## Процедура внедрения ПО Dr.Web

1. **Назначение ответственного за проведение тестирования ПО Dr.Web.**
   1. Изучение возможностей ПО Dr.Web в ходе тестовых установок систем защиты рабочих станций, файловых серверов, почтовых серверов, а также серверов управления антивирусной защитой.
   2. Проверка действия политик безопасности, сформированных в соответствии с политикой информационной безопасности компании.
   3. Проверка совместимости ПО Dr.Web и ПО, используемого в компании.
   4. Уточнение плана развертывания ПО Dr.Web по итогам тестовых установок в соответствии со структурой корпоративной сети компании и графиком работы сотрудников.
      1. Уточнение времени развертывания компонентов ПО Dr.Web в условиях локальной сети компании.
      2. Выбор типа развертывания ПО Dr.Web на локальных станциях и файловых серверах (политика AD, запуск дистрибутивов локально, сканирование сети на незащищенные станции и пр.).
      3. Выбор порядка и времени развертывания ПО Dr.Web в соответствии со структурой корпоративной сети компании и графиком работы сотрудников.
   5. Обучение администраторов безопасности компании приемам работы с ПО Dr.Web.
   6. Отработка процедур, связанных с удалением используемого антивирусного ПО и установкой ПО Dr.Web.
      1. Выработка мер защиты на период отсутствия антивирусного ПО на элементах сети компании.
   7. Проверка локальной сети (защищаемых станций и серверов) на наличие сервисов, необходимых для развертывания ПО Dr.Web в сети компании, — в зависимости от выбранного типа развертывания. В случае необходимости корректировка правил файерволов, используемых в сети компании.
   8. Утверждение плана-графика развертывания ПО Dr.Web в сети компании. Доведение плана-графика до сотрудников компании в части, их касающейся. Общая схема инсталляции антивируса в сети предприятия представлена на рис. 1.

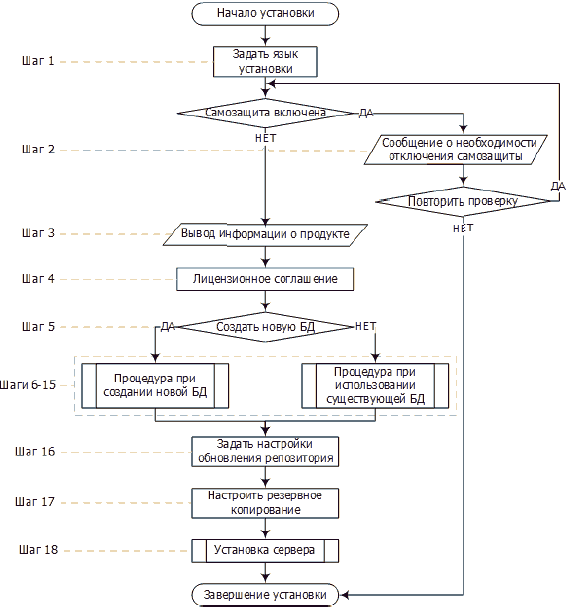


Рис. 1. План-график развертывания ПО Dr.Web в сети компании

1. **Замена антивирусного ПО в сети компании.**
   1. Подготовка ПО Dr.Web. в зависимости от выбранного типа развертывания.
      1. Установка серверов иерархической сети Dr.Web, а также, в случае необходимости, необходимой базы данных (рис. 2).

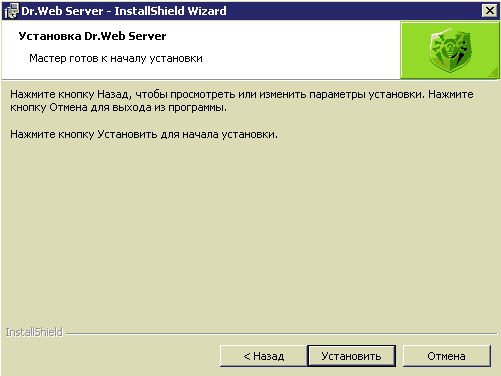


Рис. 2. Установка серверов

* + 1. Развертывание системы резервирования серверов Dr.Web (рис. 3).

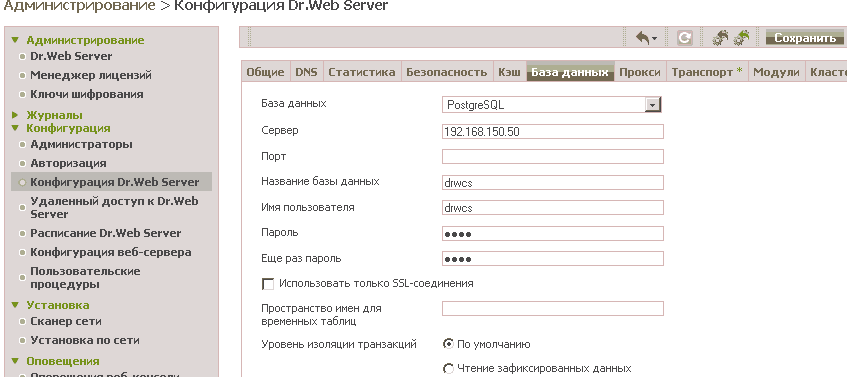


Рис. 3. Развертывание системы резервирования серверов Dr.Web

* + 1. Настройка групп и политик.
    2. В случае необходимости — назначение отдельных администраторов группы пользователей и ограничение прав данных администраторов в соответствии с политикой, действующей в компании.
    3. В зависимости от выбранной политики развертывания — проведение иных мероприятий.
  1. Сканирование сети компании сетевой утилитой Dr.Web CureNet! на наличие ранее неизвестных вредоносных программ (рис. 4).

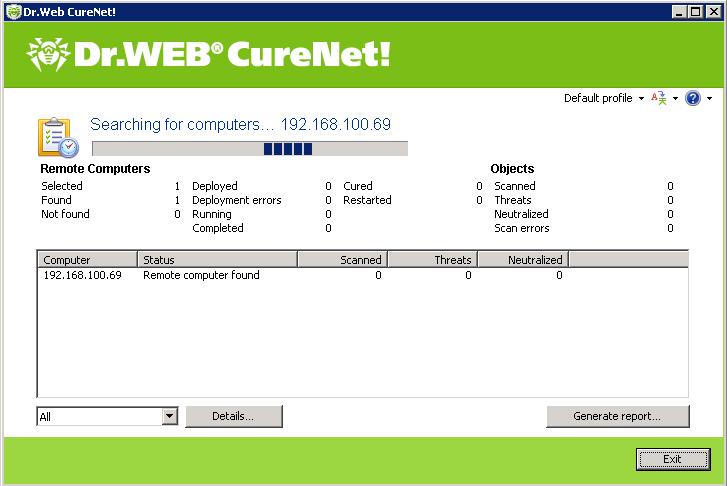
****

Рис. 4. Проверка сети компании утилитой Dr.Web CureNet!

* 1. Деинсталляция используемых антивирусных продуктов.
  2. Развертывание антивирусной сети Dr.Web Enterprise Security Suite (рис. 5).

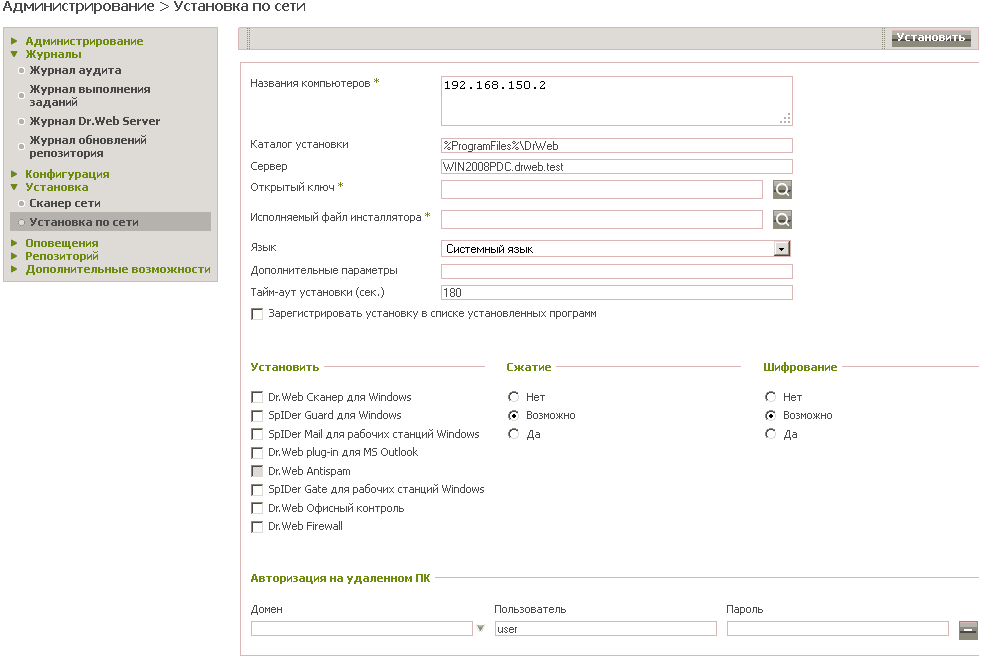


Рис. 5. Развертывание антивирусной сети

* + 1. Установка системы защиты рабочих станций и файловых серверов в соответствии с настройками, сделанными на предыдущем этапе.
    2. Установка системы защиты почтовых серверов.

1. **Эксплуатация ПО Dr.Web в течение тестового периода.** 
   1. Проведение обновлений ПО Dr.Web в соответствии с политикой, действующей в ОАО компании.
   2. Проведение периодических проверок защищаемых рабочих станций, файловых и почтовых серверов (рис. 6).

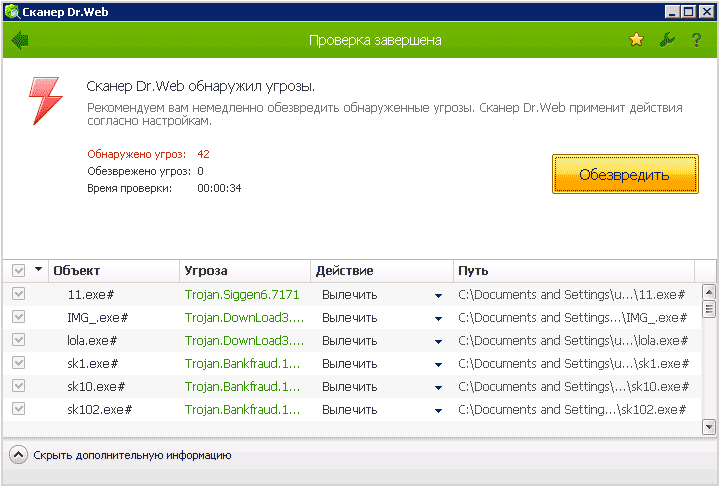


Рис. 6. Периодическая проверка защищаемых рабочих станций, файловых и почтовых серверов

* 1. Контроль действий ПО Dr.Web на тестовые воздействия вредоносного ПО.
  2. Проверка процедуры взаимодействия с технической поддержкой ООО «Доктор Веб».

1. **Подготовка отчета по результатам тестирования ПО Dr.Web в сети компании, согласование отчета с представителями ООО «Доктор Веб». Утверждение отчета.**