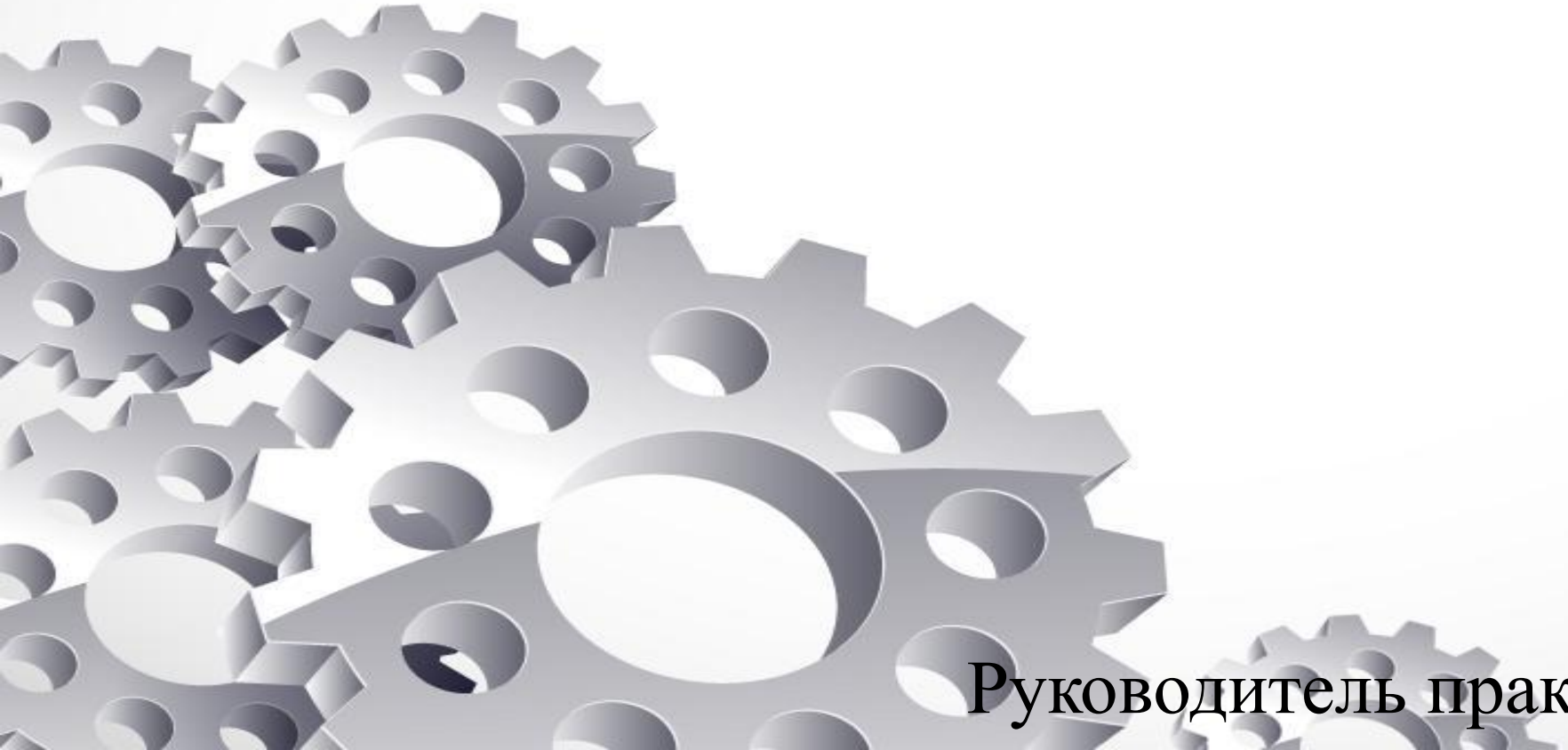
Отчет по производственной практике ПП 01.01 «Информационные системы» Общество с ограниченной ответственностью «Технология безопасности - Ачинск»



Ст. группы 16-ИС
Хаченковой Марины
Руководитель практики: Горюнова Е. А.

Цель практики:

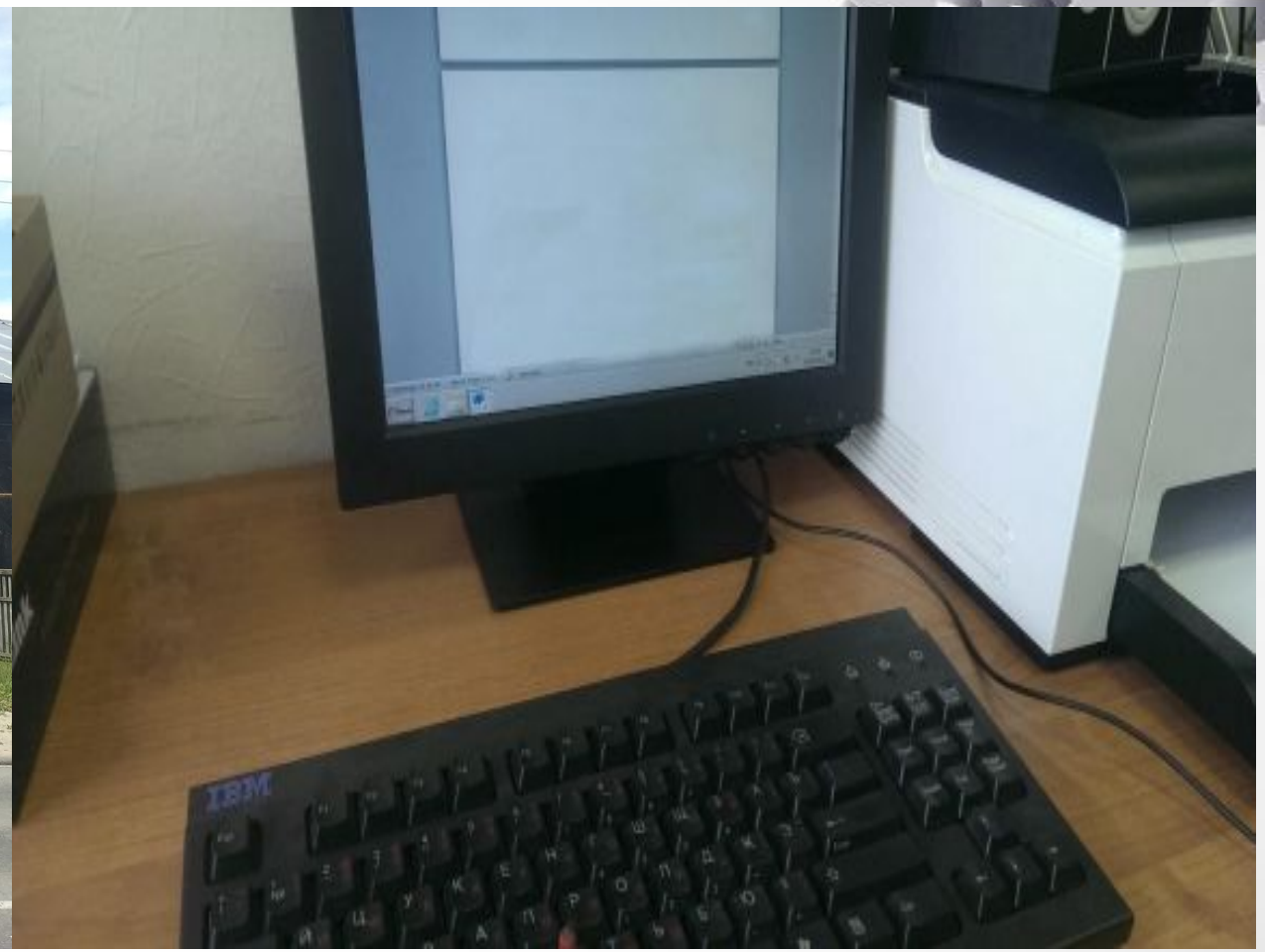
- изучать инструкцию по технике безопасности при работе на пк;
- организовать рабочее место;
- изучать цели и задачи практики;
- собирать информацию об организационной структуре предприятия, о должностных инструкций на рабочих местах, о документообороте;
- собирать информацию об основных характеристиках средств вычислительной техники и программного обеспечения;
- изучать инструкции наладчика компьютерных систем или наладчика аппаратно-программных систем;
- собирать информацию о системах профилактического обслуживания компьютеров в организации;
- описывать проведение контроля, диагностики и восстановления работоспособности компьютерных систем и комплексов;
- проводить анализ структуры информационной системы;
- описывать основные объекты информационной системы;
- составлять инструкций пользователям;
- применять методы защиты информации.

Основные задачи сопровождения информационной системы

- Во время своей практики я работала у индивидуального предпринимателя с 07 июня 2019 г. по 05 июля 2019 г. Я прошла вводную беседу по теме практики, изучила инструкции по охране труда при работе на ПК, ознакомилась с организационной структурой предприятия и ключевыми видами деятельности организации.
- Также я изучила внутренний распорядок, подготовила рабочее место, выполнила работы на ПК

Фото организации

Мое рабочее место



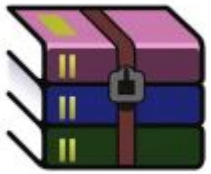
Анализ структуры организации, описание аппаратного и программного обеспечения организации

Основная ценность компании Гарант*К - уникальные знания и опыт в компьютерной и копировальной технике, накопленные за годы работы. Клиентами компании на сегодняшний день являются предприятия и частные лица г. Кулебаки, Выксы, а также р. поселков Шилокши, Ломовки, Гремячева.

В числе услуг оказываемых компанией можно выделить:

- сервисное и абонентское обслуживание организаций;
- компьютерная помощь на дому от Центра Поддержки;
- ксерокопия, черно-белая и цветная печать, набор текста, сканирование, запись CD/DVD;
- диагностика и ремонт ноутбуков, принтеров;
- установка сетей беспроводного интернета (Wi-Fi).

В компании используется следующий стандартный набор программ:



- Kaspersky Anti-Virus;
- WinRAR;
- Microsoft Office - офисный пакет;

- Google Chrome - веб-браузер;
- View FDCommander - файловый менеджер;
- STDU Viewer - универсальный просмотрщик электронных документов различных форматов;

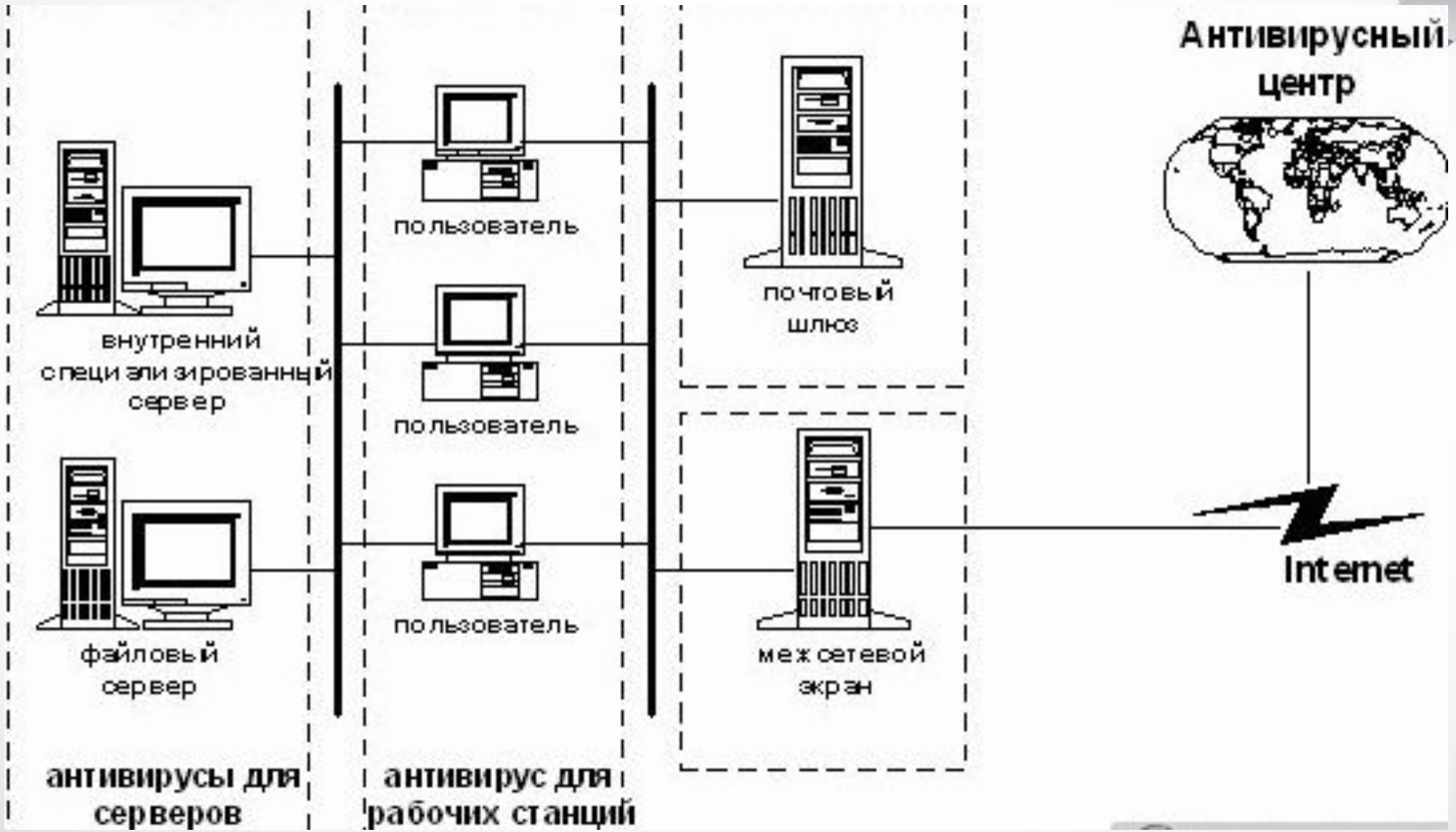
- 1С: Предприятие 8 - система автоматизации учета и управления;

Антивирусная защита компьютерной сети предприятия

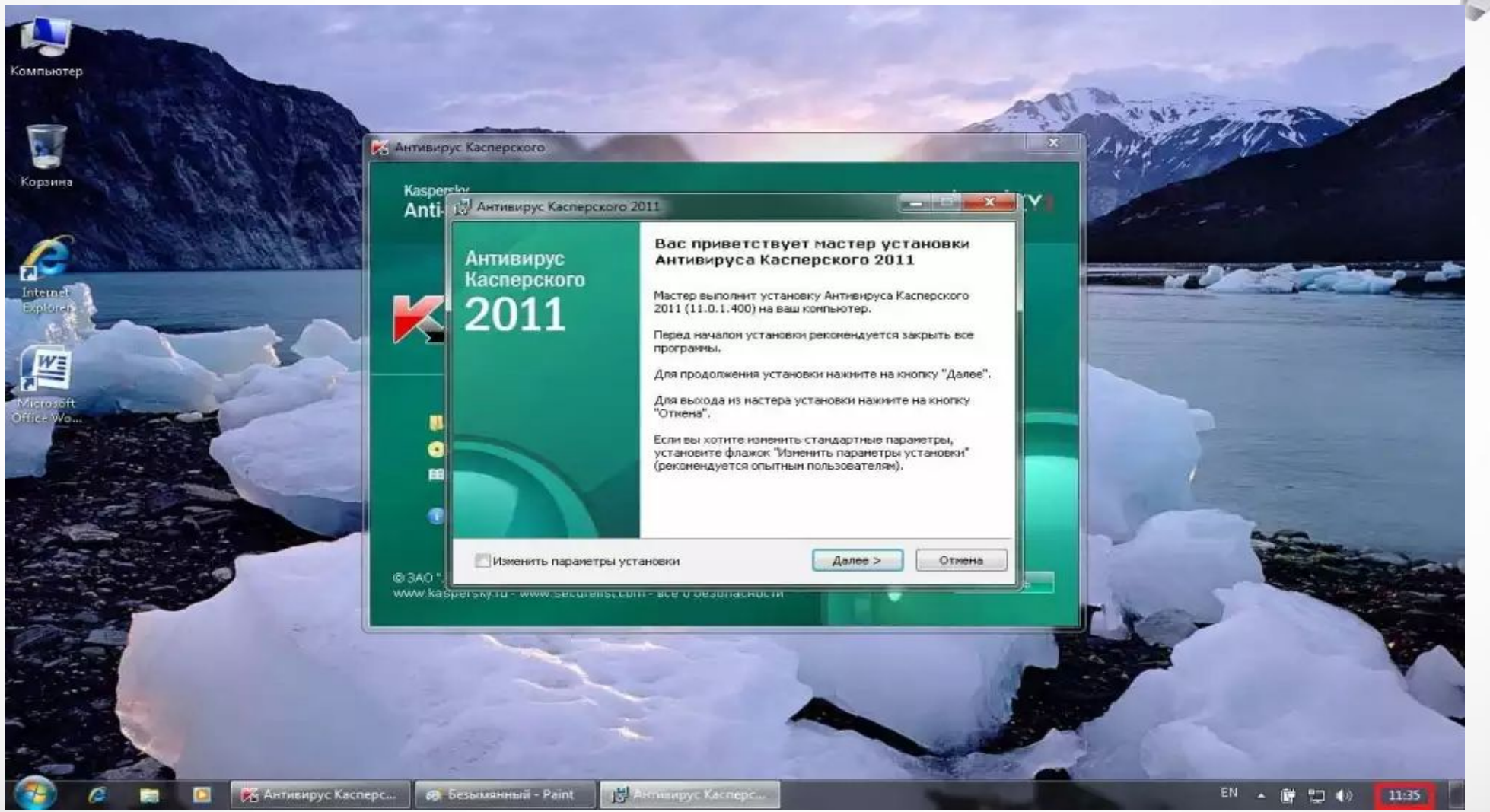
- 1 Шаг по антивирусной защите – установка антивирусного ПО на каждом компьютере в сети и обновление не реже чем ежедневно. Правильная схема обновления антивирусных баз: за обновлениями ходят 1-2 сервера и раздают обновления всем компьютерам в сети. Обязательно ставьте пароль на отключение защиты.
- 2 Шаг. Политика паролей. Вирусы (трояны) умеют заражать компьютеры в сети подбирая пароли к стандартным учетным записям: root, admin, Administrator, Администратор. Всегда используйте сложные пароли! За учетные записи без паролей либо с простыми паролями системный администратор должен быть уволен с соответствующей записью в трудовой книжке. После 10 попыток неверного ввода пароля учетная запись должна блокироваться на 5 минут, чтобы защититься от брут-форса (подбор пароля методом простого перебора). Встроенные учетные записи администраторов крайне желательно переименовать и заблокировать. Периодически пароли нужно менять.
- 3 Шаг. Ограничение прав пользователей. Вирус (троян) распространяется по сети от имени пользователя, который его запустил. Если у пользователя права ограничены: нет доступа на другие компьютеры, нет административных прав на свой компьютер, то даже запущенный вирус ничего не сможет заразить. Нередки случаи, когда сами системные администраторы становятся виновниками распространения вируса: запустили админ кей-ген и пошел вирус заражать все компьютеры в сети…
- 4 Шаг. Регулярная установка обновлений безопасности. Это сложная работа, но делать ее надо. Обновлять нужно не только ОС, но и все приложения: СУБД, почтовые серверы.
- 5 Шаг. Ограничение путей проникновения вирусов. Вирусы попадают в локальную сеть предприятия двумя путями: через сменные носители и через другие сети (Интернет). Запретив доступ к USB, CD-DVD, вы полностью перекрываете 1 путь. Ограничив доступ в Интернет, вы перекрываете 2 путь. Этот метод очень эффективен, но тяжело реализуем.

- 6 Шаг. Межсетевые экраны (МСЭ), они же файерволы (firewalls), они же брэндмауэры. Их нужно обязательно устанавливать на границах сети. Если ваш компьютер подключен к Интернет напрямую, то МСЭ должен быть включен обязательно. Если компьютер подключен только к локальной сети (ЛВС) и выходит в Интернет и другие сети через серверы, то на этом компьютере МСЭ включать необязательно.
- 7 Шаг. Разделение сети предприятия на подсети. Сеть удобно разбивать по принципу: один отдел в одной подсети, другой отдел – в другой. На подсети можно делить на физическом уровне (СКС), на канальном уровне (VLAN), на сетевом уровне (не пересекаемые по адресам ip подсети).
- 8 Шаг. В Windows есть замечательный инструмент по управлению безопасностью больших групп компьютеров – это групповые политики (ГПО). Через ГПО можно настроить компьютеры и серверы так, что заражение и распространение вредоносного ПО станет практически невозможным.
- 9 Шаг. Терминальный доступ. Поднимите в сети 1-2 терминальных сервера, через которые пользователи будут ходить в Интернет и вероятность заражения их персональных компьютеров упадет до нуля.
- 10 Шаг. Отслеживание всех запускаемых на компьютерах и серверах процессов и служб. Можно сделать так, чтобы при запуске неизвестного процесса (службы) системному администратору приходило уведомление. Коммерческое ПО, которое умеет это делать, стоит немало, но в некоторых случаях затраты оправданы.

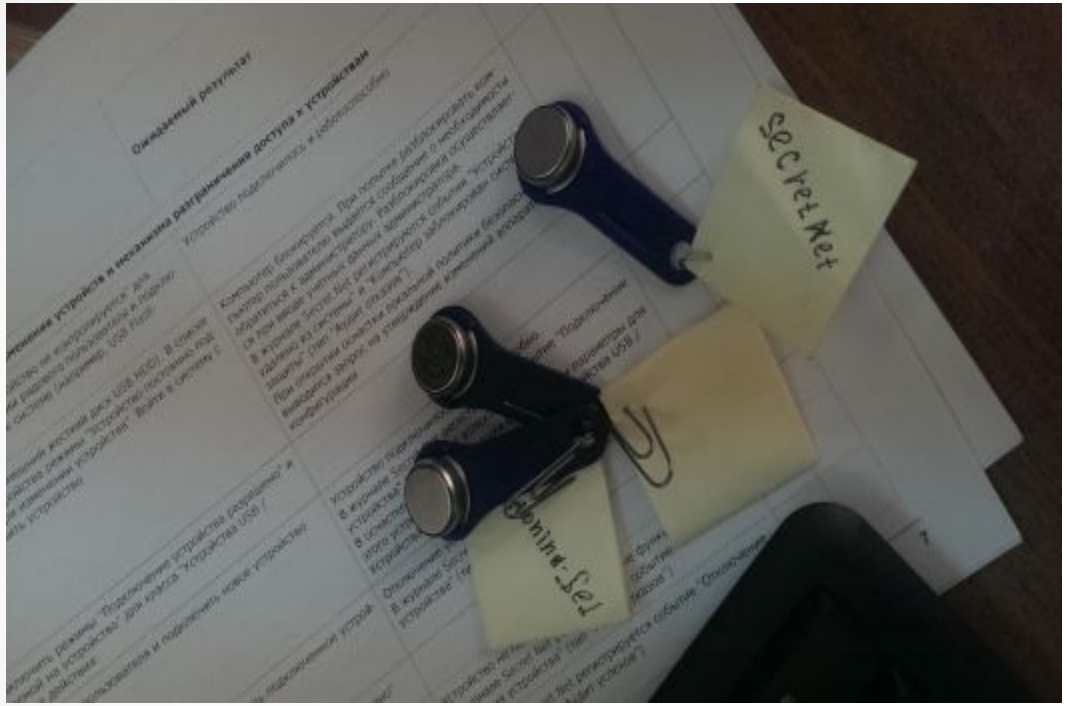
Общая структура антивирусной защиты локальной сети.



Оказание помощи в установке антивирусной защиты информационной сети



Обеспечение устойчивой работы компьютерных систем и комплексов



Перечень инструкций, необходимых для организации рабочего места наладчика компьютерных систем или наладчика аппаратно-программных систем.

Назначение ключей Ibutton на объекте, для входа в систему.

- Все ключи, которые внешне выглядят как металлические дисковые батарейки, в обязательном порядке имеют внутри микросхему-ПЗУ с уникальной для каждого устройства двоичной 48-разрядной кодовой комбинацией (идентификационным номером), а считывается эта комбинация при прикасании металлическим корпусом ключа к металлическому же зонду-считывателю.
- Все электронные ключи-идентификаторы iButton внешне похожи на дисковую металлическую батарейку. Металл представляет собой нержавеющую сталь. Диаметр диска около 17 мм, толщина 3,1 мм или 5,89 мм. Диск состоит из двух электрически разъединенных половинок.
- Внутри он полый. В герметичную полость заключена электронная схема на кремниевом кристалле. Выход схемы соединен с половинками диска двумя проводниками. Половинки диска образуют контактную часть однопроводного последовательного порта. При этом через центральную часть идет линия данных, внешняя оболочка - земля. Для того чтобы произошел обмен информации iButton с внешними устройствами, необходимо прикоснутся обеими поверхностями половинок металлического диска к контактному устройству (зонду), также состоящему из двух электрически не связанных, проводящих электрический ток частей.

Перечень инструкций, необходимых для организации рабочего места наладчика компьютерных систем или наладчика аппаратно-программных систем

- Наладчик аппаратного и программного обеспечения – специалист, управляющий работой ЭВМ и настраивающий определённый виды оборудования, связанного с компьютерной техникой и информационным обеспечением. Областью деятельности данной профессии является установка, обслуживание и модернизация средств вычислительной техники, в том числе аппаратного и программного обеспечения персональных компьютеров, серверов, а также периферийных устройств, оборудования и компьютерной оргтехники.

Основные виды работ (трудовые действия)

– обслуживание аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования, компьютерной оргтехники;

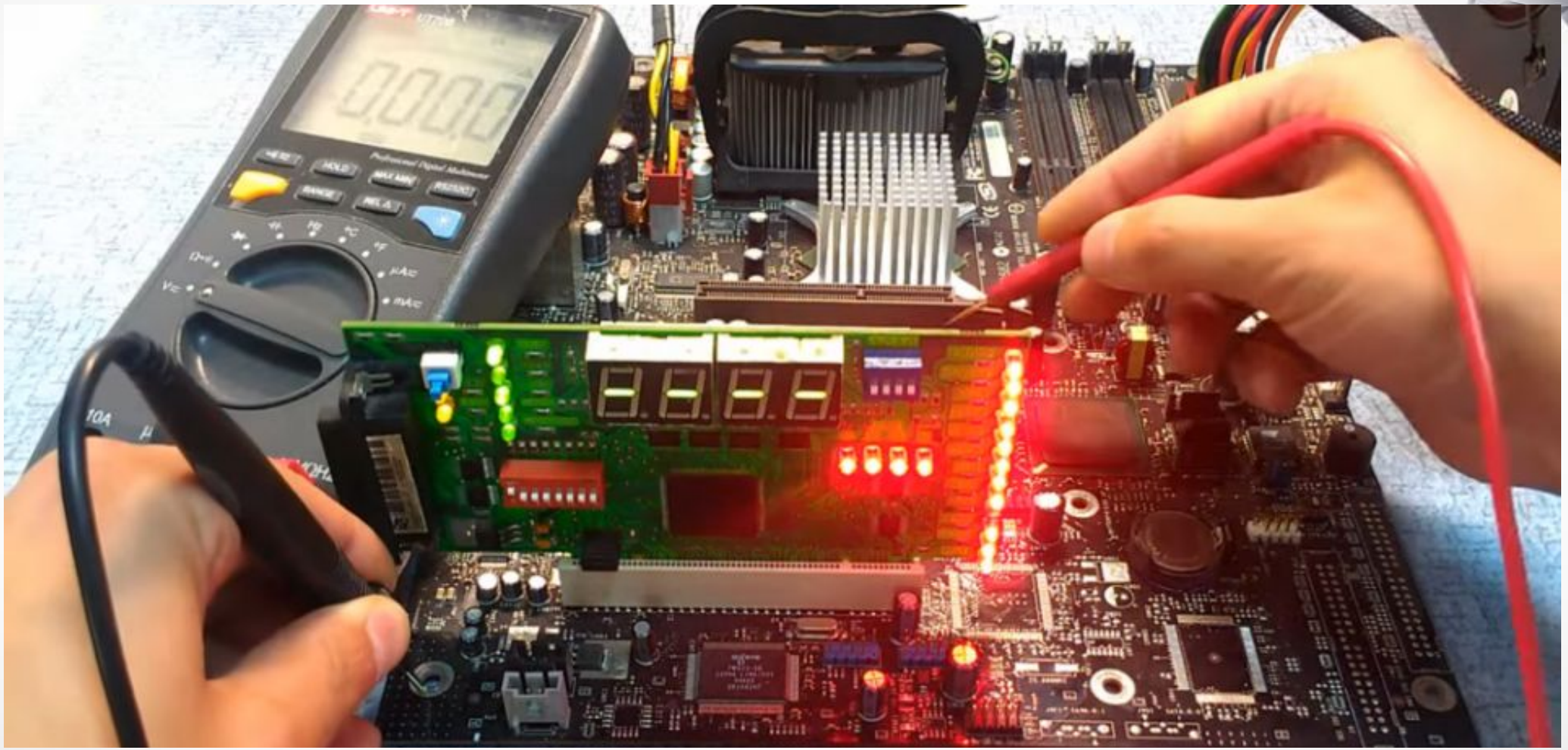
– установка и обслуживание программного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования;

– модернизация аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования;

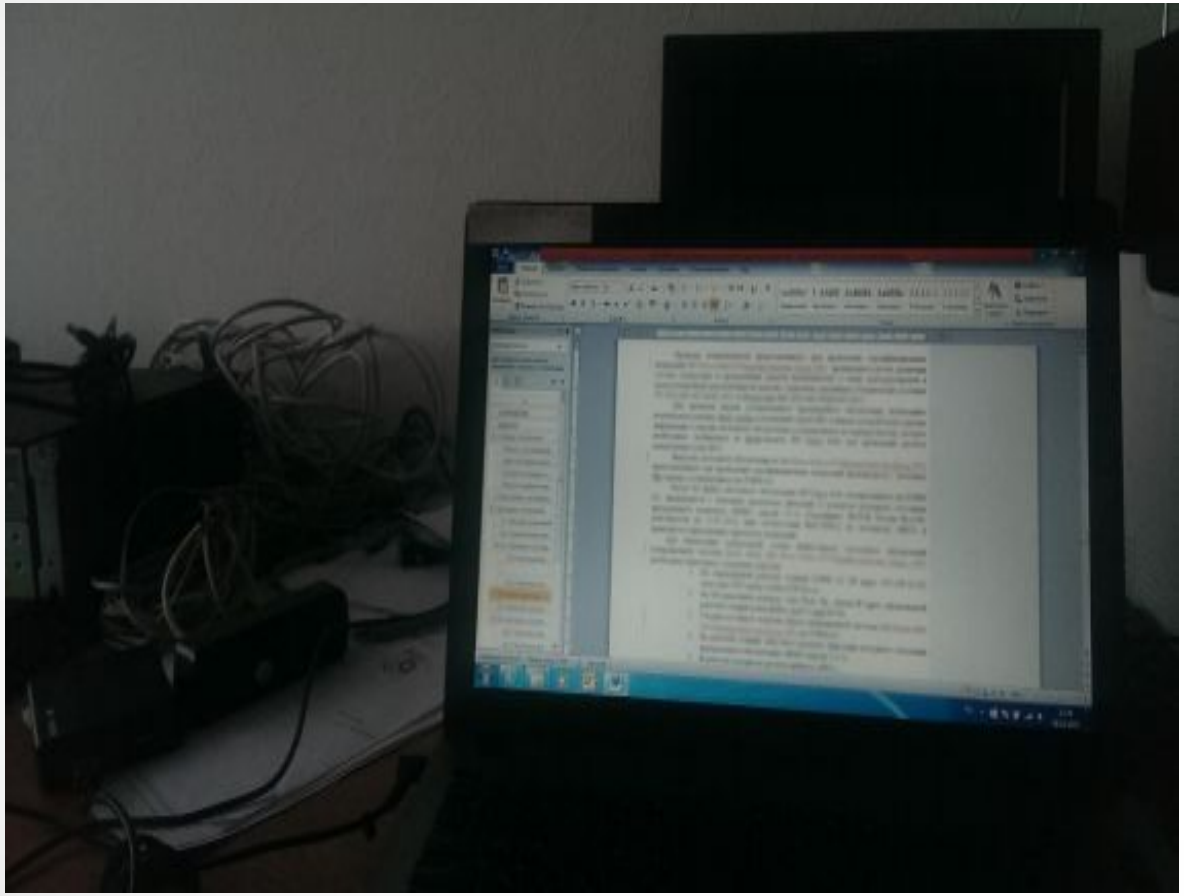
– модернизация программного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования.

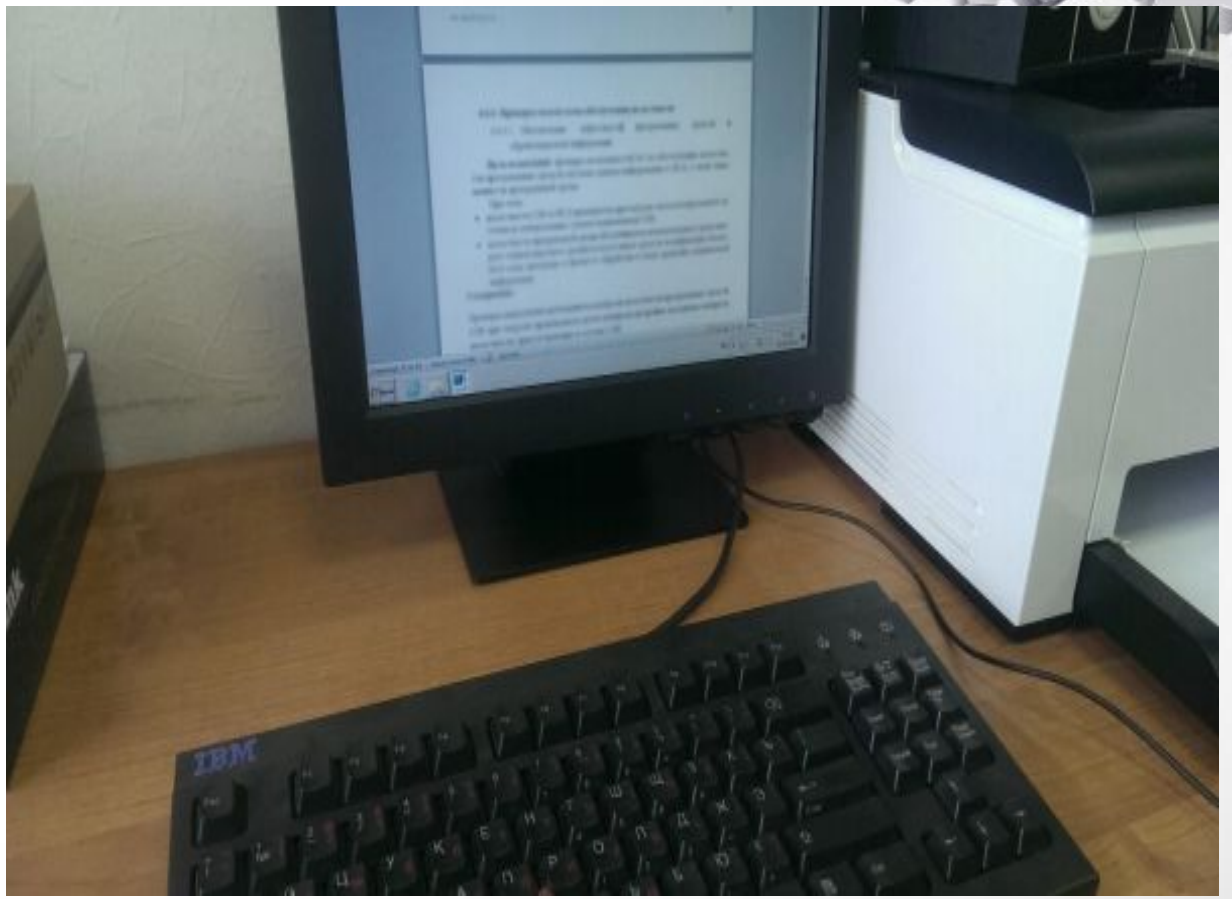
Профилактическое обслуживание аппаратной части компьютера

Диагностика неисправности компьютера

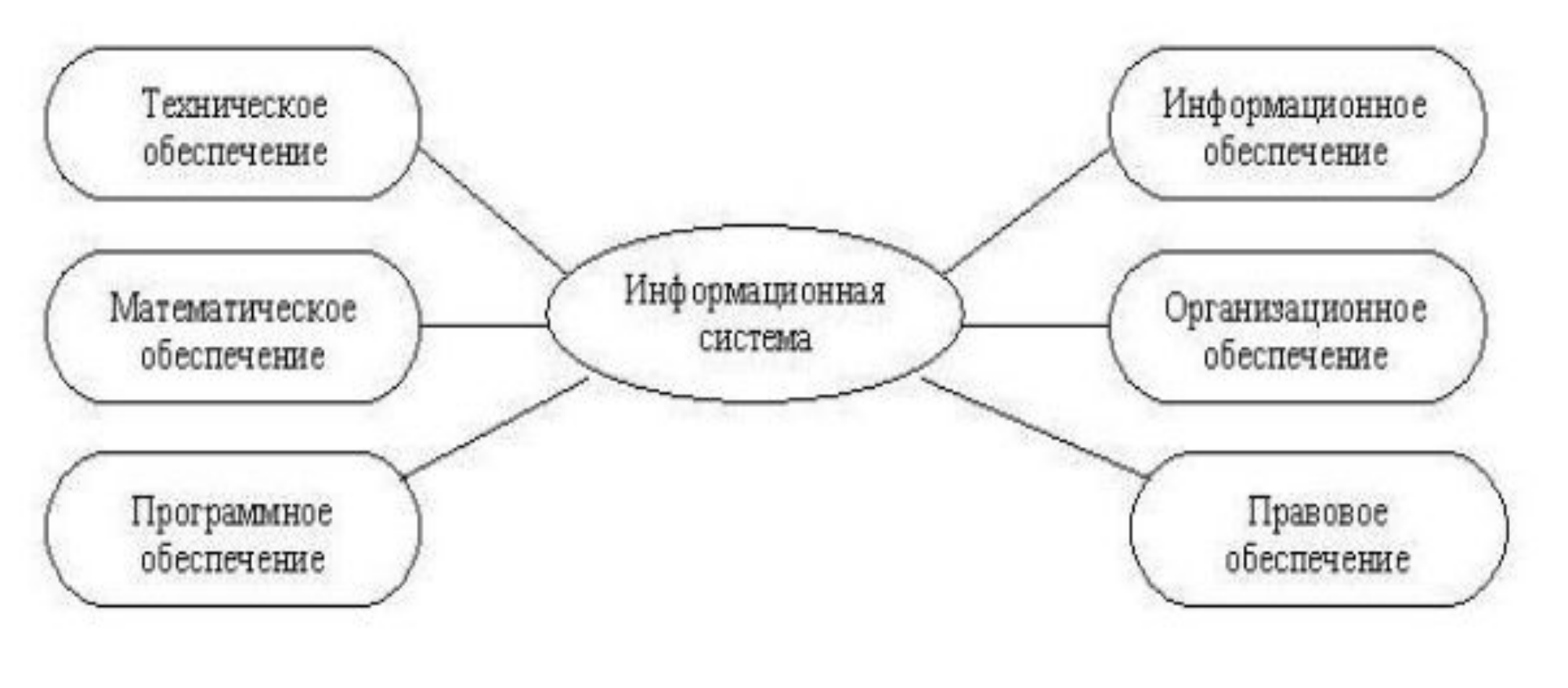


Работа с документами к аттестационным испытаниям и программами испытаний.



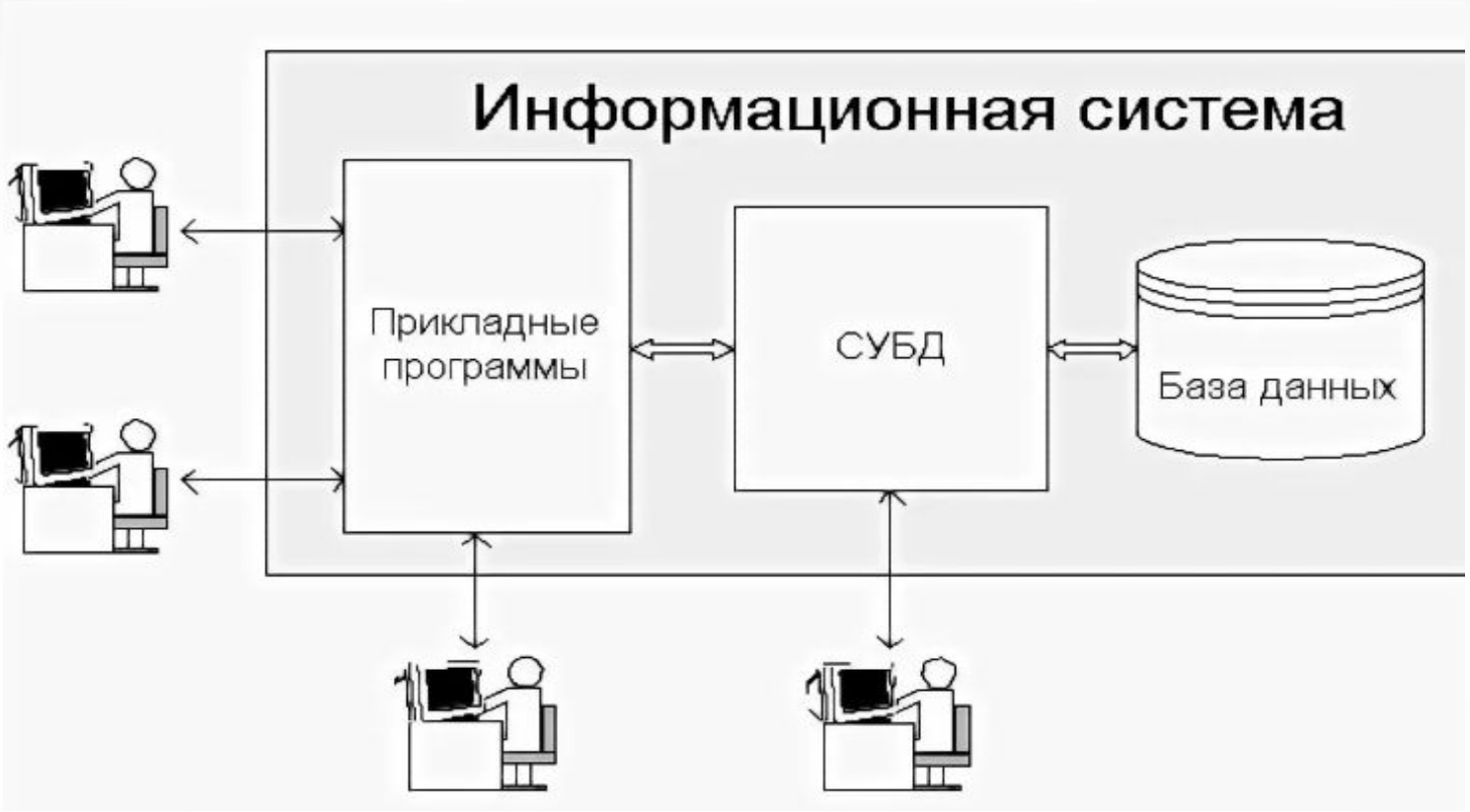


Описание информационной системы, используемой в организации



Структура ИС по типу обеспечивающих подсистем

Описание СУБД



СУБД — это программная система, поддерживающая наполнение и манипулирование данными, представляющими интерес для пользователей при решении прикладных задач. Иными словами, СУБД является интерфейсом между базой данных и прикладными задачами. Функции: опередление данных, обработка данных, усправление данными. Пример: Oracle Database, MySQL, PostgreSQL, ACCESS.

Организация доступа пользователей информационной системы в рамках своей компетенции. Описание средств, приемов защиты информации при работе с информационной системой

- Основным видом информационных угроз, для защиты от которых на каждом предприятии создается целая технология, является несанкционированный доступ злоумышленников к данным. Злоумышленники планируют заранее преступные действия, которые могут осуществляться путем прямого доступа к устройствам или путем удаленной атаки с использованием специально разработанных для кражи информации программ.

- **Маскировка** – способы защиты информации, предусматривающие преобразование данных в форму, не пригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа.
- **Управление** – способы защиты информации, при которых осуществляется управление над всеми компонентами информационной системы.
- **Регламентация** – важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.
- **Принуждение** – методы защиты информации, тесно связанные с регламентацией, предполагающие введение комплекса мер, при которых работники вынуждены выполнять установленные правила. Если используются способы воздействия на работников, при которых они выполняют инструкции по этическим и личностным соображениям, то речь идет о побуждении.

Средства защиты информационных систем

Способы защиты информации предполагают использование определенного набора средств. Для предотвращения потери и утечки секретных сведений используются следующие средства:

- Физические;
- Программные и аппаратные;
- Организационные;
- Законодательные;
- Психологические.

Физические средства защиты информации предотвращают доступ посторонних лиц на охраняемую территорию. Основным и наиболее старым средством физического препятствия является установка прочных дверей, надежных замков, решеток на окна. Для усиления защиты информации используются пропускные пункты, на которых контроль доступа осуществляют люди (охранники) или специальные системы. С целью предотвращения потерь информации также целесообразна установка противопожарной системы. Физические средства используются для охраны данных как на бумажных, так и на электронных носителях.

Аппаратные средства представлены устройствами, которые встраиваются в аппаратуру для обработки информации. **Программные** средства – программы, отражающие хакерские атаки. Также к программным средствам можно отнести программные комплексы, выполняющие восстановление утраченных сведений. При помощи комплекса аппаратуры и программ обеспечивается резервное копирование информации – для предотвращения потерь.

- **Организационные** средства сопряжены с несколькими методами защиты: регламентацией, управлением, принуждением. К организационным средствам относится разработка должностных инструкций, беседы с работниками, комплекс мер наказания и поощрения. При эффективном использовании организационных средств работники предприятия хорошо осведомлены о технологии работы с охраняемыми сведениями, четко выполняют свои обязанности и несут ответственность за предоставление недостоверной информации, утечку или потерю данных.
- **Законодательные** средства – комплекс нормативно-правовых актов, регулирующих деятельность людей, имеющих доступ к охраняемым сведениям и определяющих меру ответственности за утрату или кражу секретной информации.
- **Психологические** средства – комплекс мер для создания личной заинтересованности работников в сохранности и подлинности информации. Для создания личной заинтересованности персонала руководители используют разные виды поощрений. К психологическим средствам относится и построение корпоративной культуры, при которой каждый работник чувствует себя важной частью системы и заинтересован в успехе предприятия.


Способы защиты информации
Средства защиты информации
Управление
Препятствие
Маскировка информации
Регламентация
Принуждение
Побуждение
Формальные
Физические
Технические
Аппаратные
Программные
Организационные
Законодательные
Морально-этические
Неформальные

Заключение

- Я прошла практику по профессиональному модулю ПМ.01«Эксплуатация и модификация информационных систем». Во время нее я использовала информационно-коммуникационные технологии для совершенствования профессиональной деятельности, собирала данные для анализа использования и функционирования ИС, участвовала в составлении отчетной документации, принимала участие в разработке проектной документации на модификацию ИС, провела контроль, диагностику и восстановление работоспособности компьютерных систем и комплексов.