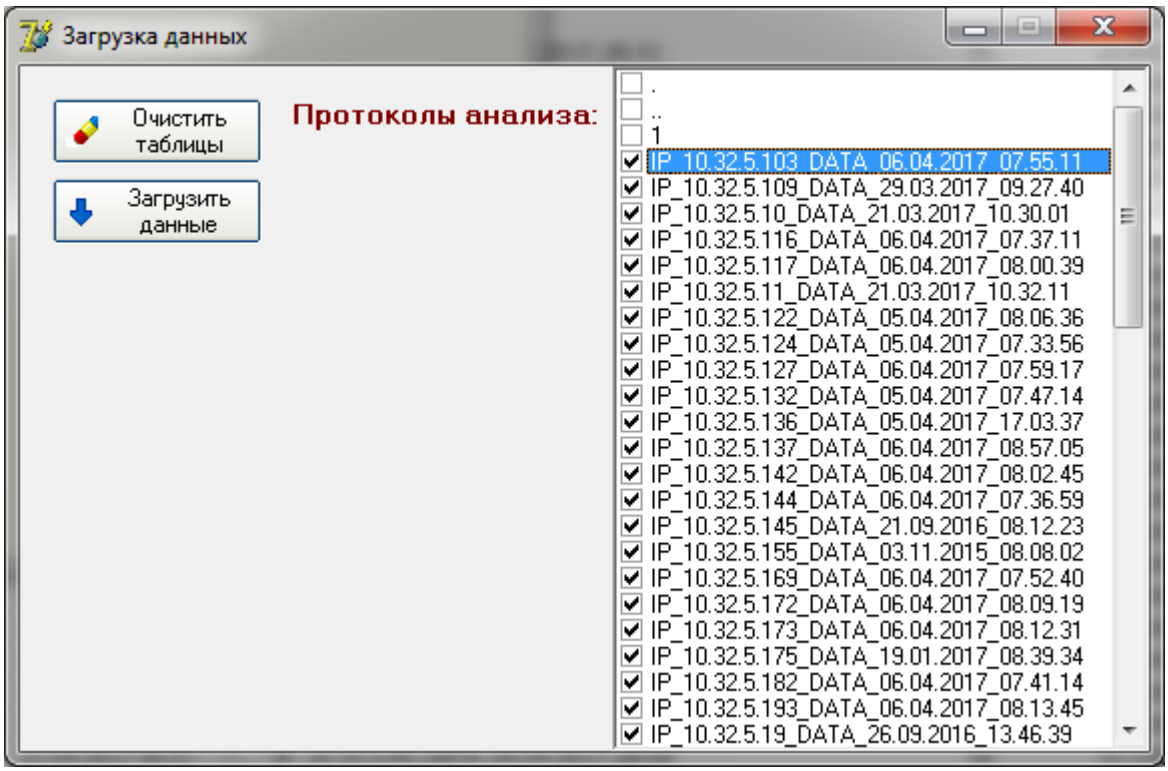


Рисунок 25 - Режим загрузки данных

На рисунке 26 приведен режим справочника компьютеров, из которого производится формирование выборочной информации:

- по наименованию;
- по пользователю;
- выборка установленного ПО;
- выборка установленного оборудования.

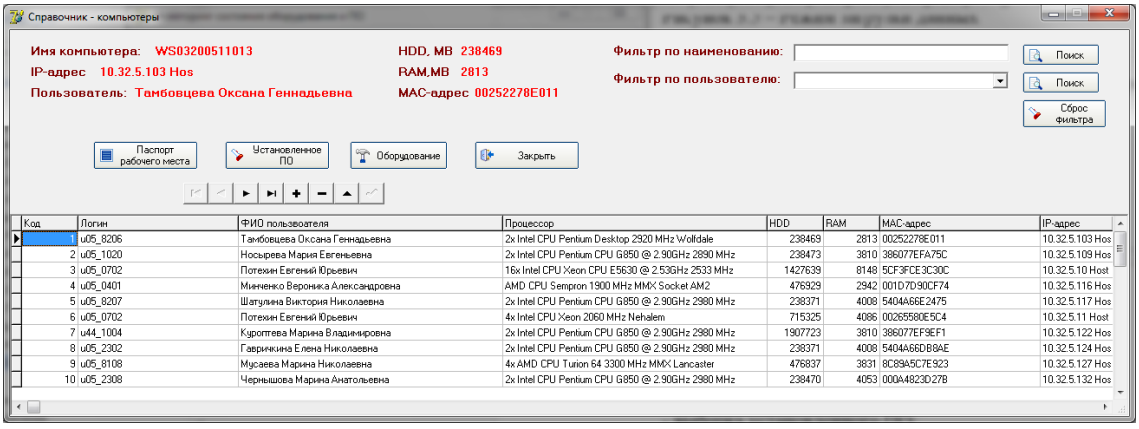


Рисунок 26 - Справочник «Компьютеры»

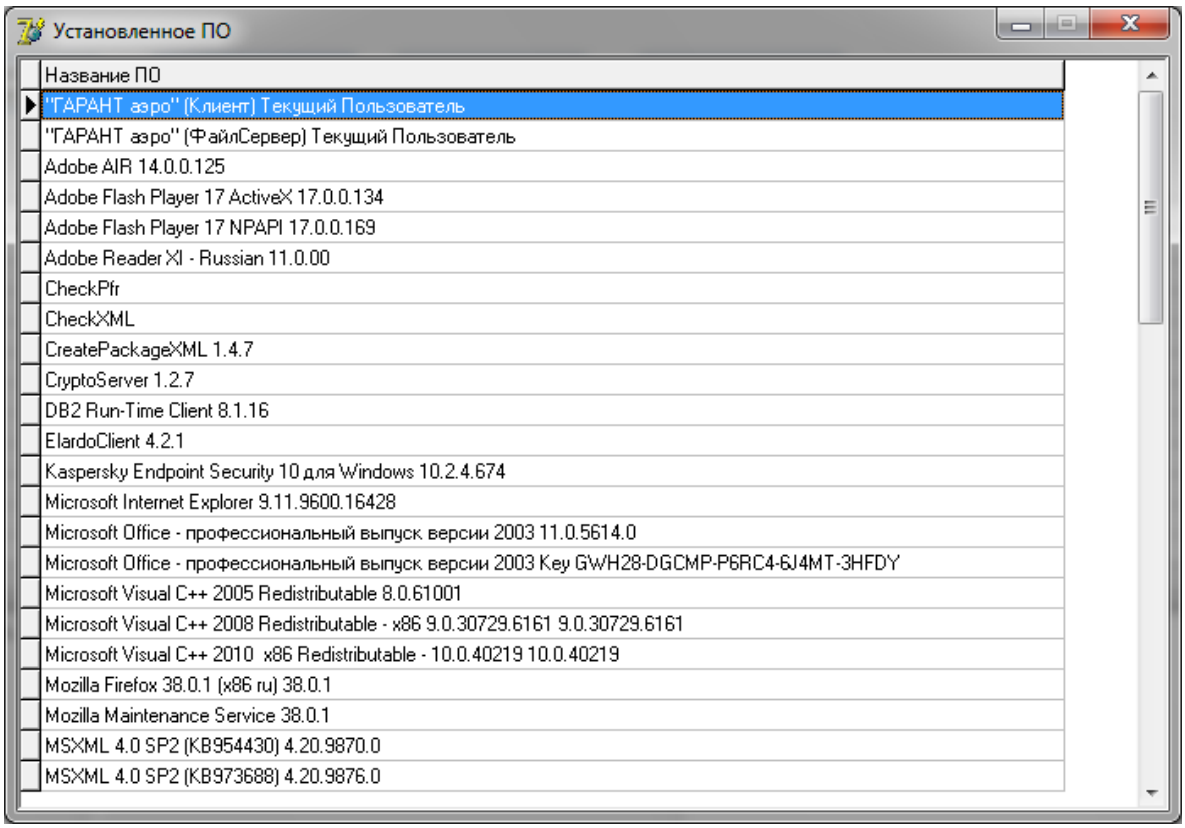


Рисунок 27 - Список установленного ПО

На рисунке 28 показан режим «Паспорт рабочего места пользователя»

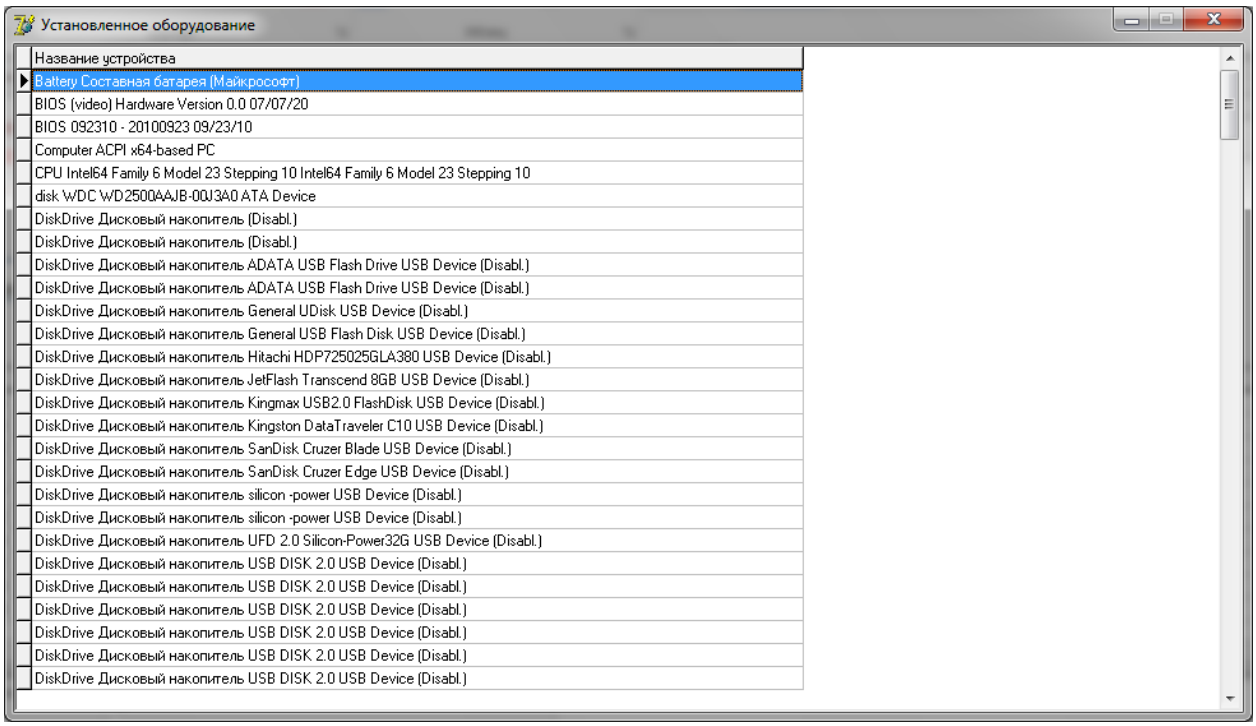


Рисунок 28 - Список оборудования

Паспорт рабочего места

Дата составления: 27.04.2017
ФИО пользователя: Тамбовцева Оксана Геннадьевна

Параметры компьютера:
Имя компьютера: WS03200511013
IP-адрес: 10.32.5.103 Hos
MAC-адрес: 2.52E+16
Оперативная память: 2813
Процессор: 2x Intel CPU Pentium Desktop 2920 MHz Wolfdale
Жесткий диск, MB: 238469
Операционная система: Windows 7 build 7601/Service Pack 1,Русский (Росси

Установленное ПО:
"ГАРАНТ аэро" (Клиент) Текущий Пользователь
"ГАРАНТ аэро" (ФайлСервер) Текущий Пользователь
Adobe AIR 14.0.0.125
Adobe Flash Player 17 ActiveX 17.0.0.134
Adobe Flash Player 17 NPAPI 17.0.0.169
Adobe Reader XI - Russian 11.0.00
CheckXML
CreatePackageXML 1.4.7
DB2 Run-Time Client 8.1.16
ElardoClient 4.2.1
Kaspersky Endpoint Security 10 для Windows 10.2.4.674
Microsoft Internet Explorer 9.11.9600.16428
Microsoft Office - профессиональный выпуск версии 2003 11.0.5614.0
Microsoft Office - профессиональный выпуск версии 2003 Key GWH28-DGCMP-P6RC4-6J4MT-3HFDY
Microsoft Visual C++ 2005 Redistributable 8.0.61001
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 10.0.40219
Mozilla Firefox 38.0.1 (x86 ru) 38.0.1
Mozilla Maintenance Service 38.0.1
MSXML 4.0 SP2 (KB954430) 4.20.9870.0
MSXML 4.0 SP2 (KB973688) 4.20.9876.0
MSXML 4.0 SP2 Parser and SDK 4.20.9818.0

Рисунок 29 - Паспорт рабочего места пользователя

На рисунке 30 приведен режим картотеки программного обеспечения.

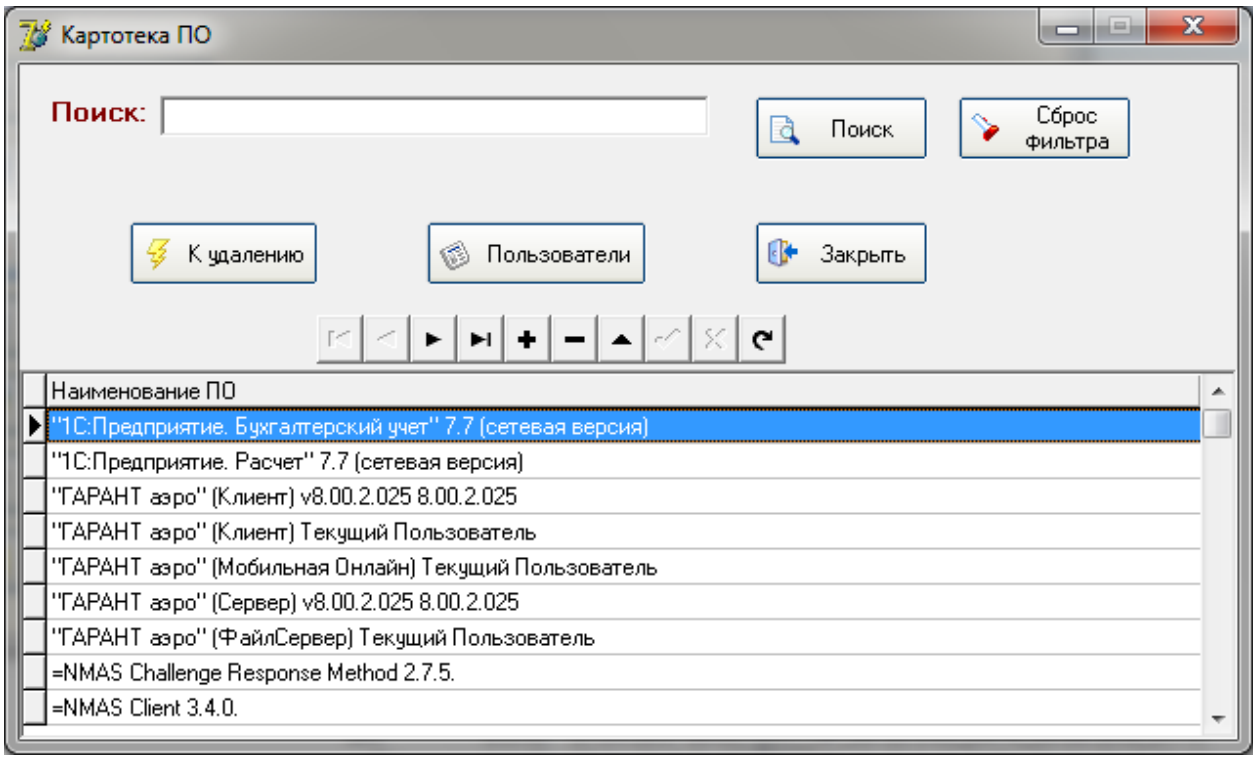


Рисунок 30 - Режим картотеки программного обеспечения

Из режима картотеки ПО можно определить перечень программного обеспечения, не разрешенного к использованию в организации и далее сформировать отчет о программах, подлежащих удалению. На рисунке 31 показан режим списка пользователей установленного ПО. На рисунке 32 показан отчет о программах, подлежащих удалению.

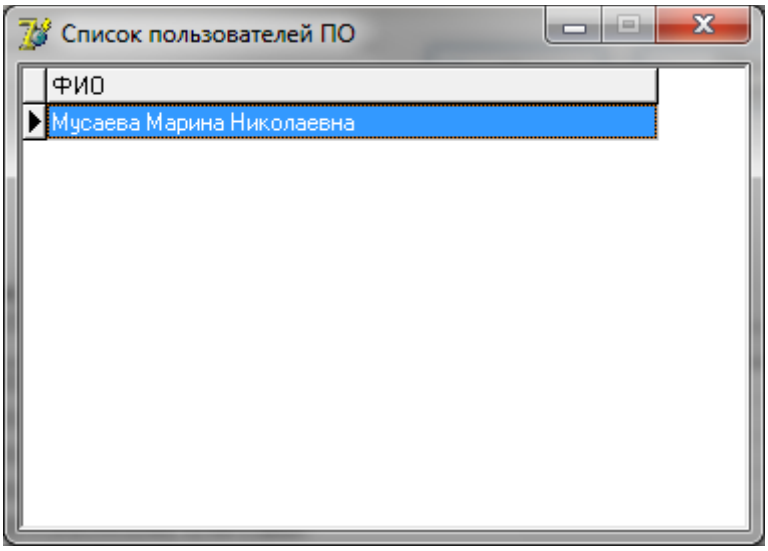


Рисунок 31 - Режим списка пользователей установленного ПО

Список ПО к удалению

Наименование ПО	Имя компьютера	ФИО пользователя
Диагностика принтеров Samsung 1.0.0.17	WS03200509002	Халяпина Татьяна Николаевна
Acronis True Image 10.0.4954	WS03200513001	Аверина Светлана Ивановна
Диагностика принтеров Samsung 1.0.0.17	WS03200521011	Кожухова Анастасия Петровна
NMAS Challenge Response Method 2.7.5.	WS032000508010	Потехин Евгений Юрьевич

Рисунок 32 - Отчет о списке ПО к удалению

Отчет о количественном составе ПО показан на рисунке 33.

Количественный состав ПО

Наименование ПО	Количество экз.
"1С:Предприятие. Бухгалтерский учет" 7.7 (сетевая версия)	1
"1С:Предприятие. Расчет" 7.7 (сетевая версия)	1
"ГАРАНТ аэро" (Клиент) v8.00.2.025 8.00.2.025	1
"ГАРАНТ аэро" (Клиент) Текущий Пользователь	16
"ГАРАНТ аэро" (Мобильная Онлайн) Текущий Пользователь	1
"ГАРАНТ аэро" (Сервер) v8.00.2.025 8.00.2.025	1
"ГАРАНТ аэро" (ФайлСервер) Текущий Пользователь	14
=NMAS Challenge Response Method 2.7.5.	1
=NMAS Client 3.4.0.	1
=Novell Client for Window	1
=Novell Client for Windows 4.91. 2007072	1
=NVIDIA Drivers 1.10.57.3	1
=NVIDIA Install Application 2.1002.115.74	1
=NVIDIA nView 136.53 136.5	1
=NVIDIA Графический драйвер 314.22 314.2	1
=OpenOffice.org 3.2 3.2.950	1
=Panasonic Document Scanner Device Driver 8.0 8.	1
=Presto! PageManager 9.23 9.23.0	1
=Punto Switcher v3.2.9.24	1
=Realtek High Definition Audio Driver 5.10.0.619	1
=Total Commander 8.0	1
=UltraISO Premium v9.6.0.3000 9.6.0.300	1
=Uninstall Too	1
=Vista Drive Icon v2.	1
=WebFldrs XP 9.50.752	1
=Winamp 5.66	1
=WinDjView 1.0.3 1.0.	1
=Windows Genuine Advantage Validation Tool (KB892130) 1.9.0042.	1
=Windows Internet Explorer 8 20090308.14074	1
=Windows Media Format 11 runtim	1
=Windows Media Player 1	1
=WinRAR 5.01 (32-разрядная) 5.01.	1

Рисунок 33 - Фрагмент отчета о составе ПО

Отчет о количественном составе устройств показан на рисунке 34.

Количественный состав по устройствам

Наименование устройства	Количество
(R) ICH10 Family USB Universal Host Controller - 3A37 PCI шина 0, устройство 26	1
(R) ICH10 Family USB Universal Host Controller - 3A38 PCI шина 0, устройство 26	1
.0 FlashDisk F:\	1
=Mouse HID-совместимая мышь (Disabl.	4
=Net Прямой параллельный пор	2
=Printer IP_10.32.5.148 Samsung ML-3050 Series PCL	1
=Printer Microsoft Document Imaging Writer Port: Microsoft Office Document Image Writer Drive	1
=Printer XPSPort: Microsoft XPS Document Write	2
=Processor Intel процессор Intel(R) Xeon(R) CPU E5630 @ 2.53GH	16
=Processor Процессор AMD Athlon(tm) II X2 240 Processo	2
=SCSIAdapter ServeRAID M1015 SAS/SATA Controller PCI шина 1, устройство 0, функция	1
=SmartCardFilter Драйвер фильтра смарт-карты ScFilter (Disabl.	2
=SmartCardReader Aladdin IFD Handler Root enumerato	4
=SmartCardReader Aladdin VR Handler Root enumerato	2
=SmartCardReader Устройство чтения смарт-карт Microsoft Usbccid (WUDF) Port_#0001.Hub_#0003 (Disabl.	1
=SmartCardReader Устройство чтения смарт-карт Microsoft Usbccid (WUDF) Port_#0002.Hub_#0004 (Disabl.	3

Рисунок 34 - Фрагмент отчета о составе устройств (фрагмент)

Отчет о списке обнаруженных компьютеров показан на рисунке 35.

Список компьютеров

Имя компьютера	IP-адрес	ФИО пользователя	ОЗУ, МВ	Жесткий диск, МБ
WS03200511013	10.32.5.103 Hos	Тамбовцева Оксана Геннадьевна	2813	238469
WS03200510050	10.32.5.109 Hos	Носырева Мария Евгеньевна	3810	238473
SW03200508001	10.32.5.10 Host	Потехин Евгений Юрьевич	8148	1427639
WS03200501002	10.32.5.116 Hos	Минченко Вероника Александровна	2942	476929
WS03203501002	10.32.5.117 Hos	Шатулина Виктория Николаевна	4008	238371
SW03200508002	10.32.5.11 Host	Потехин Евгений Юрьевич	4086	715325
WS03200521009	10.32.5.122 Hos	Куроптева Марина Владимировна	3810	1907723
WS03203511003	10.32.5.124 Hos	Гавричкина Елена Николаевна	4008	238371

Рисунок 35 - Отчет о списке обнаруженных компьютеров (фрагмент)

Таким образом, все поставленные задачи реализованы в рамках поставленной задачи.

На рисунке 36 приведена схема модульной структуры программы.

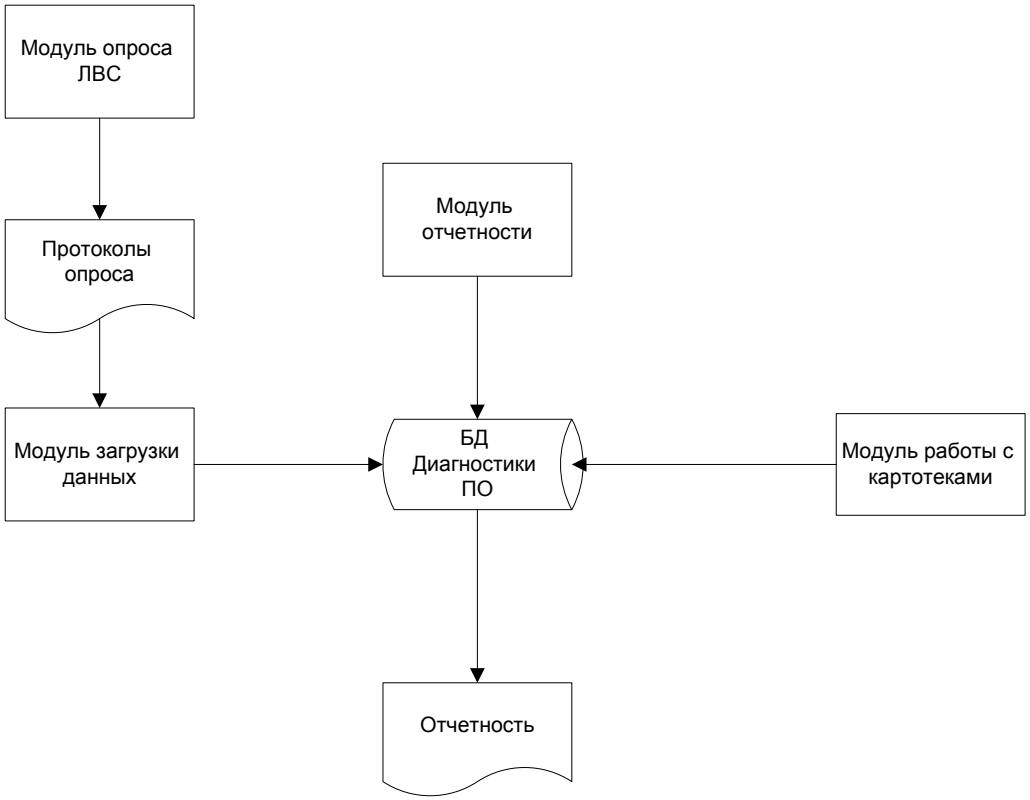


Рисунок 36 - Схема модульной структуры программы

Как показано на рисунке 36, разработанная система содержит модули:

- модуль опроса локальной сети;
- модуль загрузки данных;
- модуль работы с картотеками;
- модуль отчетности.

Проведем краткое описание модулей системы.

1.Модуль опроса локальной сети.

Опрос локальной сети производится с целью получения информации о программном и аппаратном обеспечении на рабочих станциях пользователей. Опрос сегментов локальной сети производится с использованием модуля checkcfg, который с помощью административных политик прописывается в автозагрузку на рабочие станции и сервера. Используемый протокол –

TCP/IP. Безопасность обеспечивается с использованием системы разграничения доступа, заданной системными политиками организации. На рабочие станции никакого дополнительного ПО устанавливать не требуется.

Протоколы опроса, содержащие данные о характеристиках сети, копируются в сетевой каталог, доступ к которому ограничивается с помощью административных политик.

Пример настройки системы опроса локальной сети:

[Program]

Program=C:\diag\Checkcfg.exe v.1.61

OutputDir=W:\diag\ (сетевой диск, на который копируются протоколы опроса системы)

MapNetDisk=нет

ClearThisFile=0

DOSFileName=0

MACaddrToFileName=1

NoBadMACaddr=0

MaxNameLength=30

1. Модуль загрузки данных

Протоколы системы, образец которых приведен в Приложении 1, загружаются в базу данных системы, где приобретают структурированный вид.

3.Модуль работы с картотеками

Администратор сети по результату загрузки информации проводит анализ состояния программного и аппаратного обеспечения в сети с формированием отчетов (паспорт рабочего места)

4.Модуль отчётности

Данный модуль позволяет формировать отчеты в разрезе пользователей, программ и аппаратного комплекса.

Качественные показатели проектных решений:

- вероятность отказа при работе с системой;

- правильность расчетов, проводимых программным средством;

- соответствие реализованных задач поставленным в техническом задании;

- быстродействие системы;

- устойчивость к ошибкам пользователей.

Тестирование реализованного программного средства показало следующие результаты:

- вероятность самопроизвольного отказа системы – 0%;

- правильность расчетов – 100%

- соответствие реализованных задач поставленным – 75%;

- параметры быстродействия – соответствуют технологии работы специалиста;

- устойчивость к ошибкам пользователей – 98%.

ЗАКЛЮЧЕНИЕ

Целью настоящей работы была разработка программного продукта для мониторинга программно-аппаратной среды.

Для достижения цели были поставлены задачи:

- анализ технологий мониторинга программно-аппаратной среды в удаленном режиме;

- определение области применимости для мониторинга программно-аппаратной среды в условиях исследуемого предприятия;

- рассмотрение возможных решений в области автоматизации мониторинга программно-аппаратной среды;

- разработка программного обеспечения В аналитической части дипломного проекта выполнен комплекс работ, направленных на обоснование необходимости автоматизации: определена сущность задачи, описаны основные свойства существующей информационной системы, дано описание основному бизнес-процессу, рассмотрены вопросы, связанные с анализом существующих разработок в области мониторинга программно-аппаратной среды. Также в первой главе рассмотрены вопросы обеспечения информационной безопасности в контексте решаемой задачи.

На основании проведенной работы были получены следующие результаты:

- разработана информационная система, проводящая обработку сканирования ресурсов локальной сети предприятия;

- по результатам загрузки протоколов в системе становится доступной информация о программных и аппаратных средствах вычислительной сети, а также пользователях информационной системы;

- разработанная система позволяет проводить формирование отчётности и выборок по базе данных.

Проектная часть посвящена разработке системы мониторинга программно-аппаратной среды. Показано, что решение данной задачи может

быть реализовано в виде компоненты корпоративной антивирусной защиты, в виде специализированных программных решений, а также в виде систем защиты данных.

Для каждого из указанных видов решений была определена область применимости. Итогом работы системы явилась реализация политики решения поставленной задачи – для каждого из подразделений определено оптимальное решение в области мониторинга программно-аппаратной среды.

Таким образом, задачи проекта решены и цель достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Checkcfg.exe – инвентаризация компьютеров. [Электронный ресурс]. Режим доступа: http://checkcfg.narod.ru/soft.htm
2. Акперов, И.Г. Информационные технологии в менеджменте: Учебник / И.Г. Акперов, А.В. Сметанин, И.А. Коноплева. - М.: НИЦ ИНФРА-М, 2013. - 400 с.
3. Венделева, М.А. Информационные технологии в управлении: Учебное пособие для бакалавров / М.А. Венделева, Ю.В. Вертакова. - М.: Юрайт, 2013. - 462 с.
4. Лубянская Э.Б. Информационные системы в экономике : учебное пособие / Э.Б. Лубянская, Е.Н. Лукаш. - Воронеж : ФГБОУ ВО "Воронежский государственный технический университет", 2017. - 140 с.
5. Горячев, А.В. Особенности разработки и администрирования приложений баз данных: учебное пособие / А. В. Горячев, Н. Е. Новакова. Санкт-Петербург : Издательство СПбГЭТУ, 2016. - 68 с.
6. Селяничев, О. Л. Администрирование информационных систем: учебное пособие / О. Л. Селяничев, Е. В. Майтама. - Череповец: ФГБОУ ВО "Череповецкий государственный университет", 2017. - 99 с.
7. Попов Б. Н. Администрирование информационных систем: учебное пособие / Б. Н. Попов. - Санкт-Петербург : Изд-во ГУМРФ имени адмирала С.О. Макарова, 2018. - 95 с.
8. Королев Е. Н. Администрирование операционных систем : учебное пособие / Е. Н. Королев. - Воронеж : Воронежский государственный технический университет, 2017. - 85 с.
9. Попов Б. Н. Администрирование информационных систем : учебное пособие / Б. Н. Попов. - Санкт-Петербург : Изд-во ГУМРФ имени адмирала С.О. Макарова, 2018. - 95 с.
10. Дадян, Э.Г. Современные базы данных. Часть 2: практические задания: Учебно-методическое пособие / Дадян Э.Г. - М.:НИЦ ИНФРА-М, 2017. - 68 с

11. Гвоздева, В.А. Базы и банки данных [Электронный ресурс] / В.А. Гвоздева. - М.: Альтаир-МГАВТ, 2015, - 76 с.

12. Гофман, В.Э. Работа с базами данных в Delphi: Пособие / Хомоненко А.Д., Гофман В.Э., - 3-е изд., перераб. и доп. - СПб:БХВ-Петербург, 2014. - 628 с.

13. Колдаев, В.Д. Структуры и алгоритмы обработки данных: Учебное пособие / В.Д. Колдаев. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 296 с.

14. Коннолли Т., Бегг К. Базы данных: проектирование, реализация и сопровождение: теория и практика. - Москва: Вильямс, 2017. - 1439 с.

15. Зайцев А.В. Информационные системы в профессиональной деятельности [Электронный ресурс]: Учебное пособие. - М.: РАП, 2013. - 180 с.

16. Коряковский А.В. Информационные системы предприятия: Учебное пособие. - М.: НИЦ ИНФРА-М, 2016. - 283 с.

17. Титоренко Г.А. Информационные системы в экономике/ 2-е изд. - М.: ЮНИТИ-ДАНА, 2015. - 463 с.

18. Боровская Е.В. Программирование в среде Delphi - 3-е изд., (эл.) - М.: БИНОМ. ЛЗ, 2015. - 241 с.

19. Медведев М.А. Разработка информационных систем. Учебное пособие. - М.:Флинта, Изд-во Урал. ун-та, 2017. - 64 с.

20. Шипулин Л. В., Сазонова Н. С. Базы данных : учебное пособие. - Челябинск : ЮУрГУ, 2016. - 96 с.

Приложение

Протокол работы checkcfg

[Info]
MAC_Addr=000A482314E1
Current_User_Name=U05_1302
Computer_Name=WS03200521011
IP_Addr=10.32.5.144 Host: WS03200521011
System=Windows XP build 2600/Service Pack 3,Русский
Param_0=\\SW03200508001\Checkcfg\Checkcfg.exe v.1.64
Param_1=u05_1302
Param_2=Кожухова
Param_3=А.П.
Record_Date=9.06.2014
User_Rights=Administrator
[Computer]
BIOS=08/22/12
CPU_Freq_in_MHz=2894
CPU.CPUID=0206A7
CPU.BrandName=Intel(R) Pentium(R) CPU G850 @ 2.90GHz
CPU=2x Intel CPU Pentium CPU G850 @ 2.90GHz 2890 MHz
Memory_in_Mb=2989
Total_HDD_in_Mb=238463
Drive_1=A:\
Drive_2=B:\
Drive_3=C:\ Hard Disk(),Serial 2C5F710C, 238 463 Mb NTFS (free 221 601 Mb)
Drive_4=D:\
Drive_5=E:\ Network \\KAMEN\home\
Drive_6=F:\
Drive_7=G:\
Drive_8=H:\ Network \\KAMEN\apps\soft_pu\
Drive_9=I:\
Drive_10=J:\
Drive_11=K:\
Drive_12=L:\
Drive_13=M:\
Drive_14=N:\
Drive_15=O:\
Drive_16=P:\ Network \\KAMEN\apps\pen\
Drive_17=Q:\
Drive_18=R:\
Drive_19=S:\ Network \\10.32.5.10\files\
Drive_20=T:\ Network \\10.32.5.10\files\obmen\
Drive_21=U:\
Drive_22=V:\
Drive_23=W:\ Network \\10.32.5.12\scan\
Drive_24=X:\ Network \\KAMEN\apps\soft_pen\
Drive_25=Y:\
Drive_26=Z:\
[Current_Config]
Device_0=Display Intel(R) HD Graphics
Device_1=HDD WDC WD2500AAKX-00ERMA0
Device_2=Monitor <AOC1941> S\N:DLUC7HA016227
Device_3=Monitor <AOC1941> S\N:DLUC7HA016227
Device_4=Net Intel(R) 82579LM Gigabit Network Connection
[Windows_Devices]
Win_Device_0=BIOS (video) Hardware Version 0.0 08/03/20
Win_Device_1=BIOS KRFTWY - 1 InsydeH2O Version 03.61.10KWQ67 R1.12 InsydeH2O Version 03.61.10KWQ67 R1.12 InsydeH2O Version 03.61.10KWQ67 R1.12 08/22/12
Win_Device_2=Computer Многопроцессорный компьютер с ACPI
Win_Device_3=CPU x86 Family 6 Model 42 Stepping 7 x86 Family 6 Model 42 Stepping 7

Win_Device_4=disk WDC WD2500AAKX-00ERMA0
Win_Device_5=DiskDrive Дисковый накопитель Kingston DataTraveler 2.0 USB Device (Disabl.)
Win_Device_6=DiskDrive Дисковый накопитель Kingston DataTraveler 2.0 USB Device (Disabl.)
Win_Device_7=DiskDrive Дисковый накопитель SanDisk Cruzer Pop USB Device (Disabl.)
Win_Device_8=DiskDrive Дисковый накопитель silicon-power USB Device (Disabl.)
Win_Device_9=DiskDrive Дисковый накопитель USB FLASH DRIVE USB Device (Disabl.)
Win_Device_10=DiskDrive Дисковый накопитель WDC WD2500AAKX-00ERMA0 0
Win_Device_11=DiskPeripheral WDC WD2500AAKX-00ERMA0
Win_Device_12=Display Intel(R) HD Graphics PCI шина 0, устройство 2, функция 0
Win_Device_13=HIDClass HID-совместимое устройство
Win_Device_16=HIDClass HID-совместимое устройство (Disabl.)
Win_Device_17=HIDClass HID-совместимое устройство управления
Win_Device_18=HIDClass HID-совместимое устройство управления (Disabl.)
Win_Device_19=HIDClass HID-совместимое устройство управления (Disabl.)
Win_Device_20=HIDClass HID-совместимое устройство управления (Disabl.)
Win_Device_21=HIDClass USB HID-совместимое устройство
Win_Device_22=HIDClass USB HID-совместимое устройство
Win_Device_23=HIDClass USB HID-совместимое устройство (Disabl.)
Win_Device_24=HIDClass USB HID-совместимое устройство (Disabl.)
Win_Device_25=HIDClass USB HID-совместимое устройство (Disabl.)
Win_Device_26=HIDClass USB HID-совместимое устройство OM (Disabl.)
Win_Device_27=HIDClass USB HID-совместимое устройство OM (Disabl.)
Win_Device_28=HIDClass USB HID-совместимое устройство OM (Disabl.)
Win_Device_29=HIDClass USB HID-совместимое устройство USB Device (Disabl.)
Win_Device_30=HIDClass USB HID-совместимое устройство USB Device (Disabl.)
Win_Device_31=HIDClass USB HID-совместимое устройство USB Keykoard (Disabl.)
Win_Device_35=Image CanoScan LiDE 210 CanoScan LiDE 210 (Disabl.)
Win_Device_36=Image CanoScan LiDE 210 CanoScan LiDE 210 CanoScan (Disabl.)
Win_Device_37=Image CanoScan LiDE 210 CanoScan LiDE 210 CanoScan (Disabl.)
Win_Device_38=Image KV-SS081 KV-SS081 USB Device (Disabl.)
Win_Device_39=Keyboard Клавиатура HID
Win_Device_40=Keyboard Клавиатура HID (Disabl.)
Win_Device_41=Keyboard Клавиатура HID (Disabl.)
Win_Device_42=Keyboard Клавиатура HID (Disabl.)
Win_Device_43=Keyboard Клавиатура HID (Disabl.)
Win_Device_44=Keyboard Стандартная (101/102 клавиши) или клавиатура PS/2 Microsoft Natural
Win_Device_45=MEDIA Realtek High Definition Audio Внутренняя шина для High Definition Audio
Win_Device_46=MEDIA Аудио Intel(R) для дисплеев Внутренняя шина для High Definition Audio
Win_Device_47=MEDIA Аудио кодеки
Win_Device_48=MEDIA Видео кодеки
Win_Device_49=MEDIA Драйвер совместимости звука Microsoft (WINMM WDM)
Win_Device_50=MEDIA Драйверы аудио (без PnP)
Win_Device_51=MEDIA Синтезатор звуковой таблицы Microsoft Kernel GS
Win_Device_52=MEDIA Устройства записи видео (без PnP)
Win_Device_53=MEDIA Устройство управления
Win_Device_54=Monitor Модуль подключения монитора
Win_Device_55=Monitor Модуль подключения монитора
Win_Device_56=Monitor Модуль подключения монитора (Disabl.)
Win_Device_57=Monitor Модуль подключения монитора (Disabl.)
Win_Device_58=Monitor Монитор по умолчанию (Disabl.)
Win_Device_59=Monitor Монитор по умолчанию (Disabl.)
Win_Device_60=Mouse HID-совместимая мышь (Disabl.)
Win_Device_61=Mouse HID-совместимая мышь (Disabl.)
Win_Device_62=Mouse HID-совместимая мышь (Disabl.)
Win_Device_63=Mouse HID-совместимая мышь (Disabl.)
Win_Device_64=Mouse HID-совместимая мышь (Disabl.)
Win_Device_65=Mouse Microsoft PS/2 мышь
Win_Device_66=Net [1]Card Intel(R) 82579LM Gigabit Network Connection
Win_Device_67=Net [1]DefaultGateway 10.32.5.254
Win_Device_68=Net [1]DhcpServer 255.255.255.255
Win_Device_69=Net [1]IPAddress 10.32.5.144
Win_Device_70=Net [1]SubnetMask 255.255.255.0

Win_Device_71=Net [2]Card Intel(R) 82574L Gigabit Network Connection
Win_Device_72=Net [2]DefaultGateway 10.32.5.254
Win_Device_73=Net [2]DhcpServer 255.255.255.255
Win_Device_74=Net [2]IPAddress 10.32.5.206
Win_Device_75=Net [2]SubnetMask 255.255.255.0
Win_Device_76=Net DNSconfig 10.32.5.10
Win_Device_77=Net DNSconfig 10.32.5.10
Win_Device_78=Net HostName ws03200521011.PFR.ALTAI.RU
Win_Device_79=Net Intel(R) 82574L Gigabit Network Connection PCI шина 3, устройство 0, функция 0
Win_Device_80=Net Intel(R) 82579LM Gigabit Network Connection PCI шина 0, устройство 25, функция 0
Win_Device_81=Net RAS асинхронный адаптер (Disabl.)
Win_Device_82=Net Минипорт WAN (IP)
Win_Device_83=Net Минипорт WAN (IPX)
Win_Device_84=Net Минипорт WAN (L2TP)
Win_Device_85=Net Минипорт WAN (PPPoE)
Win_Device_86=Net Минипорт WAN (PPTP)
Win_Device_87=Net Минипорт планировщика пакетов Intel(R) 82574L Gigabit Network Connection - Минипорт планировщика пакетов
Win_Device_88=Net Минипорт планировщика пакетов Intel(R) 82579LM Gigabit Network Connection - Минипорт планировщика пакетов
Win_Device_89=Net Минипорт планировщика пакетов Минипорт WAN (IP) - Минипорт планировщика пакетов
Win_Device_90=Net Прямой параллельный порт
Win_Device_91=Printer Microsoft Document Imaging Writer Port: Microsoft Office Document Image Writer Driver
Win_Device_92=Printer NUL PageManager PDF Writer
Win_Device_93=Printer USB001 Samsung ML-375x Series PCL 6
Win_Device_94=Printer XPSPort: Microsoft XPS Document Writer
Win_Device_95=Processor Intel процессор Intel(R) Pentium(R) CPU G850 @ 2.90GHz
Win_Device_96=Processor Intel процессор Intel(R) Pentium(R) CPU G850 @ 2.90GHz
Win_Device_97=SmartCardReader Aladdin IFD Handler Root enumerator
Win_Device_98=SmartCardReader Aladdin IFD Handler Root enumerator
Win_Device_99=SmartCardReader Aladdin VR Handler Root enumerator
Win_Device_100=USB Intel(R) 6 Series/C200 Series Chipset Family USB Enhanced Host Controller - 1C26 PCI шина 0, устройство 29, функция 0
Win_Device_101=USB Intel(R) 6 Series/C200 Series Chipset Family USB Enhanced Host Controller - 1C2D PCI шина 0, устройство 26, функция 0
Win_Device_102=USB NEC Electronics USB 3.0 Host Controller PCI шина 2, устройство 0, функция 0
Win_Device_103=USB NEC Electronics USB 3.0 Root Hub
Win_Device_104=USB USB Token eToken Pro 4254
Win_Device_105=USB USB Token Token JC (Disabl.)
Win_Device_106=USB Запоминающее устройство для USB DataTraveler 2.0 (Disabl.)
Win_Device_107=USB Запоминающее устройство для USB DataTraveler 2.0 (Disabl.)
Win_Device_108=USB Запоминающее устройство для USB Firebird USB Flash Drive (Disabl.)
Win_Device_109=USB Запоминающее устройство для USB silicon-power (Disabl.)
Win_Device_110=USB Запоминающее устройство для USB USB FLASH DRIVE (Disabl.)
Win_Device_111=USB Корневой USB концентратор
Win_Device_112=USB Корневой USB концентратор
Win_Device_113=USB Неизвестное устройство USB Device (Disabl.)
Win_Device_114=USB Неизвестное устройство USB Device (Disabl.)
Win_Device_115=USB Поддержка USB принтера ML-375x Series
Win_Device_116=USB Составное USB устройство
Win_Device_117=USB Составное USB устройство (Disabl.)
Win_Device_118=USB Составное USB устройство USB Device (Disabl.)
Win_Device_119=USB Составное USB устройство USB Keykoard (Disabl.)
Win_Device_120=USB Составное USB устройство USB Keykoard (Disabl.)
Win_Device_121=USB Универсальный USB концентратор USB Device
Win_Device_122=USB Универсальный USB концентратор USB Device
Win_Device_123=USB Универсальный USB концентратор USB2.0 Hub
Win_Device_124=Volume Универсальный том
Win_Device_125=Volume Универсальный том (Disabl.)

Win_Device_126=Volume Универсальный том (Disabl.) RemovableMedia Kingston DataTraveler 2.0 USB Device
Win_Device_127=Volume Универсальный том (Disabl.) RemovableMedia Kingston DataTraveler 2.0 USB Device
Win_Device_128=Volume Универсальный том (Disabl.) RemovableMedia SanDisk Cruzer Pop USB Device
Win_Device_129=Volume Универсальный том (Disabl.) RemovableMedia silicon-power USB Device
Win_Device_130=Volume Универсальный том (Disabl.) RemovableMedia USB FLASH DRIVE USB Device
[Windows_Updates]
Win_Update_0=Internet Explorer BASEIE40_W2K v.8,0,6001,18702
Win_Update_1=Internet Explorer Core Fonts Fontcore v.8,0,6001,18702
Win_Update_2=Internet Explorer Help HelpCont v.8,0,6001,18702
Win_Update_3=Internet Explorer IEACCESS v.8,0,6001,18702
Win_Update_4=Internet Explorer Setup Tools GenSetup v.8,0,6001,18702
Win_Update_5=KB2508272
Win_Update_6=KB2570791
Win_Update_7=KB2809289-IE8
Win_Update_8=KB898461
Win_Update_9=KB942288-v3
Win_Update_10=KB954550-v5
Win_Update_11=KB958644
Win_Update_12=KB958687
Win_Update_13=Microsoft Outlook Express 6 MailNews v.6,0,2900,5512
Win_Update_14=Microsoft Windows Media Player Microsoft Windows Media Player v.9,0,0,4503
Win_Update_15=Microsoft Windows Media Player WMPACCESS v.9,0,0,4503
Win_Update_16=Microsoft Windows Script 5.7 MSVBScript v.5,7,0,16599
Win_Update_17=Outlook Express OEACCESS v.2,0,0,0
Win_Update_18=Q147222
Win_Update_19=RootsUpdate Windows Roots Update v.38,0,2195,0
Win_Update_20=Windows Desktop Update IE4Shell_NT v.6,0,2900,5512
Win_Update_21=Проигрыватель Windows Media (Microsoft) 6.4 Microsoft Windows Media Player v.9,0,0,4503
[Windows_StartUp]
Win_Start_0=Common Startup folder desktop.ini
Win_Start_1=Registry ()
Win_Start_2=Registry Adobe ARM ("C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe")
Win_Start_3=Registry AVP ("C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 8 for Windows\avp.exe")
Win_Start_4=Registry CDAServer (C:\Program Files\Common Files\Common Desktop Agent\CDASrv.exe)
Win_Start_5=Registry Client Access Check Version ("C:\Program Files\IBM\Client Access\cwbckver.exe" LOGIN)
Win_Start_6=Registry Client Access Express Welcome ("C:\Program Files\IBM\Client Access\cwbwlwiz.exe")
Win_Start_7=Registry Client Access Help Update ("C:\Program Files\IBM\Client Access\cwbinhlp.exe")
Win_Start_8=Registry Client Access PC5250 Sound ("C:\Program Files\IBM\Client Access\Emulator\pcssnd.exe")
Win_Start_9=Registry Client Access Service ("C:\Program Files\IBM\Client Access\cwbsvstr.exe")
Win_Start_10=Registry CryptoServer (C:\Program Files\CryptoServer\CryptoServer.exe)
Win_Start_11=Registry CTFMON.EXE (C:\WINDOWS\system32\ctfmon.exe)
Win_Start_12=Registry eTMonitor ("C:\Program Files\Aladdin\eToken\PKIClient\x32\PKIMonitor.exe")
Win_Start_13=Registry eTokenSSO (C:\Program Files\Aladdin\eToken\eTokenSSO\eSSOClient.exe /hide)
Win_Start_14=Registry HotKeysCmds (C:\WINDOWS\system32\hkcmd.exe)
Win_Start_15=Registry IAStorIcon (C:\Program Files\Intel\Intel(R) Rapid Storage Technology\IAStorIcon.exe)
Win_Start_16=Registry IgfxTray (C:\WINDOWS\system32\igfxtray.exe)
Win_Start_17=Registry ITCSCLITE ("C:\Program Files\InfoTeCS\ViPNet CryptoService\CLite.exe" /startup)
Win_Start_18=Registry NWTRAY (NWTRAY.EXE)
Win_Start_19=Registry Persistence (C:\WINDOWS\system32\igfxpers.exe)
Win_Start_20=Registry PMSpeed (C:\Program Files\NewSoft\Presto! PageManager 9.23\PMSpeed.EXE)
Win_Start_21=Registry RTHDCPL (RTHDCPL.EXE)
Win_Start_22=Registry Startcpls (c:\software.dst\Startcpls\StartCPLs.exe)
Win_Start_23=Registry SunJavaUpdateSched ("C:\Program Files\Java\jre6\bin\jusched.exe")
Win_Start_24=Registry WrtMon.exe (C:\WINDOWS\system32\spool\drivers\w32x86\3\WrtMon.exe)
Win_Start_25=Startup folder desktop.ini
Win_Start_26=Startup folder OpenOffice.org 3.2.lnk
[Windows_Soft]
Win_Soft_0=Adobe Reader XI (11.0.02) - Russian 11.0.02

Win_Soft_1=CanoScan LiDE 210 Scanner Driver
Win_Soft_2=CheckPfr
Win_Soft_3=CheckXML
Win_Soft_4=Common Desktop Agent 1.53.0
Win_Soft_5=CreatePackageXML 1.4.1
Win_Soft_6=CryptoServer 1.2.7
Win_Soft_7=DB2 Run-Time Client 8.1.16
Win_Soft_8=eToken Network Logon 5.1 5.1.5.0
Win_Soft_9=eToken PKI Client 5.1 SP1 5.1.66.0
Win_Soft_10=eToken Single Sign-On 5.1 5.1.5.0
Win_Soft_11=FAR file manager
Win_Soft_12=Hotfix for Microsoft .NET Framework 3.5 SP1 (KB953595) 1
Win_Soft_13=IBM iSeries Access for Windows
Win_Soft_14=Intel(R) Network Connections Drivers 16.3
Win_Soft_15=Intel(R) Rapid Storage Technology 11.0.0.1032
Win_Soft_16=J2SE Runtime Environment 5.0 Update 11 1.5.0.110
Win_Soft_17=Java Auto Updater 2.0.2.1
Win_Soft_18=Java(TM) 6 Update 20 6.0.200
Win_Soft_19=Kaspersky Endpoint Security 8 для Windows 8.1.1.1042
Win_Soft_20=KV-SS081 TWAIN Driver 10.1
Win_Soft_21=Lotus Notes 7.0.2 ru 7.02.6269
Win_Soft_22=Microsoft .NET Framework 2.0 Service Pack 2 2.2.30729
Win_Soft_23=Microsoft .NET Framework 3.0 Service Pack 2 3.2.30729
Win_Soft_24=Microsoft .NET Framework 3.5 SP1
Win_Soft_25=Microsoft .NET Framework 3.5 SP1 3.5.30729
Win_Soft_26=Microsoft .NET Framework 4 Client Profile 4.0.30319
Win_Soft_27=Microsoft .NET Framework 4 Extended 4.0.30319
Win_Soft_28=Microsoft Internet Explorer 8.0.6001.18702
Win_Soft_29=Microsoft Office - профессиональный выпуск версии 2003 11.0.7969.0
Win_Soft_30=Microsoft Office - профессиональный выпуск версии 2003 Key GWH28-DGCMP-P6RC4-6J4MT-3HFDY
Win_Soft_31=Microsoft SOAP Toolkit 3.0 3.0.1325.4
Win_Soft_32=Microsoft Visual C++ 2005 Redistributable 8.0.59193
Win_Soft_33=Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022 9.0.21022
Win_Soft_34=Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148 9.0.30729.4148
Win_Soft_35=Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 10.0.40219
Win_Soft_36=Microsoft Windows XP Key H63MC-KJ7C8-YFY2Q-GGV2W-CKTMM
Win_Soft_37=NICI (Shared) U.S./Worldwide (128 bit) (2.7.3-1)
Win_Soft_38=NMAS Challenge Response Method 2.7.5.0
Win_Soft_39=NMAS Client 3.4.0.0
Win_Soft_40=Novell Client for Windows
Win_Soft_41=Novell Client for Windows 4.91. 20070720
Win_Soft_42=OpenOffice.org 3.2 3.2.9502
Win_Soft_43=Panasonic Document Scanner Device Driver 8.0 8.0
Win_Soft_44=Presto! BizCard 6 6.11.10
Win_Soft_45=Presto! PageManager 9.23 9.23.02
Win_Soft_46=Realtek High Definition Audio Driver 5.10.0.6662
Win_Soft_47=Samsung Easy Printer Manager 1.02.03.00
Win_Soft_48=Samsung Printer Live Update
Win_Soft_49=Signature ActiveX 1.0.0
Win_Soft_50=SPU
Win_Soft_51=Total Commander 7.02a PowerPack
Win_Soft_52=ViPNet CryptoService 3.2 (9.14725)
Win_Soft_53=WebFldrs XP 9.50.7523
Win_Soft_54=WinDjView 1.0.3 1.0.3
Win_Soft_55=Windows Internet Explorer 8 20090308.140743
Win_Soft_56=XP_Check 3.0.0.0
Win_Soft_57=Агент администрирования Kaspersky Security Center 9.3.75
Win_Soft_58=Клиент служб терминалов
Win_Soft_59=Программа Spu_orb (remove only)
Win_Soft_60=Статистика БД ПТК СПУ (Is2002-Ufa) 2.4.71
[Internet]

Param_1=User Agent : Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Param_2=ProxyEnable : No
Param_3=EnableHttp1_1 : Yes
Param_4=MigrateProxy : Yes
Param_5=DisableCachingOfSSLPages : No
Param_6=EnableNegotiate : Yes
Param_7=WarnOnZoneCrossing : No
Param_8=Local intranet Sec.Level : Customized
Param_9=Надежные узлы Sec.Level : Low
Param_10=Internet Sec.Level : Customized
Param_11=Restricted sites Sec.Level : Customized
Connection_1=DefaultConnectionSettings :
Connection_2=SavedLegacySettings :
[Sharing]
print$=CSCFlags:0 MaxUses:4294967295 Path:C:\WINDOWS\system32\spool\drivers Permissions:0 Remark: Type:0
rp0320052101101=CSCFlags:0 MaxUses:4294967295 Path:Samsung ML-375x Series PCL 6,LocalsplOnly Permissions:0 Remark:Samsung ML-375x Series PCL 6 Type:1
[Checkcfg_Log]
25.11.2013 8:27:59=U05_1302, Run param.: u05_1302 Кожухова А.П.
25.11.2013 8:28:12=U05_1302, Run param.: u05_1302 Кожухова А.П.
25.11.2013 8:27:57=U05_1302, Run param.: u05_1302 Кожухова А.П.
26.11.2013 7:38:51=U05_1302, Run param.: u05_1302 Кожухова А.П.
26.11.2013 7:39:05=U05_1302, Run param.: u05_1302 Кожухова А.П.
26.11.2013 8:09:28=U05_1302, Run param.: u05_1302 Кожухова А.П.
26.11.2013 8:09:20=U05_1302, Run param.: u05_1302 Кожухова А.П.
26.11.2013 8:09:33=U05_1302, Run param.: u05_1302 Кожухова А.П.
26.11.2013 8:09:22=U05_1302, Run param.: u05_1302 Кожухова А.П.
26.11.2013 10:06:26=U05_1302, Run param.: u05_1302 Кожухова А.П.
27.11.2013 7:36:00=U05_1302, Run param.: u05_1302 Кожухова А.П.
28.11.2013 7:50:26=U05_1302, Run param.: u05_1302 Кожухова А.П.
[Config_changes]
25.11.2013 08:27:59 2=Internet counter has changed FROM :0 TO :13
25.11.2013 08:27:59 3=Sharing counter has changed FROM :0 TO :2
25.11.2013 08:27:59 4=ADDED in Sharing : print$=CSCFlags:0 MaxUses:4294967295 Path:C:\WINDOWS\system32\spool\drivers Permissions:0 Remark: Type:0
25.11.2013 08:27:59 5=ADDED in Sharing : rp0320052101101=CSCFlags:0 MaxUses:4294967295 Path:Samsung ML-375x Series PCL 6,LocalsplOnly Permissions:0 Remark:Samsung ML-375x Series PCL 6 Type:1
30.05.2014 08:02:01 2=Computer\Drive_16 has changed FROM :P:\ Network \\KAMEN\apps\pen\ TO :P:\
30.05.2014 08:02:01 3=Computer\Drive_24 has changed FROM :X:\ Network \\KAMEN\apps\soft_pen\ TO :X:\
04.06.2014 07:34:07 0=Computer\Drive_5 has changed FROM :E:\ Network \\KAMEN\home\ TO :E:\
04.06.2014 07:34:07 1=Computer\Drive_8 has changed FROM :H:\ Network \\KAMEN\apps\soft_pu\ TO :H:\
04.06.2014 07:34:07 2=Computer\Drive_16 has changed FROM :P:\ Network \\KAMEN\apps\pen\ TO :P:\
04.06.2014 07:34:07 3=Computer\Drive_24 has changed FROM :X:\ Network \\KAMEN\apps\soft_pen\ TO :X:\
05.06.2014 07:45:57 0=Computer\Drive_5 has changed FROM :E:\ Network \\KAMEN\home\ TO :E:\
05.06.2014 07:45:57 1=Computer\Drive_8 has changed FROM :H:\ Network \\KAMEN\apps\soft_pu\ TO :H:\
05.06.2014 07:45:57 2=Computer\Drive_16 has changed FROM :P:\ Network \\KAMEN\apps\pen\ TO :P:\
05.06.2014 07:45:57 3=Computer\Drive_24 has changed FROM :X:\ Network \\KAMEN\apps\soft_pen\ TO :X:\
[Signature]
0=4JYO-3QYL-E326-SSIQ-XQHC-ZUXH-TWBB-F3E9
1=\\10.32.5.10\confws\000A482314E1 09.06.2014 7:41:12
[S.M.A.R.T.]
HDD0_Info=
HDD1_Info=
HDD2_Info=
HDD3_Info=
[Hardware]
BIOS ReleaseDate=08/22/2012
BIOS Vendor=INSYDE
BIOS Version=KWQ67 R1.12
Board Asset Tag=Board_Asset_Tag
Board Product=KWQ67

Board ser.N=Board_Serial_Number
Board type=Motherboard
Board vendor=Kraftway
Board version=1.0
Chassis Asset Tag=Chassis_Asset_Tag
Chassis ser.N=Chassis_Serial_Number
Chassis type=Desktop
Chassis vendor=Chassis_Manufacturer
Chassis version=Chassis_Version
MEM1 info=Non-volatileCache DRAMWindow DRAMEDOCMOSSynchronousERAMBUSPseudo-staticStatic columnFast-paged 780bits, Memory device not installed
MEM2 asset Tag=0123456789
MEM2 bank=BANK 0
MEM2 device=ChannelA-DIMM0
MEM2 info=DIMM Synchronous 64bits, 1333MHz, 2048MB
MEM2 part N=AV32G1339U1
MEM2 Ser.N=00000000
OnboardDevice 1=Type:Ethernet Hanksville Gbe Lan Connection
Product name=Kraftway Credo KCxx
Product version=1.00
RAM1 info=DIMM type, 2048MB single-bank connection
RAM1 socket=ChannelA-DIMM0
System ser.N=11255939
System UID=0000B09A11A3204D9974000A482314E1
System vendor=KRAFTWAY
[History]
25.11.2013 8:27:38=File_Name 000A4823307F -> 000A482314E1
25.11.2013 8:27:40=MAC_Addr 000A4823307F -> 000A482314E1