ESET
Remote Administrator 4

Инструкция по установке и руководство пользователя

ESET Remote Administrator 4

Международная служба поддержки: www.eset.eu/support
Служба поддержки в Северной Америке: www.eset.com/support

Версия 3. 11. 2010

Содержание

1. Введение

ESET Remote Administrator (ERA) — это приложение, которое позволяет централизованно управлять продуктами компании ESET в сети, состоящей из рабочих станций и серверов. С помощью встроенного в ESET Remote Administrator диспетчера задач можно устанавливать продукты безопасности ESET на удаленных компьютерах и быстро реагировать на новые проблемы и угрозы.

Сам по себе ESET Remote Administrator не обеспечивает никакой другой защиты от злонамеренного кода. Работа ERA зависит от присутствия на рабочих станциях или серверах продуктов ESET для обеспечения безопасности, таких как ESET NOD32 Antivirus или ESET Smart Security.
Для полного развертывания пакета продуктов безопасности ESET необходимо выполнить указанные ниже действия.

- Установка сервера ERA Server (ERAS),
- Установка консоли ERA Console (ERAC),
- Установка на клиентские компьютеры (ESET NOD32 Antivirus, ESET Smart Security, клиент ESET Security для Linux и др.).

Примечание. В некоторых разделах этого документа используются системные переменные, которые описывают точные размещение папок и файлов:

%ProgramFiles% = обычно в *C:\Program Files*
%ALLUSERSPROFILE% = обычно в *C:\Documents and Settings\All Users*

1.1 Что нового?

ESET Remote Administrator версия 4.0

- поддержка ESET Smart Security/ESET NOD32 Antivirus 4.2
- поддержка ESET Mail Security 4 for Microsoft Exchange Server
- поддержка решения безопасности для ПК с Linux/Mac (ESET NOD32 Antivirus 4)
- поддержка ESET Mobile Security

Новые возможности
- удаленная установка: новый дизайн;
- управление группами: новый дизайн (статические группы, параметрические группы, улучшенная синхронизация с Active Directory);
- фильтр: улучшенная функциональность (фильтры политик, фильтры статических и параметрических групп);
- политики: новые параметры в правилах политик (поддержка параметрических групп), импорт и экспорт политик и правил политики, объединение задач планировщика, мастер правил политик;
- уведомления: поддержка параметрических групп, несколько незначительных улучшений;
- централизованное представление карантина клиентов (для клиентов ESS/EAV версии 4 и выше);
- отчеты: поддержка статических и параметрических групп, новые типы отчетов (мобильный журнал, карантин, файервол), новые шаблоны;
- мастер объединения правил файервола: мастер для объединения правил, созданных в режиме обучения;
- проверка подлинности Windows/домен для пользователей ERA Console;
- поддержка пассивного кластера Windows;
- поддержка переустановки ERA старых версий (3.x, 2.x, 1.x), включая перенос данных;
- зашифрованная передача данных посредством AES-256.

Новый ESET Configuration Editor
- поддержка новых продуктов безопасности ESET;
- поддержка новых функций ERA Server;
- файлы лицензий в ZIP-архиве;
- возможность добавления преопределенных задач планировщика.

ESET Remote Administrator версия 3.0

- поддержка продуктов безопасности ESET версии 4.x;
- поддержка решений на базе Linux.

Новые возможности
- управление политиками;
- диспетчер уведомлений;
- доступ к консоли в режиме только для чтения;
- поддержка ESET SysInspector;
- улучшена масштабируемость при передаче данных;
- удаление реплицированных клиентов;
- объединение ключей лицензий (диспетчер лицензий);
- зеркало для ESET NOD32 Antivirus 2.x;
- новая программа установки;
- в функцию поиска незарегистрированных компьютеров добавлен параметр фильтрации по домену;
- сжатие файлов журнала сервера (.zip);
- исправлены незначительные ошибки и добавлено несколько дополнительных возможностей;
- компакт-диск аварийного восстановления.

Внутренние усовершенствования сервера
- поддержка дополнительных СУБД (MS Access, MS SQL Server, Oracle, MySQL).

Новый ESET Configuration Editor
- поддержка продуктов безопасности ESET версии 4.x.

ESET Remote Administrator версия 2.0

- поддержка новых продуктов безопасности ESET версии 3 (ESET Smart Security, ESET NOD32 Antivirus);
- новые журналы (новые столбцы, журналы персонального файервола ESET);
- новые сведения о состоянии клиента с продуктами безопасности версии 3 (состояние защиты, свойства защиты, сведения о системе);
- задачи (конфигурация, обновление, сканирование по требованию, интерактивные задачи);
- поддержка продуктов NOD32 версии 2.

Новые возможности
- улучшена идентификация клиентов (добавлен MAC-адрес);
- улучшена удаленная установка (поддержка MSI-файлов и пользовательских пакетов);
- усовершенствования в защите (возможность шифрования для всех новых клиентов сервера);
- повышение производительности (сжатие в протоколе обмена данными);
- добавлена возможность отправки данных системы своевременного обнаружения ThreatSense.Netчерез сервер ERA Server;
- улучшен графический интерфейс пользователя (новые графические возможности, дополнительные цвета для обозначения состояния, расширенные фильтры, диалоговые окна изменяемого размера);
- новый шаблон для отчетов (схема ESS);
- мониторинг производительности сервера (данные, запросы);
- возможности обновления на сервере ERA Server (обновление важной информации);
- использование зеркала на сервере ERA Server;
- усовершенствована удаленная установка (поддержка MSI-файлов и пользовательских пакетов, удаленная установка ERA, диагностика).

Внутренние усовершенствования сервера
- новые возможности репликации (приоритет репликации, улучшенная многоуровневая репликация);
- новая структура базы данных;
- новая структура папок;
- улучшена внутренняя безопасность.

Новый ESET Configuration Editor
- поддержка продуктов безопасности ESET версий 2 и 3;
- возможность настраивать сервер ERA Server;
- другие менее существенные новые возможности (поиск, пользовательские параметры).

Новая программа установки (MSI)
- перенос баз данных из предыдущих версий.

Новая документация (справка, руководство)

1.2 Архитектура программы

Технически программа ESET Remote Administrator состоит из двух отдельных компонентов: ERA Server (ERAS) и ERA Console (ERAC). В сети можно запускать неограниченное число экземпляров ERA Server и консолей ERA, так как в лицензионном соглашении на их использование нет никаких ограничений. Единственным ограничением является общее число клиентов, которыми может управлять установленное средство ERA.

ERA Server (ERAS)

Серверный компонент ERA запускается как служба в следующих операционных системах на базе Microsoft Windows® NT: NT4 с пакетом обновления 6 (SP6), 2000, XP, 2003, Vista, 7 и 2008. Основной задачей этой службы является сбор сведений на клиентах и отправка им различных запросов. Эти запросы, к числу которых относятся задачи настройки, запросы удаленной установки и т. д., создаются с помощью консоли ERA Console (ERAC). ERAS — это промежуточная точка между ERAC и клиентскими компьютерами, место, в котором выполняется обработка, сохранение или изменение всех сведений перед их передачей клиентам или консоли ERAC.

ERA Console (ERAC)

ERAC — это клиентский компонент ERA, который обычно устанавливается на рабочей станции. Администратор с помощью этой рабочей станции удаленно управляет решениями ESET, установленными на отдельных компьютерах-клиентах. С помощью консоли ERAC администратор может подключаться к серверу ERA по TCP-порту 2223. Обмен данными управляется процессом console.exe, который обычно находится в следующем каталоге:

%ProgramFiles%\ESET\ESET Remote Administrator\Console

При установке консоли ERAC может понадобиться ввести имя сервера ERAS. После запуска консоль будет автоматически подключаться к этому серверу. Консоль ERAC можно также настроить после установки.

2. Установка сервера ERA Server и консоли ERA Console

2.1 Требования

Сервер ERAS работает как служба, поэтому для его работы необходим компьютер, на котором установлена одна из операционных систем на базе Microsoft Windows NT (NT4 SP6, 2000, XP, 2003, Vista, 7 или 2008). Хотя для работы сервера ERAS наличие версий операционной системы Microsoft Windows Server не обязательно, для надежной работы сервер ERAS рекомендуется устанавливать на серверные операционные системы. Компьютер, на котором установлена служба ERAS, должен быть постоянно подключен к сети и доступен для:

- клиентов (обычно рабочих станций);
- компьютеров с консолью ERA Console;
- других экземпляров сервера ERAS (в случае репликации).

Примечание. ESET Remote Administrator 4 полностью поддерживает установку поверх старых версий (3.x, 2.x, 1.x), включая перенос данных.

2.1.1 Требования к программному обеспечению

ERA Server

32-разрядные операционные системы:	Windows NT4 с пакетом обновления 6 (SP6) и более поздние
64-разрядные операционные системы:	Windows XP и более поздние
Базы данных:	Microsoft Access (встроенная) Microsoft SQL Server 2005 или более поздней версии MySQL 5.0 или более поздней версии ORACLE 9i или более поздней версии
Установщик Windows:	2.0

ERA Console

32-разрядные операционные системы:	Windows 2000 и более поздние
64-разрядные операционные системы:	Windows XP и более поздние
Установщик Windows:	2.0
Internet Explorer:	рекомендуется версия 6.0, минимальная — 4.0 (некоторые отчеты могут отображаться неверно)

2.1.2 Требования к быстродействию

Производительность сервера может меняться в зависимости от указанных ниже параметров.

1. **Используемая база данных**
   - База данных MS Access устанавливается по умолчанию с сервером. Это решение рекомендуется при обслуживании сотен клиентов. Однако размер базы данных ограничен 2 гигабайтами. Следовательно, потребуется активировать очистку на сервере и задать интервал (в меню **«Служебные программы»** > **«Настройки сервера»** > **«Обслуживание сервера»**) для удаления устаревших данных.
   - Другие базы данных (MySQL, MSSQL, ORACLE) нужно устанавливать отдельно, но они могут повысить быстродействие сервера. Важно использовать подходящие оборудования для каждого ядра СУБД (в основном для ORACLE) в соответствии с техническими рекомендациями его поставщика.
   - Если в качестве базы данных выбрана ORACLE, необходимо установить количество курсоров, превышающее значение **«Максимальное количество активных подключения»** (меню **«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные настройки»** > **«Дополнительно»**; значение по умолчанию — 500). Окончательное число курсоров должно учитывать количество серверов нижнего уровня (если используется репликации) и курсоры, которые используются другими приложениями для доступа к ядру СУБД.
   - Как правило, быстродействие сервера выше при использовании внешних баз данных (то есть установленных на другом физическом компьютере).

2. Интервал подключения клиентов

- В ESET Smart Security / ESET NOD32 Antivirus версии 4.2 и выше интервал подключения клиента по умолчанию равняется 10 минутам. Если состояние клиентов необходимо обновлять чаще или реже, чем установлено по умолчанию, значение интервала можно изменить. Следует учесть, что уменьшенный интервал подключения клиента повлияет на производительность сервера.

3. Среднее число событий, сообщаемое клиентами за одно подключение

- Любые данные, отправленные клиентом серверу, перечисляются в определенном событии (например, журнал угроз, журнал событий, журнал сканирования, изменение конфигурации). Этот параметр нельзя изменить напрямую, но на него его можно повлиять при изменении других связанных с ним параметров. Например в дополнительной конфигурации сервера (в меню **«Служебные программы»** > **«Настройки сервера»** > **«Обслуживание сервера»**) можно настроить максимальный размер журналов, принимаемых сервером (этот параметр включает клиентов, которые подключаются напрямую, а также реплицированных клиентов). Для периодических операций среднее значение за долгий период можно оценить под одному событию за каждые 4 часа для каждого клиента.

4. Используемое оборудование и операционная система

- Настоятельно рекомендуется использовать минимальные рекомендации к оборудованию для операционной системы сервера с учетом количества обслуживаемых клиентов.

Перегрузка

Если сервер перегружен (например, 20 000 клиентов подключается к серверу, который способен обслуживать только 10 000 клиентов с интервалом через каждые 10 минут), это приведет к пропуску некоторых подключенных клиентов. Если интервал подключения клиента настроен на 20 минут вместо 10 минут, в среднем будет обслуживаться только каждое второе подключение клиента. Каждый отказ в обслуживании будет регистрироваться следующим образом: "*<SERVERMGR_WARNING> ServerThread: maximum number of threads for active connections reached (500), the server will skip this connection* (достигнуто максимальное количество потоков для активных подключений (500), сервер пропустит это подключение)". Отказ в обслуживании может также возникнуть при временных перегрузках сервера.
Это значение можно изменить в поле **«Максимальное количество активных подключений»** (по умолчанию — 500) в дополнительных параметрах сервера, однако изменять его рекомендуется только в крайних случаях (например, при решении специфических проблем). При переизбытке системных ресурсов и производительности ядра СУБД этот параметр можно использовать для настройки общей производительности сервера.

Передача данных по сети

В штатном режиме работы сервера подразумевается, что клиент, подключающийся каждые 10 минут, за одно подключение будет сообщать о 0,04 события, что составляет 1 сообщение о событии каждые 4 часа для каждого клиента. При этом создается примерно 2 килобайта трафика на подключение.
При появлении вируса у клиента, который сообщает о 7 событиях при каждом подключении, трафик может возрасти до 240 килобайт на подключение. Если включено сжатие (по умолчанию), размер передаваемых данных будет примерно на 50% меньше, то есть примерно 120 килобайт на подключение.
Данные включают в себя прямые подключения клиента без учета реплицированных подключений. Репликация происходит гораздо реже и предназначена для отправки новых событий с подчиненных серверов. События автоматически реплицируются и уровень их детализации настраивается в дополнительных параметрах сервера (в меню **«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные настройки»** > **«Репликация»**). В разделе обслуживания сервера можно настроить максимальный уровень детализации журналов, принимаемых сервером верхнего уровня. Этот параметр применяется как к клиентам, подключающимся напрямую, так и к реплицированных клиентам.

Требования к объему хранилища

Для чистой установки продукта с базой данных MS Access требуется до 60 МБ места на диске.
Основная часть хранилища занята событиями клиентов, которые хранятся в базе данных и в репозитории на диске (в каталоге по умолчанию *C:\Documents and Settings\All Users\Application Data\Eset\ESET Remote Administrator\Server*). Для ERA требуется не менее 5% свободного места на диске. В случае превышения этого минимума сервер не будете получать некоторые из клиентских событий. Этот параметр настраивается в меню **«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные настройки»** > **«Дополнительно»** > **«Максимальное использование дискового пространства»**. Для штатной работы с параметрами очистки по умолчанию (удаление событий старше 3 месяцев) требуется около 10 ГБ свободного дискового пространства на 1 000 клиентов/

Конкретный пример

Сервер с базой данных MS Access, к которому клиенты подключаются каждые 5 минут и сообщают о 7 событиях (например, в журнале угроз, журнале событий, журнале сканирования, об изменениях конфигурации и т. д.) за подключение, в среднем может временно обслуживать до 3 000 клиентов. Этот сценарий описывает временную ситуацию перегрузки, например, сообщения о вспышке вируса и т. п.
Если сервер использует внешнюю базу данных MySQL, интервал подключения клиентов установлен в 10 минут (0,02 события на подключение), максимальное число клиентов, которых может обслуживать сервер, увеличивается до 30 000. Этот сценарий демонстрирует оптимальную производительность базы данных, где клиенты сообщают об относительно небольшом числе событий.
В штатном режиме при использовании базы данных MS Access и интервале подключения клиентов в 10 минут сервер в состоянии обслуживать более 10 000 клиентов.

2.1.3 Используемые порты

В приведенной ниже таблице перечислены все возможные сетевые соединения, используемые при установке сервера ERAS. Процесс EHttpSrv.exe принимает данные на TCP-порту 2221, а процесс era.exe — на портах 2222, 2223, 2224 и 2846. Все остальные соединения устанавливаются встроенными процессами операционной системы (например, NetBIOS через TCP/IP).

Протокол	Порт	Описание
TCP	2221 (прием данных сервером ERAS)	Порт по умолчанию, используемый функцией зеркала, встроенной в ERAS (HTTP-версия)
TCP	2222 (прием данных сервером ERAS)	Обмен данными между клиентами и сервером ERAS
TCP	2223 (прием данных сервером ERAS)	Обмен данными между ERAC и ERAS

При использовании всех функций данной программы необходимо открыть перечисленные ниже порты.

Протокол	Порт	Описание
TCP	2224 (прием данных сервером ERAS)	Обмен данными между агентом *einstaller.exe* и ERAS в ходе удаленной установки
TCP	2846 (прием данных сервером ERAS)	Репликация ERAS.
TCP	139 (целевой порт со стороны сервера ERAS)	Копирование агента *einstaller.exe* с ERAS на клиента через ресурс общего доступа admin$
UDP	137 (целевой порт со стороны сервера ERAS)	Разрешение имен в ходе удаленной установки
UDP	138 (целевой порт со стороны сервера ERAS)	Обзор файлов в ходе удаленной установки
TCP	445 (целевой порт со стороны сервера ERAS)	Прямой доступ к общим ресурсам по протоколу TCP/IP в ходе удаленной установки (вместо TCP 139)

Предопределенные порты 2221, 2222, 2223, 2224 и 2846 можно изменить, если они уже используются другими приложениями.

Чтобы изменить порты по умолчанию, используемые ERA, нажмите **«Служебные программы»** > **«Настройки сервера...»**. Чтобы изменить порт 2221, откройте вкладку **«Обновления»** и измените значение параметра **«Порт сервера HTTP»**. Порты 2222, 2223, 2224 и 2846 можно изменить в разделе **«Порты»** на вкладке **«Дополнительно»**.

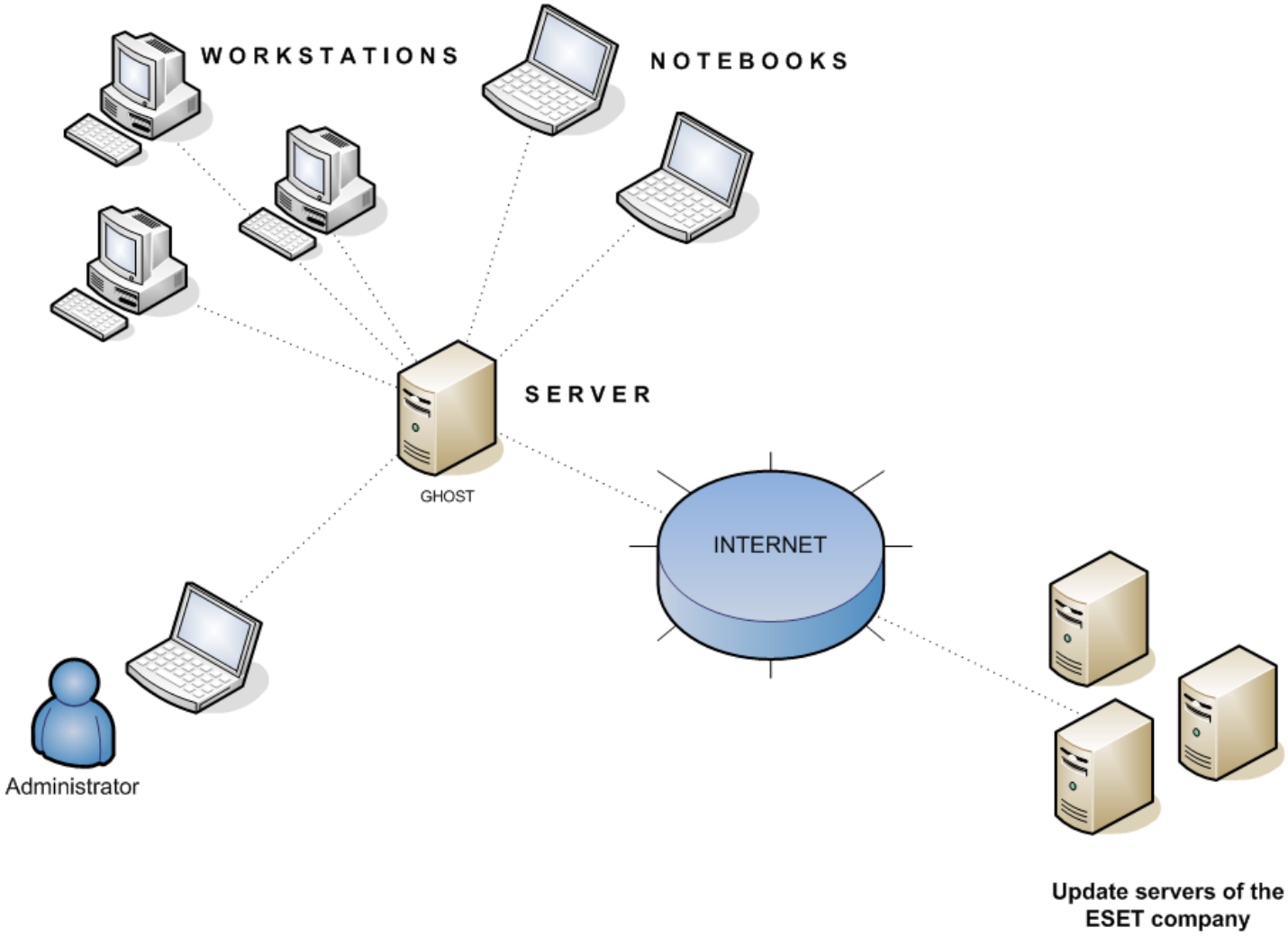
Предопределенные порты 2222, 2223, 2224 и 2846 также можно изменить в расширенном режиме установки (сервер ERAS).

2.2 Основные рекомендации по установке

2.2.1 Обзор среды (структура сети)

Сеть компании обычно представляет собой одну локальную сеть (LAN), поэтому рекомендуется устанавливать сервер ERAS и сервер с зеркалом. Зеркало можно создать либо в ERAS, либо в ESET NOD32 Antivirus Business Edition / ESET Smart Security Business Edition.

Предположим, что все клиенты являются рабочими станциями и ноутбуками под управлением Microsoft Windows 2000, Windows XP или Windows Vista и находятся в одном домене. Сервер GHOST постоянно подключен к сети и может быть рабочей станцией с операционной системой Windows, Professional или Server Edition (он не обязан быть сервером Active Directory). Кроме того, предположим, что переносные компьютеры отсутствуют в сети компании во время установки клиентских решений ESET. Структура сети может быть похожей на приведенную ниже схему:



2.2.2 Перед установкой

Перед установкой с веб-узла компании ESET необходимо загрузить следующие установочные пакеты.

компоненты ESET Remote Administrator:

ESET Remote Administrator — сервер
ESET Remote Administrator — консоль

Клиентские решения ESET:

ESET Smart Security 4.x
ESET Smart Security 3.x
ESET NOD32 Antivirus 4.x
ESET NOD32 Antivirus 3.x
ESET NOD32 Antivirus 2.7

Загружайте только те клиентские решения, которые будут использоваться на рабочих станциях-клиентах.

2.2.3 Установка

2.2.3.1 Установка сервера ERA Server

Установите сервер ERAS на сервер с именем GHOST (см. пример в разделе Обзор среды 11). При этом можно выбрать **обычный** или **расширенный** режим установки.

В обычном режиме потребуется указать ключ лицензии — файл с расширением LIC или ZIP, — который позволяет серверу ERAS работать в течение времени, определяемого лицензией. Затем надо будет настроить параметры обновления (имя пользователя, пароль и сервер обновления). Этот шаг можно и пропустить, поскольку параметры обновления можно настроить позже.

В расширенном режиме можно настроить дополнительные параметры программы установки. Значения этих параметров можно изменить позже в консоли ERAC, но в большинстве случаев в этом нет необходимости. Единственным исключением является имя сервера, которое должно совпадать с именем DNS, значением % COMPUTERNAME % операционной системы или же IP-адресом, присвоенным данному компьютеру. Это самый важный элемент данных при удаленной установке. Если при установке не указать имя, программа установки автоматически воспользуется значением переменной %COMPUTERNAME%, чего в большинстве случаев будет достаточно. Также важно выбрать правильную базу данных, в которой будут храниться данные сервера ERAS. Дополнительные сведения см. в разделе Типы баз данных, поддерживаемых ERA Server 14.

Внимание! В последних версиях ОС Microsoft Windows (Windows Vista, Windows Server 2008 и Windows 7) используются политики безопасности, ограничивающие разрешения учетной записи локального пользователя, то есть пользователь может быть не в состоянии выполнять определенные действия с сетью. Если служба ERA работает в учетной записи локального пользователя, в некоторых конфигурациях сети могут возникнуть проблемы с запуском установки (например, при удаленной установке из домена в рабочей группе). В системах Windows Vista, Windows Server 2008 или Windows 7 рекомендуется запускать службу ERA с достаточными разрешениями доступа к сети. В сценарии расширенной установки можно указать учетную запись, от имени которой должна выполняться служба ЭРА.

Примечание: Несмотря на то что сервер ERA Server полностью поддерживает Юникод, в некоторых ситуациях (например, при обработке сообщений электронной почты или имен компьютеров) он преобразует символы в кодировку ANSI или наоборот. При этом применяется параметр «Язык программ, не поддерживающих Юникод». Даже если используется нелокализованная версия ERA (т. е. версия на одной из разновидностей английского языка), рекомендуется, чтобы этот параметр соответствовал языку среды, в которой находится сервер. Чтобы найти этот параметр, на **панели управления** щелкните по элементу **«Язык и региональные стандарты»** и откройте вкладку **«Дополнительно»**.

По умолчанию программные компоненты сервера ERAS устанавливаются в папку

%ProgramFiles%\ESET\ESET Remote Administrator\Server

Все остальные компоненты (такие как журналы, пакеты установки, конфигурация и т. п.) хранятся в папке

%ALLUSERSPROFILE%\Application Data \ESET\ESET Remote Administrator\Server

Служба ERAS запускается автоматически после установки. Результаты текущей работы службы ERAS записываются в файл

%ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server\logs\era.log

Установка из командной строки

Сервер ERAS можно установить с указанными ниже параметрами командной строки.

/q — автоматическая установка. Вмешательство пользователя невозможно. Диалоговые окна не отображаются.
/qb — вмешательство пользователя невозможно, но ход установки отображается на индикаторе.

Пример *era_server_nt32_ENU.msi /qb*

Параметры и конфигурация установки из командной строки могут быть дополнены конфигурационным *XML*-файлом администратора *cfg.xml*, который должен находиться в каталоге с установочным *MSI*-файлом ERA. Файл конфигурации можно создать в редакторе ESET Configuration Editor. Этот файл позволяет настроить различные параметры ERA. Дополнительные сведения см. в разделе ESET Configuration Editor 34.

2.2.3.1.1 Установка в режиме кластера

Сценарий расширенной установки позволяет активировать **установку в режиме кластера**. При установке в режиме кластера можно указать путь к папке общих данных кластера, которая полностью доступна для всех узлов кластера (то есть у всех узлов должен быть доступ на чтение и запись в эту папку). Это может быть кворумный диск кластера либо сетевой путь к общей папке. Если используется общая папка, необходимо включить общий доступ для **компьютеров** в свойствах этой папки. В группу **«Разрешения»** необходимо добавить имя узла кластера с полными правами.
Необходимо установить сервер ERA Server на все узлы кластера. Если используется база данных, отличная от встроенной MS Access, необходимо убедится, что все узлы ERA Server подключены к той же базе данных. На следующих этапах также важно задать имя узла кластера, где в качестве имени сервера должно быть установлено ERA.

Внимание! В консоли администратора кластера необходимо настроить службу ESET Remote Administrator Server (ERA_SERVER) как обычную службу кластера.

Перед удалением сервера ERA Server необходимо сначала отключить узел кластера.

2.2.3.2 Установка консоли ERA Console

Установите ESET Remote Administrator Console на компьютер администратора. На завершающем этапе установки в расширенном режиме введите название сервера ERA Server (или его IP-адрес), к которому консоль ERAC будет автоматически подключаться при запуске. В нашем примере он назван GHOST.

После установки запустите консоль ERAC и проверьте соединение с сервером ERAS. По умолчанию для подключения к серверу ERA Server пароль не требуется (текстовое поле пароля пустое), однако настоятельно рекомендуется его установить. Чтобы создать пароль для подключения к серверу ERA Server, вызовите команду **«Файл»** > **«Изменить пароль...»** и изменить пароль для консоли, нажав кнопку **«Изменить...»**.

Администратор может указать пароль для доступа с правами администратора и доступа только для чтения (что позволяет пользователям только просматривать конфигурацию сервера ERAS, но не изменять ее).

2.2.3.3 Зеркало

С помощью консоли ERA Console можно активировать сервер обновления в локальной сети — зеркало сервера ERA Server. Сервер затем можно использовать для обновления рабочих станций сети. Включение зеркала позволяет уменьшить объем данных, передаваемых через подключение к Интернету.

Выполните указанные ниже действия.

1) Подключите консоль ERA Console к серверу ERA Server, выбрав команду **«Файл»** > **«Подключение»**.
2) В консоли ERA Console выберите команду **«Служебные программы»** > **«Настройки сервера...»** и откройте вкладку **«Обновления»**.
3) В раскрывающемся меню **«Сервер обновления»** выберите команду **«Выбирать автоматически»** и установите интервал обновления в 60 минут. Укажите **«Имя пользователя обновления»** (EAV-****), нажмите кнопку **«Установить пароль...»** и введите или вставьте из буфера обмена пароль, полученный с именем пользователя.
4) Выберите команду **«Создать зеркало обновления»**. Оставьте путь по умолчанию для дублируемых файлов и порт сервера HTTP (2221). Для параметра **«Аутентификация»** оставьте значение «Нет».
5) Откройте вкладку **«Дополнительно»** и нажмите кнопку **«Изменить дополнительные настройки...»**. В дереве параметров выберите команду **ERA Server** > **«Настройка»** > **«Зеркало»** > **«Создать зеркало для выбранных компонентов программы»**. Нажмите кнопку **«Изменить»** справа и выберите компоненты программы для загрузки. Выберите все языковые версии компонентов, которые будут использоваться в данной сети.
6) На вкладке **«Обновления»** нажмите кнопку **«Обновить»**, чтобы создать зеркало.

Дополнительные сведения о параметрах конфигурации зеркала см. в разделе Включение и настройка зеркала 85.

2.2.3.4 Типы баз данных, поддерживаемые сервером ERA Server

По умолчанию в программе используется ядро Microsoft Access (СУБД Jet). В сервере ERAS версии 4.0 также поддерживаются следующие СУБД:

- Microsoft SQL Server 2005 или более поздней версии
- MySQL 5.0 или более поздней версии
- Oracle 9i или более поздней версии

Тип СУБД можно выбрать при установке сервера ERAS в расширенном режиме. После установки изменить тип СУБД прямо из ERA будет невозможно, однако это можно сделать с помощью ERA Maintenance Tool 92.

Примечание.
- СУБД Microsoft Access не поддерживается ядром системы Windows Server 2008.
- Для SQL Server Express максимальный размер баз данных составляет 4 Гб.

2.2.3.4.1 Основные требования

Сначала необходимо создать базу данных на сервере базы данных. Программа установки сервера ERAS может создать пустую базу данных MySQL, которой автоматически присваивается имя ESETRADB.

По умолчанию программа установки автоматически создает новую базу данных. Чтобы создать базу данных вручную, нажмите кнопку **«Экспортировать сценарий»**. Флажок **«Автоматически создать таблицы в новой базе данных»** должен быть снят.

Параметры сравнения

Сортировка будет выполняться согласно параметрам по умолчанию в каждой базе данных. При необходимости активируйте параметра CASE INSENSIVITY (CI) (нечувствительность к регистру).

Чтобы активировать:

- для MS SQL и MySQL необходимо установить параметр COLLATE с активированным CI;
- для ORACLE необходимо установить параметр NLS_SORT с активированным CI;
- для MS Access никаких действий предпринимать не надо, поскольку CI уже активирован.

Кодировка

Очень важно использовать кодировку UNICODE (рекомендуется UTF-8), особенно если у клиентов настроены определенные региональные параметры или если сервер ERA работает в локализованной версии. Если репликация не планируется, и все клиенты подключены к одному серверу, можно использовать кодировку для локализованной версии ERA, которая устанавливается.

MARS (Multiple Active Result Sets)

Если используется база данных MS SQL, для надежной работы требуется ODBC-драйвер с поддержкой MARS. В противном случае сервер будет работать менее эффективно, и в журнал сервера будет зарегистрировано следующее сообщение об ошибке:

Database connection problem. It is strongly recommended to use odbc driver that supports multiple active result sets (MARS). The server will continue to run but the database communication may be slower. See the documentation or contact ESET support for more information. (Ошибка подключения к базе данных. Настоятельно рекомендуется использовать ODBC-драйвер, который поддерживает MARS. Сервер будет продолжать работать, но может замедлиться связь с базой данных. Дополнительные сведения см. в документации или обратитесь в службу поддержки ESET.)

Если проблема возникает с другой базой данных (не MS SQL), сервер регистрирует следующее сообщение в журнале сервера и останавливается:

Database connection problem. Updating the odbc driver may help. You can also contact ESET support for more information. (Ошибка подключения к базе данных. Может помочь обновление ODBC-драйвера. За дополнительными сведения обращайтесь в службу поддержки ESET.)

Драйверы без поддержки MARS:
- SQLSRV32.DLL (2000.85.1117.00);
- SQLSRV32.DLL (6.0.6001.18000) — изначально есть в ОС Windows Vista и Windows Server 2008;

Драйвер с поддержкой MARS:
- SQLNCLI.DLL (2005.90.1399.00).

2.2.3.4.2 Настройка подключения к базе данных

После создания новой базы данных необходимо задать параметры подключения к серверу базы данных одним из следующих способов.

1. С использованием DSN (имени источника данных).
   Чтобы вручную указать DSN, запустите
   администратор источников данных (OBDC)
   (откройте **«Пуск» > «Выполнить»** и введите *odbcad32.exe*).

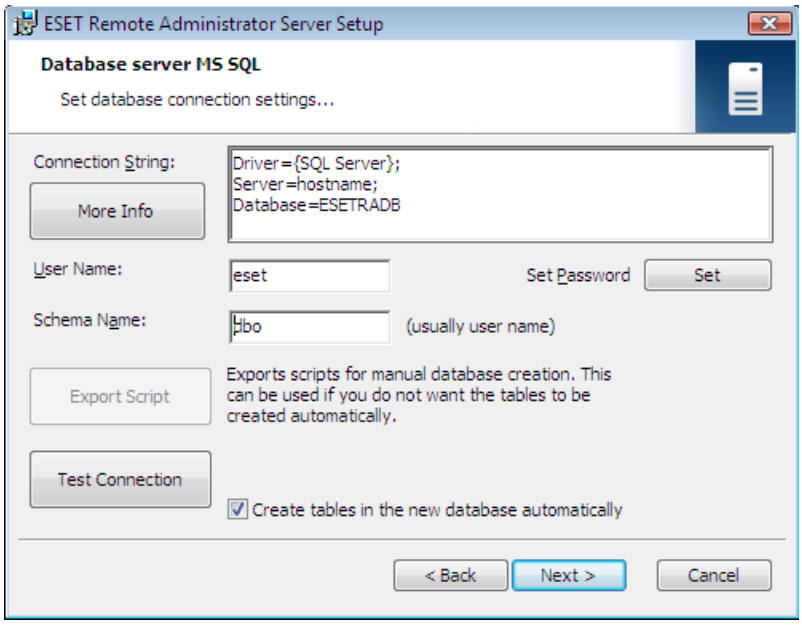
   Пример DSN-соединения:
   DSN =ERASqlServer

   Внимание! Для нормальной работы ERA рекомендуется использовать *System DSN*.

   При установке в MSSQL с аутентификацией Windows или домена в строке подключения необходимо указать формат DNS.

2. Напрямую с использованием полной строки соединения.
   Необходимо указать все обязательные параметры: драйвер, сервер и название базы данных.

   Вот пример полной строки соединения для сервера MS SQL:
   Driver ={SQL Server}; Server =имя_сервера; Database =ESETRADB



Вот пример полной строки соединения для сервера Oracle:
Driver ={Oracle in instantclient10_1}; dbq =имя_сервера: 1521/ESETRADB

Вот пример полной строки соединения для сервера MySQL:
Driver ={MySQL ODBC 3.51 Driver}; Server =имя_сервера; Database =ESETRADB

Затем введите **имя пользователя** и **пароль** для подключения (нажав кнопку **«Задать»**). Для СУБД Oracle и MS SQL также требуется **название схемы** (для сервера MS SQL им обычно является имя пользователя). Нажмите кнопку **«Проверить соединение»**, чтобы проверить соединение с сервером базы данных.

Примечание. Вместо аутентификации Windows или домена рекомендуется использовать аутентификацию сервера базы данных.

2.2.3.4.3 Установка поверх существующей базы данных

Если в базе данных уже существуют таблицы, программа установки выдаст уведомление. Чтобы перезаписать содержимое существующих таблиц, выберите команду **«Перезаписать»** (***Предупреждение.*** В результате содержимое таблиц будет удалено, а их структура перезаписана!) Чтобы оставить таблицы без изменений, выберите команду **«Пропустить»**.

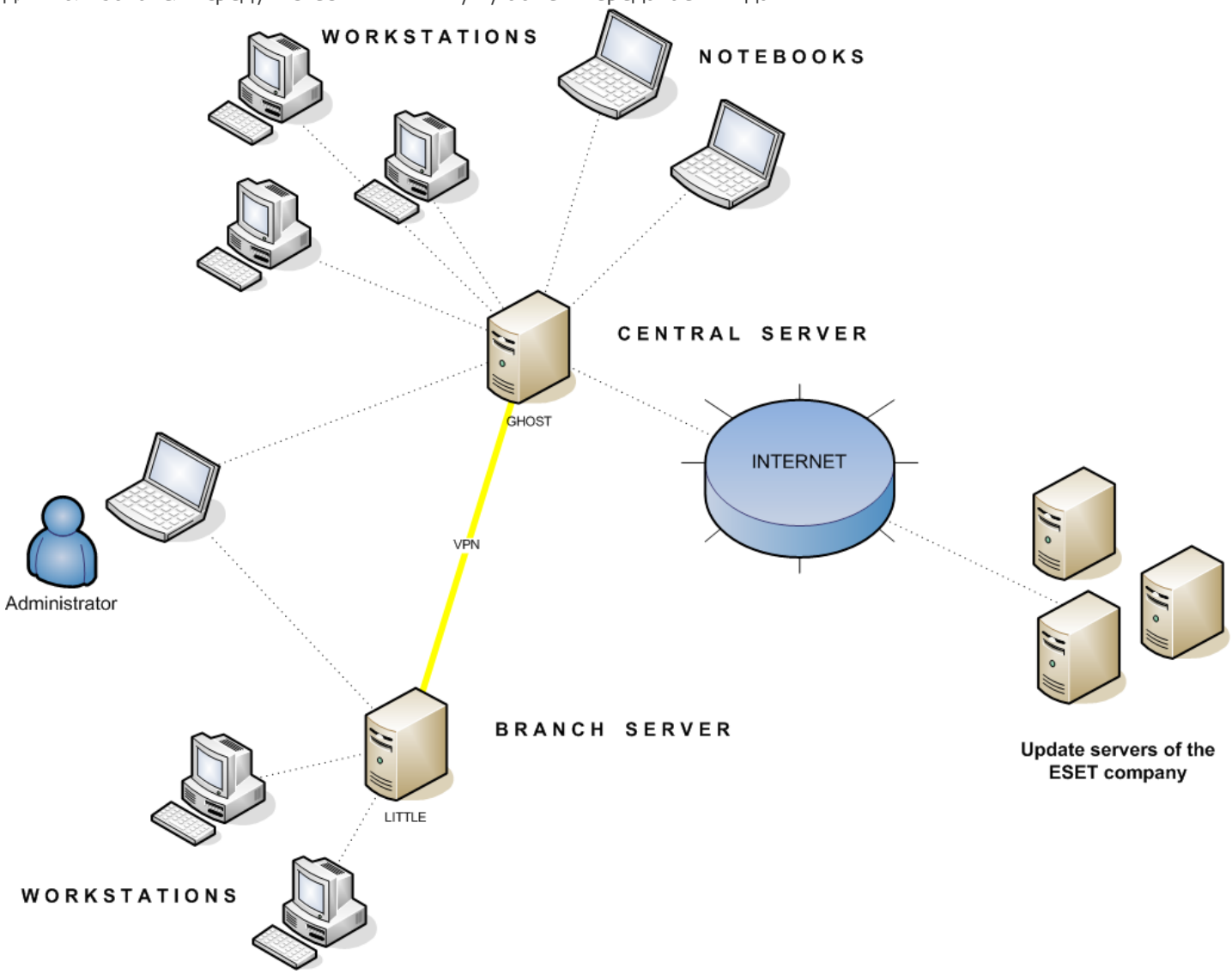
Примечание. Выбор команды **«Пропустить»** в определенных условиях может привести к ошибкам несогласованности базы данных, особенно в ситуации, когда таблицы повреждены или несовместимы с текущей версией.

Чтобы отменить установку сервера ERAS и вручную проанализировать базу данных, выберите команду **«Отмена»**.

2.3 Сценарий: установка в корпоративной среде

2.3.1 Обзор среды (структура сети)

Ниже представлена копия вышеописанной сетевой структуры, в которую включен один дополнительный филиал, несколько клиентов и один сервер под именем LITTLE. Предположим, что для связи между головным офисом и филиалом используется медленное VPN-соединение. В этом сценарии зеркало следует установить на сервер LITTLE. Также установим на сервер LITTLE второй сервер ERA Server, чтобы создать более удобную для пользователя среду и свести к минимуму объем передаваемых данных.

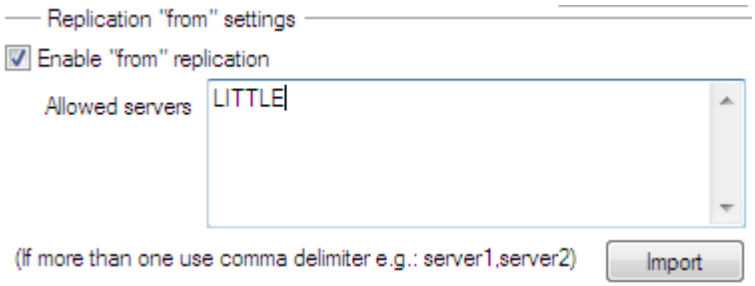


2.3.2 Установка

2.3.2.1 Установка в головном офисе

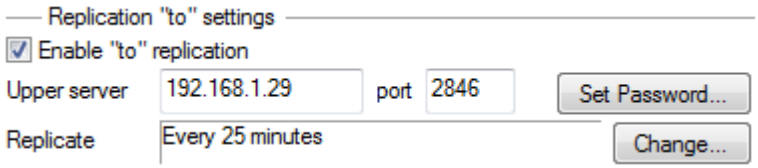
Установка ERAS, ERAC и клиентских рабочих станций очень похожа на установку в предыдущем сценарии. Единственным отличием является конфигурация главного сервера ERAS (GHOST). В меню **«Служебные программы»** > **«Настройки сервера...»** > **«Репликация»** установите флажок **«Включить репликацию "из"»** и введите имя дополнительного сервера в группе **«Разрешенные серверы»**. В нашем случае сервер нижнего уровня называется LITTLE.

Если на сервере верхнего уровня задан пароль для репликации (**«Служебные программы»** > **«Настройки сервера...»** > **«Безопасность»** > **«Пароль для репликации»**), этот пароль нужно использовать для аутентификации на сервере нижнего уровня.



2.3.2.2 Филиал: установка сервера ERA Server

Как и в примере выше, установите дополнительные сервер ERAS и консоль ERAC. Снова активируйте и настройте параметры репликации. В этот раз установите флажок **«Включить репликацию»** (**«Служебные программы»** > **«Настройки сервера...»** > **«Репликация»**) и укажите имя главного сервера ERAS. Рекомендуется указать IP-адрес основного сервера, то есть IP-адрес сервера GHOST.



2.3.2.3 Филиал: установка HTTP-сервера зеркала

В этом случае также можно использовать конфигурацию установки зеркала, описанную в предыдущем сценарии. Единственные отличия заключаются в разделах, в которых определяются имя пользователя и пароль.

Как показано на рисунке из раздела Обзор среды 17, обновления для филиала загружаются не с серверов обновления компании ESET, а с сервера в головном офисе (GHOST). Источник обновления определяется следующим URL-адресом:

http://ghost:2221 (или http://IP_сервера_ghost:2221)

По умолчанию не нужно указывать имя пользователя или пароль, поскольку интегрированному HTTP-серверу не требуется аутентификация.

Дополнительные сведения о настройке зеркала ERAS см. в разделе Зеркало сервера 83.

2.3.2.4 Филиал: удаленная установка на клиентах

В этом случае также можно использовать предыдущую модель с тем отличием, что все действия можно выполнять в консоли ERAC, напрямую подключенной к серверу ERAS филиала (в нашем примере: LITTLE). Это делается для предотвращения передачи установочных пакетов по каналу VPN, на котором скорость обмена данными является более низкой.

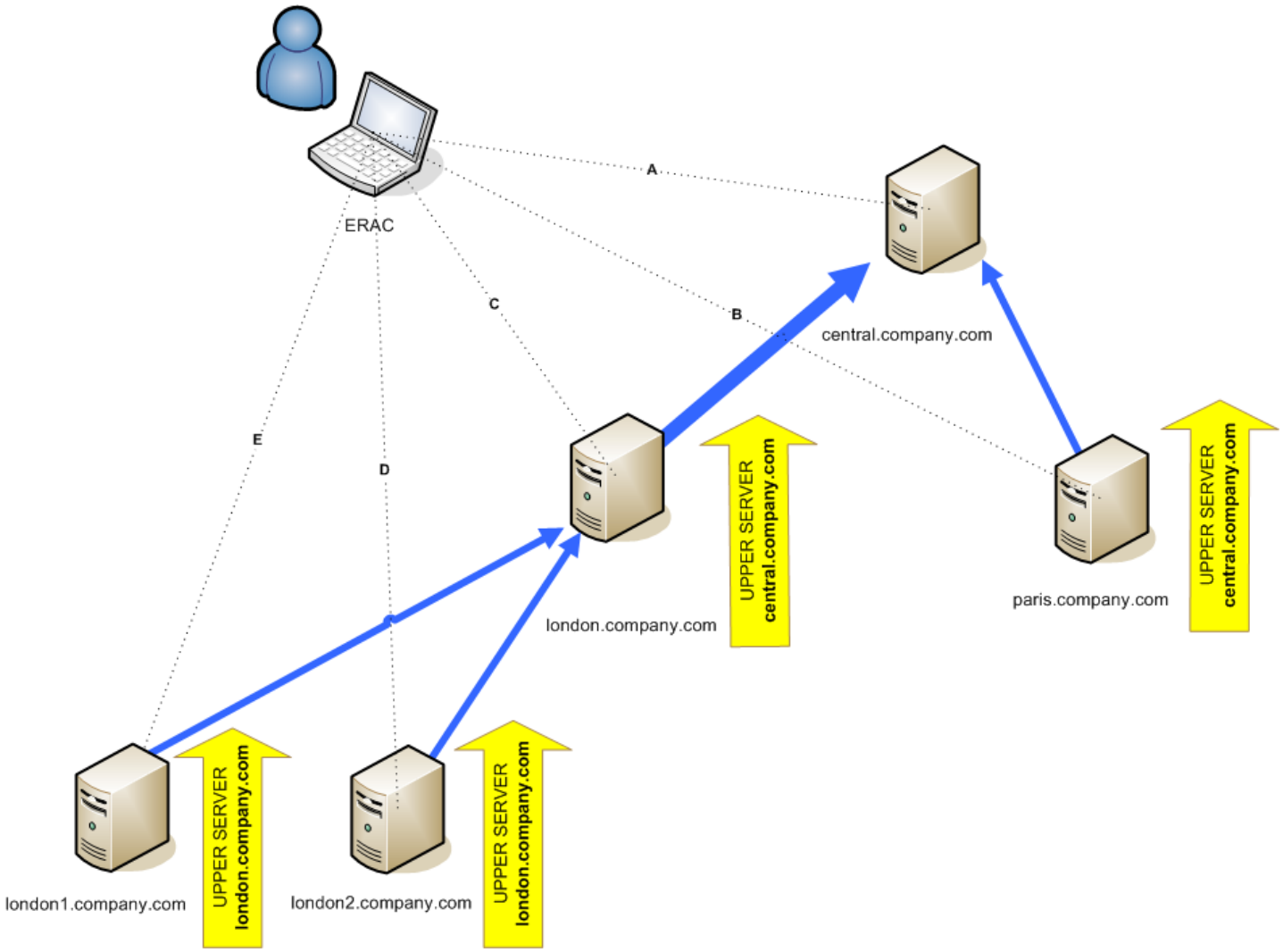
2.3.3 Прочие требования к корпоративным средам

В больших сетях можно устанавливать несколько серверов ERA Server для удаленной установки на клиентских компьютерах с более доступных серверов. Для этого север ERAS предлагает функцию *репликации* (см. разделы Установка в головном офисе 18 и Филиал: установка сервера ERA Server 18), которая позволяет хранить сведения, перенаправляемые родительскому серверу ERAS (*сервер верхнего уровня*). Репликацию можно настроить с помощью консоли ERAC.

Функция репликации очень полезна для компаний, в состав которых входит несколько филиалов или удаленных офисов. Сценарий развертывания данной модели описан ниже. Установите сервер ERAS в каждом офисе и реплицируйте их на центральный сервер ERAS. Преимущество этой конфигурации особенно очевидно в частных сетях, подключенных через VPN, в которых скорость передачи обычно является более низкой — администратору нужно будет подключаться только к центральному серверу ERAS (соединение, помеченное буквой A на рисунке ниже). При этом нет необходимости в использовании сети VPN для доступа к отдельным подразделениям (соединения B, C, D и E). Обход более медленного канала связи делает возможным репликация сервера ERAS.

Настройка репликации позволяет администратору определять сведения, которые будут автоматически передаваться серверам верхнего уровня через заданный интервал времени, и сведения, которые будут отправляться по запросу администратора сервера верхнего уровня. Репликация делает интерфейс ERA более удобным для пользователя, а также позволяет снизить объем сетевого трафика.

Еще одно преимущество репликации состоит в том, что несколько пользователей могут входить в систему с разными уровнями разрешений. Администратор, который через консоль обращается к серверу ERAS по адресу london2.company.com (соединение E), может управлять только теми клиентами, которые подключены к веб-узлу london2.company.com. Администратор, который обращается к центральному узлу по адресу company.com (A), может управлять всеми клиентами, размещенными в головном офисе, в отделениях и филиалах.


ERAC
A
B
C
D
E
central.company.com
london.company.com
paris.company.com
UPPER SERVER central.company.com
UPPER SERVER central.company.com
UPPER SERVER london.company.com
UPPER SERVER london.company.com
london1.company.com
london2.company.com

3. Работа с консолью ERAC

3.1 Подключение к серверу ERAS

Основная часть функций ERAC становится доступной только после подключения к ERAS. Перед подключением укажите имя или IP-адрес сервера следующим образом:

Откройте ERAC и выберите в меню команду **«Файл»** > **«Изменить соединения...»** (или **«Служебные программы»** > **«Настройки консоли...»**) и откройте вкладку **«Соединение»**.

Нажмите кнопку **«Добавить/удалить...»**, чтобы добавить новые серверы ERA Server или изменить перечисленные. Выберите нужный сервер в раскрывающемся меню **«Выбор соединения»**. Затем нажмите кнопку **«Подключиться»**.

Другие параметры в этом окне описаны ниже.

- **«Соединить с выбранным сервером при запуске консоли»**
  Если выбран этот вариант, консоль автоматически подключится к выбранному серверу ERAS после запуска.
- **«Показывать сообщение при ошибке соединения»**
  При возникновении ошибки в ходе обмена данными между ERAC и ERAS на экран выводится предупреждение.

Существует два типа аутентификации.

ERA Server

Аутентификация пользователя с применением учетных данных ERAS. По умолчанию для подключения к серверу ERAS пароль не требуется, однако настоятельно рекомендуется его установить. Чтобы создать пароль для подключения к серверу ERAS, выполните указанные ниже действия.

Выберите в меню команду **«Файл»** > **«Изменить пароль...»** (или **«Служебные программы»** > **«Настройки сервера»** > **«Безопасность»**) и нажмите кнопку **«Изменить...»** напротив параметра **«Пароль для консоли»**.

При вводе пароля можно установить флажок **«Запомнить пароль»**. Прежде чем воспользоваться им, оцените возможный риск для безопасности. Чтобы удалить все сохраненные пароли, выберите в меню **«Файл»** команду **«Удалить пароли из кэша...»**.

Выберите в раскрывающемся меню **«Доступ»** тип доступа (возможные варианты: **«Администратор»** и **«Только чтение»**), введите свой пароль и нажмите кнопку **«ОК»**.

«Windows/домен»

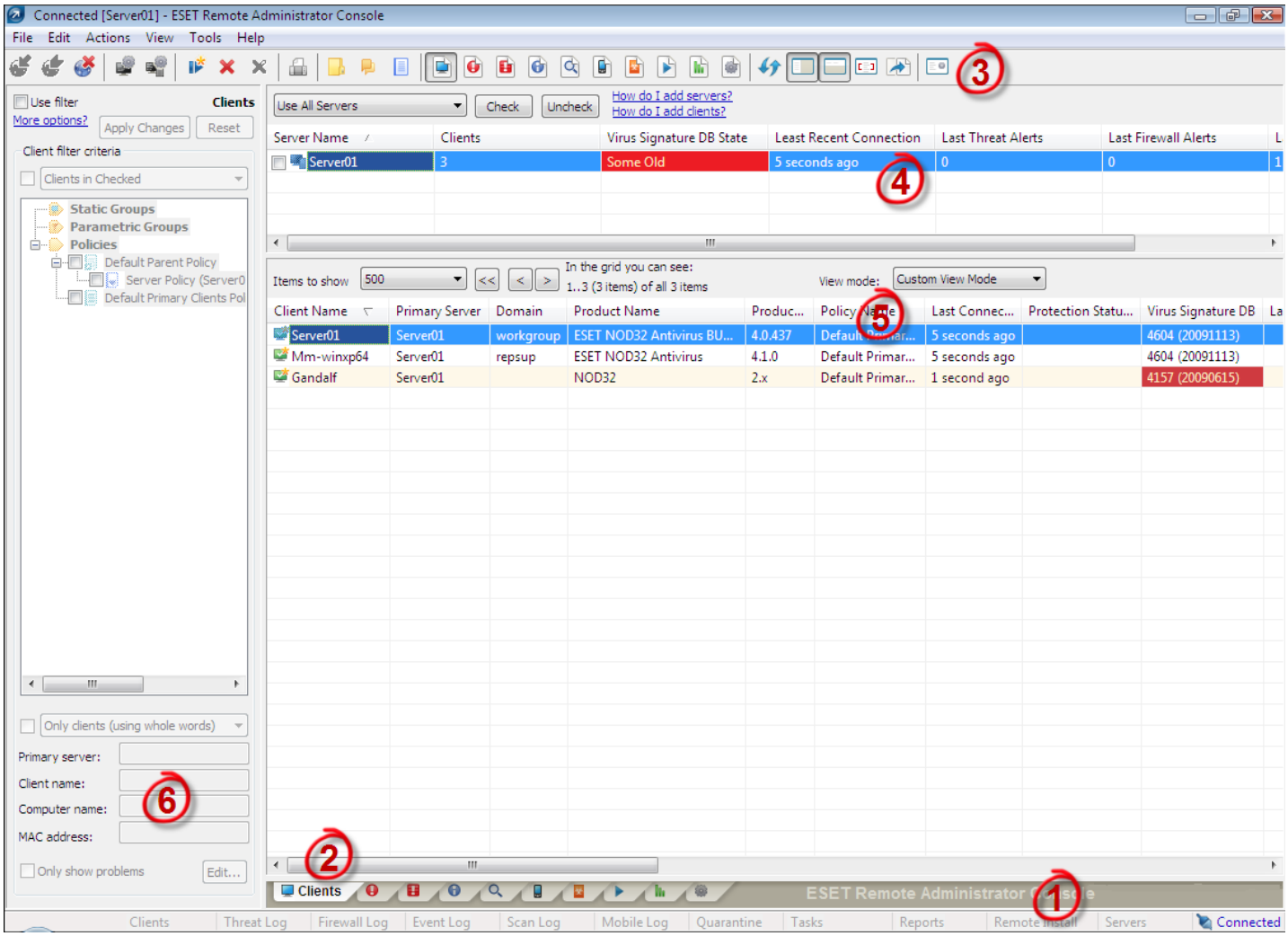
Аутентификация пользователя с применением учетных данных Windows или домена. Чтобы аутентификация Windows или домена выполнялась правильно, установите ERAS с помощью учетной записи Windows или домена с достаточным уровнем доступа. Эта функция включается с помощью следующей команды: меню **«Служебные программы»** > **«Настройки сервера...»** > вкладка **«Дополнительно»** > **«Изменить дополнительные настройки...»** > **ESET Remote Administrator** > **ERA Server** > **«Настройка»** > **«Безопасность»**.

Параметр **«Разрешить аутентификацию Windows/домен»** включает или отключает аутентификацию Windows или домена.
Параметр **«Группы администраторов»** позволяет указать группы, для которых будет включена аутентификация Windows или домена.
Параметр **«Группы только для чтения»** позволяет указать группы с доступом только для чтения.

После установки соединения заголовок программы изменится на строку **«Подключено к [имя_сервера]»**. Кроме того, для подключения к серверу ERAS можно выбрать в меню **«Файл»** команду **«Подключение»**.

Примечание. Данные, передаваемые между ERAC и ERAS, шифруются по алгоритму AES-256.

3.2 Главное окно консоли ERAC



Текущее состояние соединения между консолью ERAC и сервером ERAS отображается в строке состояния (1). Все необходимые данные регулярно обновляются с сервера ERAS (по умолчанию каждую минуту — см. **«Служебные программы»** > **«Параметры консоли...»**). Ход обновления также отображается в строке состояния.

Примечание. Для обновления отображаемых данных нажмите клавишу F5.

Информация распределена по нескольким вкладкам в порядке ее значимости (2). В большинстве случаев данные можно отсортировать в возрастающем или в убывающем порядке, щелкнув по их заголовку (5), и переупорядочить с помощью операции перетаскивания. Число обрабатываемых строк данных можно ограничить с помощью раскрывающегося меню **«Элементы для отображения»** и кнопок **«Просмотр страниц одна за одной»**. Для отображения нужного набора атрибутов выберите **режим просмотра** (более подробные сведения см. в разделе Фильтрация данных 23).

Раздел «Сервер» (4) имеет важное значение при репликации серверов ERA Server. В этом разделе отображаются сводные данные о консоли, к которой подключен сервер ERAS, а также сведения о дочерних или («подчиненных») серверах ERA Server. Раскрывающееся меню «Серверы» в разделе 4 влияет на диапазон данных, отображаемых в разделе 5.

- **«Использовать все серверы»**
  Отображение данных со всех серверов ERA Server — раздел (5).

- **«Использовать только выбранные серверы»**
  Отображение данных с выбранных серверов ERA Server — раздел (5).

- **«Исключить выбранные серверы»**
  Исключение данных с выбранных серверов ERA Server.

Столбцы в разделе 4

- **«Имя сервера»**
  Отображает имя сервера.

- **«Клиенты»**
  Общее число подключенных клиентов или клиентов в базе данных выбранного сервера ERAS.

- **«Диапазон БД сигнатур вирусов»**
  Версия БД сигнатур вирусов на клиентах выбранного сервера ERAS.

- **«Самое старое подключение»**
  Время, прошедшее с момента последнего подключения к серверу.

- **«Последние предупреждения об угрозах»**
  Общее число предупреждений о вирусах (см. атрибут **Последнее предупреждение об угрозе** в разделе 5).

- **«Последние предупреждения файервола»**
  Общее число предупреждений файервола.

- **«Предупреждения о последнем событии»**
  Общее число текущих событий (см. атрибут **«Последнее событие»** в разделе 5).

Если в данный момент отсутствует соединение, щелкните правой кнопкой мыши в разделе «Сервер» (4) и выберите команду **«Соединение с этим сервером»**, чтобы подключиться к выбранному серверу ERAS.

Если включена репликация, в разделе «Сервер» (4) отобразятся дополнительные сведения.

Важнейшие функции консоли ERAC доступны из главного меню или с панели инструментов консоли ERAC (3).

Последний раздел — **«Настройка фильтра компьютеров»** (6) см. раздел Фильтрация данных 23.

3.3 Фильтрация данных

В консоли ERAC представлены различные возможности и средства для удобного администрирования клиентских компьютеров и событий. Наличие расширенной системы фильтрации часто может быть очень важным, особенно в системах с большим числом клиентов, когда отображаемая информация должна быть сгруппированной и простой в управлении. В ERAC есть несколько средств для эффективной сортировки и фильтрации данных о подключенных клиентах.

3.3.1 Фильтр

Фильтр позволяет администратору вывести на экран информацию только об определенных серверах или клиентских рабочих станциях. Чтобы отобразить параметры фильтра, выберите в меню ERAC команду **«Вид»** > **«Показать/скрыть панель фильтра»**.

Чтобы активировать фильтрацию, установите флажок **«Использовать фильтр»** в верхней левой части окна ERAC. При всех последующих изменениях в критериях фильтрации отображаемые данные будут обновляться автоматически, если иное не задано на вкладке **«Служебные программы»** > **«Настройки консоли...»** > **«Другие настройки»**.

Задайте критерии фильтрации в соответствующем разделе для клиентов. Клиенты могут принадлежать нескольким группам и политикам. Назначение клиента в статическую или параметрическую группу может эффективно использоваться не только для фильтрации, но и для таких действий, как формирование отчетов. Дополнительные сведения об управлении группами см. в разделе Диспетчер групп 55. Использование политик для разделения клиентов также может преследовать выполнение несколько задач. Дополнительные сведения о создании политик и управления ими см. в разделе Политики 57.

Первым средством фильтрации является раздел выбора группы и политики. Доступны три перечисленных ниже варианта.

- **«Клиенты в отмеченных»**
  На панели клиентов будут отображены клиенты в выбранных группах или политиках.

- **«Клиенты в неотмеченных»**
  На панели клиентов будут отображены клиенты, не выбранные в группах или политиках, и клиенты, не входящие в группы.
- **«Клиенты не в группах»**
  Будут отображены только клиенты, принадлежащие какой-либо группе или политике.

Примечание. После выбора группы в списке будут также отображены все ее подгруппы.

В нижней части раздела «Фильтр» можно задать и другие параметры.
- **«Только клиенты (исп. целые слова)»**
  В выходные данные попадают только те клиенты, имена которых совпадают с введенной строкой.
- **«Только клиенты, начинающиеся с (?,*)»**
  В выходные данные попадают только те клиенты, имена которых начинаются с указанной строки.
- **«Только клиенты типа (?,*)»**
  В выходные данные попадают только те клиенты, в именах которых содержится указанная строка.
- **«Исключить клиенты (исп. целые слова)», «Исключить клиенты, начинающиеся с (?,*)», «Исключить клиенты типа (?,*)»**
  Эти параметры позволяют получить результаты, противоположные предыдущим трем вариантам.

В полях «Главный сервер», «Имя клиента», «Имя компьютера» и «MAC-адрес» допустимы целые строки. При заполнении любого из этих полей в базу данных отправляется запрос, а результаты фильтруются на основании заполненного поля; при этом используется логический оператор «И».

Последний параметр реализует фильтрацию по признакам проблем: отображаются только клиенты с указанным видом проблемы. Чтобы отобразить список проблем, выберите команду **«Показать проблему»** и нажмите кнопку **«Изменить...»**. Выберите проблемы, которые нужно отобразить, и нажмите кнопку **«ОК»**, чтобы вывести список клиентов с выбранными проблемами.

Все изменения, внесенные в настройки фильтрации, вступят в силу после нажатия кнопки **«Применить изменения»**. Чтобы восстановить значения по умолчанию, нажмите кнопку **«Сброс»**. Чтобы автоматически генерировать новые выходные данные при каждом внесении изменений в настройки фильтрации, выберите параметр **«Служебные программы»** > **«Настройки консоли...»** > **«Другие настройки...»** > **«Автоматически применять изменения»**.

3.3.2 Контекстное меню

Правая кнопка мыши вызывает контекстное меню, с помощью которого настраиваются выходные данные в столбцах. Контекстное меню содержит перечисленные ниже команды.

- **«Выбрать все»**
  Выбор всех записей.
- **«Выбрать по „...“»**
  Эта команда позволяет щелкнуть правой кнопкой мыши по любому атрибуту и автоматически выбрать (выделить) все остальные рабочие станции или серверы с таким же атрибутом. Строка «...» автоматически заменяется значением текущей вкладки.
- **«Обратить выбор»**
  Инвертирование выбора записей в списке.
- **«Скрыть выбранное»**
  Скрытие выбранных записей.
- **«Скрыть невыбранное»**
  Скрытие всех невыбранных записей списка.

- **«Отобразить/скрыть столбцы»**
  Открывает окно **«Настройки консоли»** > **«Отобразить/скрыть столбцы»**, в котором можно указать столбцы, которые будут доступны на выбранной панели.

Команды **«Скрыть выбранное/невыбранное»** используются в ситуации, когда после фильтрации требуется дальнейшее упорядочивание. Чтобы отключить все фильтры, установленные в контекстном меню, выберите в меню **«Вид»** команду **«Ограниченный просмотр»** или щелкните по значку на панели инструментов ERAC. Также можно нажать клавишу **F5**, чтобы обновить данные и отключить фильтры.

Пример

- Отображение клиентов с предупреждениями об угрозе.
  На вкладке**«Клиенты»** щелкните правой кнопкой мыши по пустой панели с полем «Последнее предупреждение о вирусе» и выберите в контекстном меню команду **«Выбрать по „...“»**. Затем выберите в контекстном меню команду **«Скрыть выбранное»**.

- Вывод предупреждений об угрозе для клиентов Joseph и Charles
  Откройте вкладку **«Журнал угроз»** и щелкните правой кнопкой мыши по любому атрибуту в столбце «Имя клиента» со значением Joseph. В контекстном меню выберите команду **«Выбрать по „Joseph“»**. Затем, нажав и удерживая клавишу CTRL, щелкните правой кнопкой мыши и выберите команду **«Выбрать по „Charles“»**. Наконец, щелкните правой кнопкой мыши, выберите в контекстном меню команду **«Скрыть невыбранное»** и отпустите клавишу CTRL.

С помощью клавиши CTRL можно выделять отдельные записи и отменять их выделение, а с помощью клавиши SHIFT — выделять и отменять выделение групп записей.

Примечание. Фильтрация также упрощает создание новых задач для конкретных (выделенных) клиентов. Доступны различные варианты фильтрации: просто экспериментируйте с различными их сочетаниями.

3.3.3 Режим просмотра

На вкладке **«Клиенты»** число отображаемых столбцов регулируется с помощью раскрывающегося меню **«Режим отображения»** с правого края консоли. В **режиме полного просмотра** отображаются все столбцы, в то время как в **режиме минимального просмотра** показаны только самые важные из них. Эти режимы определены заранее, и изменить их невозможно. Для перехода в пользовательский режим просмотра выберите команду **«Пользовательский режим просмотра»**. Его можно настроить на вкладке **«Служебные программы»** > **«Настройки консоли...»** > **«Столбцы» > «Отобразить/Скрыть»**.

3.4 Вкладки в консоли ERAC

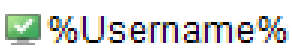
3.4.1 Общее описание вкладок и клиентов

Большая часть данных на вкладках относится к подключенным ПК. Каждый компьютер, подключенный к серверу ERAS, идентифицируется следующими атрибутами:
Имя компьютера (имя клиента), MAC-адрес, Главный сервер.

Поведение сервера ERAS в связи с определенными операциями в сети (такими как переименование ПК) определяется в разделе «Расширенная настройка сервера ERAS». Это позволяет предотвращать дублирование записей на вкладке **«Клиенты»**. Например, если один из компьютеров в сети был переименован, а его MAC-адрес не изменился, можно избежать создания новой записи на вкладке **«Клиенты»**.

Клиенты, которые подключаются к серверу ERAS в первый раз, отмечены значением **«Да»** в столбце **«Новый пользователь»**. Они также отмечены маленькой звездочкой в правом верхнем углу на значке клиента (см. рисунок ниже). Эта функция позволяет администратору легко обнаружить новый подключившийся компьютер. Этот атрибут может иметь разное значение в зависимости от используемых администратором рабочих процедур.

На случай перенастройки и перемещения клиента в определенную группу назначение состояния «Новый клиент» можно отменить, щелкнув клиента и выбрав команду **«Задать/снять отметки»** > **«Снять отметку „Новый“»**. Значок этого клиента будет заменен значком, показанным на рисунке ниже, а значение атрибута в столбце **«Новый пользователь»** будет изменено на **«Нет»**.



Примечание. Атрибут «Примечание» является необязательным на всех трех вкладках. Администратор может вставить сюда любое описание (например, *«Офис №129»*).

Временные значения в сервере ERAS отображаются в относительном (*«2 дня назад»*), абсолютном (20.5.2008) или системном (с учетом региональных параметров) режимах.

В большинстве случаев данные можно отсортировать в возрастающем или в убывающем порядке, щелкнув их заголовок, и переупорядочить с помощью операции перетаскивания.

При выборе конкретных значений активируются другие вкладки, на которых отображаются более подробные сведения. Например, если щелкнуть значение в столбце **«Последнее предупреждение об угрозе»** программа откроет вкладку **«Журнал угроз»** и отобразит записи, относящиеся к данному клиенту. Если щелкнуть значение, информация о котором не помещается на вкладке, откроется диалоговое окно с подробными сведениями о соответствующем клиенте.

3.4.2 Репликация и данные на отдельных вкладках

Если консоль ERAC подключена к серверу ERAS, выполняющему роль сервера верхнего уровня, все данные от серверов нижнего уровня будут показываться автоматически, если только соответствующий подчиненный сервер не настроен иным образом. Типы реплицируемых данных настраиваются на сервере нижнего уровня в меню **«Служебные программы»** > **«Настройки сервера»** > **«Репликация»** > **«Параметры репликации "на"»**.

В таком сценарии могут отсутствовать приведенные ниже данные:

- данные журнала предупреждений (вкладка **«Журнал угроз»**);
- данные журнала сканирования по требованию (вкладка **«Журнал сканирования»**);
- подробные конфигурации текущего клиента в XML-формате (вкладка **«Клиенты»**, столбец **«Конфигурация»**, **«Состояние защиты»**, **«Свойства защиты»**, **Сведения о системе»**).

Также могут отсутствовать данные программы ESET SysInspector. Модуль ESET SysInspector встроен в продукты ESET версий 4.x и более поздних.

Если данные не удается найти в диалоговых окнах программы, нажмите кнопку **«Запрос»** (находится в разделе **«Действия»** > **«Свойства»** > **«Конфигурация»**). Нажатие этой кнопки позволяет загрузить недостающие сведения с сервера ERAS нижнего уровня. Поскольку репликация всегда инициируется сервером ERAS нижнего уровня, недостающие данные обычно передаются в пределах заданного интервала репликации.

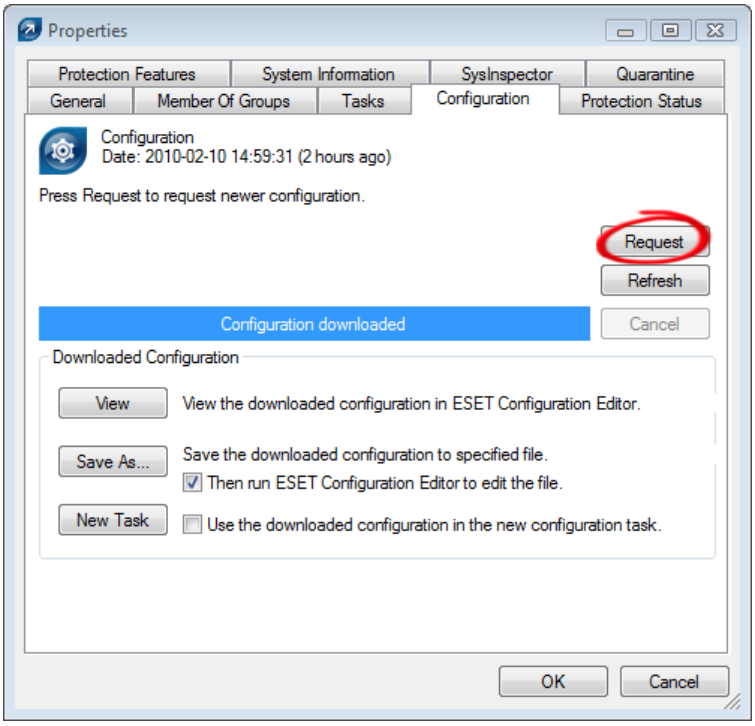


Рисунок: нажатие кнопки «Запрос» для загрузки недостающих данных с серверов ERA Server нижнего уровня.

На сервере верхнего уровня можно настроить уровень детализации журналов, которые будут получены севером (**«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные параметры...»** > **ESET Remote Administrator** > **ERA Server** > **«Настройка»** > **«Обслуживание сервера»** > **«Принимаемые журналы...»**).

Примечание. Этот параметр применяется ко всем клиентам, подключенным к серверу (а не только к реплицируемым).

3.4.3 Вкладка «Клиенты»

На этой вкладке отображаются общие сведения об отдельных клиентах.

Атрибут	Описание
Имя клиента	Имя клиента (можно изменить в окне «Свойства клиента» на вкладке «Общие»).
Имя компьютера	Имя рабочей станции/сервера (имя хоста).
MAC-адрес	MAC-адрес (сетевой адаптер).
Главный сервер	Имя сервера ERAS, с которым клиент ведет обмен данными.
Домен	Имя домена или группы, к которым принадлежит клиент (это не группы, созданные в ERAS).
IP	IP-адрес.
Имя продукта	Название продукта безопасности ESET.
Версия продукта	Версия продукта безопасности ESET.
Название политики	Название назначенной клиенту политики.
Последнее подключение	Время последнего подключения клиента к ERAS (эта метка времени включается во все остальные данные, полученные от клиентов, за исключением некоторых данных, полученных при репликации).
Текст состояния защиты	Текущее состояние продукта безопасности ESET, установленного на клиенте.
БД сигнатур вирусов	Версия базы данных сигнатур вирусов.
Последнее предупреждение об угрозе	Последний инцидент с вирусом.
Последнее предупреждение файервола	Последнее событие, обнаруженное персональным файерволом ESET Smart Security (отображаются события уровня «Предупреждение» и выше).
Последнее предупреждение о событии	Последнее сообщение об ошибке.
Проверено файлов в прошлый раз	Количество файлов, проверенных во время последнего сканирования по требованию.
Заражено файлов в прошлый раз	Количество зараженных файлов, которые были обнаружены во время последнего сканирования по требованию.
Очищено файлов в прошлый раз	Количество файлов, очищенных (или удаленных) в ходе последнего сканирования по требованию.
Дата последнего сканирования	Время последнего сканирования по требованию.
Запрос перезапуска	Запрос о необходимости перезагрузки (например, после обновления программы).
Дата запроса перезапуска.	Время первого запроса на перезагрузку.
Последний запуск продукта	Время последнего запуска клиентской программы.
Дата установки продукта	Дата установки продукта безопасности ESET на клиентский компьютер.
Пользователь в роуминге	Для клиентов с этим атрибутом задача «обновить сейчас» выполняется при каждом подключении к серверу ERAS (такой вариант рекомендуется для ноутбуков). Обновление производится только в том случае, если база данных сигнатур вирусов не является актуальной.
Новый клиент	Новый подключенный компьютер (см. раздел Общее описание вкладок и клиентов 25).
Имя ОС	Название клиентской операционной системы.
Платформа ОС	Платформа операционной системы (Windows, Linux и т. п.).
Аппаратная платформа	32-разрядная или 64-разрядная.
Конфигурация	Конфигурация клиента в файле current.xml (включая время и дату создания конфигурации).
Состояние защиты	Отчет об общем состоянии (смысл этого атрибута аналогичен смыслу атрибута «Конфигурация»).
Свойства защиты	Отчет об общем состоянии программных компонентов (аналогично атрибуту «Конфигурация»).
Сведения о системе	Сведения о системе, переданные клиентом на сервер ERAS (включая время отправки этих данных).
SysInspector	Клиенты, в состав которых входит средство ESET SysInspector, могут отправлять журналы

Атрибут	Описание
	из этого дополнительного приложения.
Прочие сведения	Прочие данные, отображение которых включено администратором (настраиваются в консоли ERAC в меню **«Служебные программы» > «Настройки сервера...» > «Дополнительно» > «Изменить дополнительные настройки...» > ESET Remote Administrator > ERA Server > «Настройка» > «Другие настройки» > «Прочие данные клиента»**).
Примечание	Краткое описание клиента (вводится администратором).

Примечание. Некоторые значения выводятся только в информационных целях и могут быть неактуальны на момент просмотра их администратором в консоли. Например, в 7:00 утра могла быть ошибка обновления, но в 8:00 утра обновление было успешно выполнено. Это относится к значениям **«Последнее предупреждение об угрозе»** и **«Последнее предупреждение о событии»**. Если администратор знает, что эти данные устарели, он может удалить их, щелкнув правой кнопкой мыши и выбрав в меню команду **«Удалить информацию»** > **«Удалить последнее предупреждение об угрозе»** или **«Удалить последнее предупреждение о событии»**. В результате информация о последнем инциденте с вирусом или последнем системном событии будет удалена.

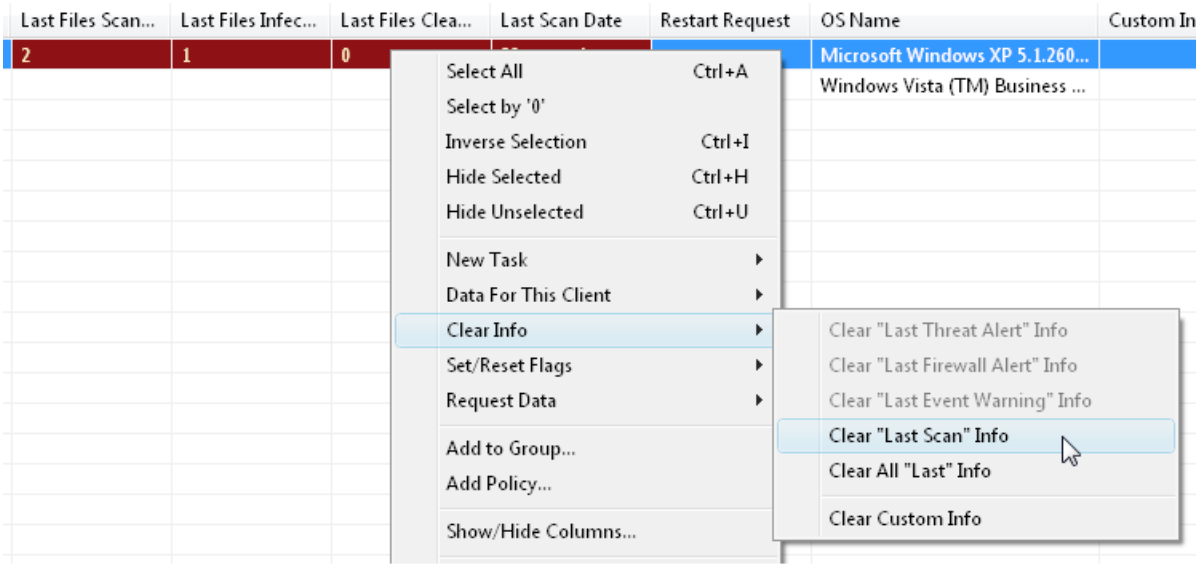


Рисунок: устаревшие события в столбцах последнего предупреждения об угрозе и последнего предупреждения о событии легко удаляются.

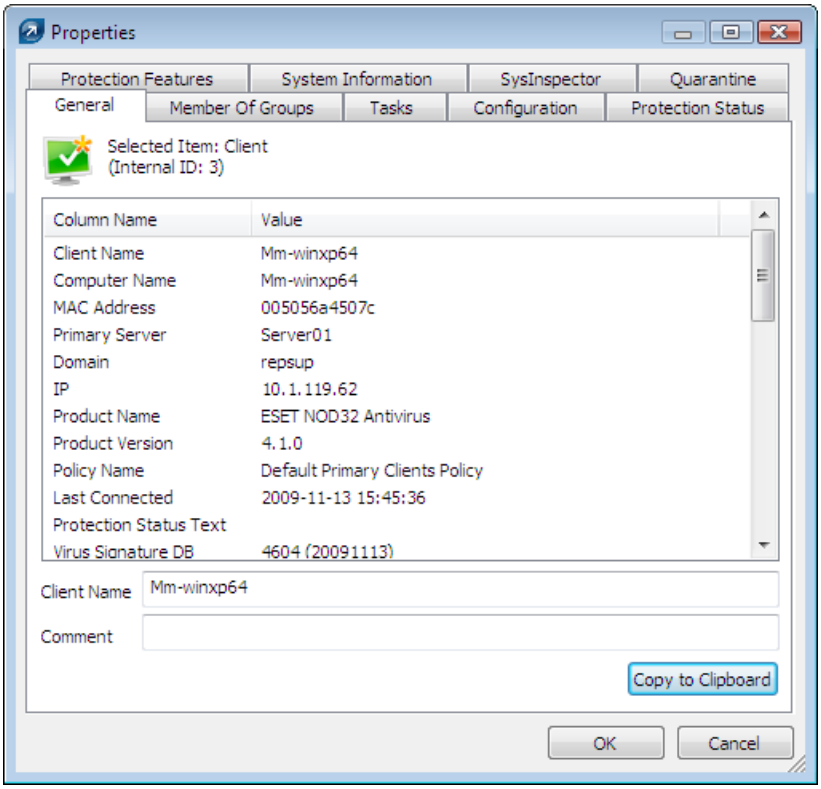


Рисунок: подробные сведения о клиентской рабочей станции.

Двойной щелчок по имени клиента на вкладке **«Клиенты»** позволяет вызвать одну из следующих функций.

- **«Общее»**
Содержит информацию, аналогичную представленной на вкладке «Клиенты». Здесь можно задать имя клиента (имя, под которым клиент виден в ERA), а также необязательный комментарий.

- **«Член группы»**
На этой вкладке перечислены все группы, в которые входит клиент. Дополнительные сведения см. в разделе Фильтрация данных 23.

- **«Задачи»**
Задачи, связанные с данным клиентом. Дополнительные сведения см. в разделе Задачи 50.

- **«Конфигурация»**
На этой вкладке можно просмотреть текущую конфигурацию клиента и экспортировать ее в XML-файл. Далее в этом руководстве будет рассказано, как с помощью *XML*-файлов создавать шаблоны конфигурации для новых и измененных конфигурационных *XML*-файлов. Дополнительные сведения см. в разделе Задачи 50.

- **«Состояние защиты»**
Это отчет об общем состоянии всех программ ESET. Некоторые из отчетов являются интерактивными и позволяют немедленно выполнять нужные действия. Смысл этой функции заключается в том, что таким образом отпадает необходимость вручную определять новые задачи для разрешения конкретных проблем в системе защиты.

- **«Свойства защиты»**
Состояние всех компонентов системы защиты ESET (модуля защиты от спама, персонального файервола и т. д.).

- **«Сведения о системе»**
Подробные сведения об установленной программе, версиях ее компонентов и т. п.

- **SysInspector**
Подробные сведения об автоматически запускаемых процессах и процессах, выполняющихся в фоновом режиме.

- **«Карантин»**
Содержит список всех файлов, помещенных в карантин. Файлы, помещенные в карантин, можно запросить у клиента и сохранить на локальном диске.

3.4.4 Вкладка «Журнал угроз»

На этой вкладке содержатся подробные сведения о конкретных вирусах и инцидентах.

Атрибут	Описание
Имя клиента	Имя клиента, сообщившего о наличии угрозы.
Имя компьютера	Имя рабочей станции/сервера (имя хоста).
MAC-адрес	MAC-адрес (сетевой адаптер).
Главный сервер	Имя сервера ERAS, с которым клиент ведет обмен данными.
Дата получения	Время регистрации данного события сервером ERAS.
Дата обнаружения	Время возникновения данного события.
Уровень	Уровень предупреждения.
Сканер	Название средства безопасности, обнаружившего угрозу.
Объект	Тип объекта.
Имя	Как правило, это папка, в которой обнаружено заражение.
Угроза	Название обнаруженного злонамеренного кода.
Действие	Действие, выполненное соответствующим средством безопасности.
Пользователь	Имя пользователя, находившегося в системе во время инцидента.
Информация	Сведения об обнаруженной угрозе.
Детали	Состояние отправки клиентского журнала.

3.4.5 Вкладка «Журнал файервола»

На этой вкладке отображаются сведения о работе клиентского файервола.

Атрибут	Описание
Имя клиента	Имя клиента, сообщившего о событии.
Имя компьютера	Имя рабочей станции/сервера (имя хоста).
MAC-адрес	MAC-адрес (сетевой адаптер).
Главный сервер	Имя сервера ERAS, с которым клиент ведет обмен данными.
Дата получения	Время регистрации данного события сервером ERAS.
Дата обнаружения	Время возникновения данного события.
Уровень	Уровень предупреждения.
Событие	Описание события.
Источник	IP-адрес источника.
Объект	IP-адрес целевого объекта.
Протокол	Задействованный протокол.
Правило	Задействованное правило файервола.
Приложение	Задействованное приложение.
Пользователь	Имя пользователя, находившегося в системе во время инцидента.

3.4.6 Вкладка «Журнал событий»

На этой вкладке перечислены все системные события.

Атрибут	Описание
Имя клиента	Имя клиента, сообщившего о событии.
Имя компьютера	Имя рабочей станции/сервера (имя хоста).
MAC-адрес	MAC-адрес (сетевой адаптер).
Главный сервер	Имя сервера ERAS, с которым клиент ведет обмен данными.
Дата получения	Время регистрации данного события сервером ERAS.
Дата обнаружения	Время возникновения данного события.
Уровень	Уровень предупреждения.
Программный модуль	Название программного компонента, сообщившего о событии.
Событие	Описание события.
Пользователь	Имя пользователя, связанного с данным событием.

3.4.7 Вкладка «Журнал сканирования»

На этой вкладке представлены результаты проверок компьютеров по требованию, которые запускались удаленно, локально на клиентских компьютерах или в качестве запланированных задач.

Атрибут	Описание
ID сканирования	код соответствующей записи в базе данных (код имеет вид *Номер проверки*)
Имя клиента	Имя клиентского ПК, на котором была выполнена проверка.
Имя компьютера	Имя рабочей станции/сервера (имя хоста).
MAC-адрес	MAC-адрес (сетевой адаптер).
Главный сервер	Имя сервера ERA Server, с которым клиент ведет обмен данными.
Дата получения	Время регистрации события сканирования на сервере ERAS.
Дата об	Время выполнения проверки на клиенте.
Проверенные объекты	Проверенные файлы, папки и устройства.
Проверено	Количество проверенных файлов.
Заражено	Количество зараженных файлов.
Очищено	Количество очищенных (или удаленных) объектов.
Статус	Статус проверки.
Пользователь	Имя пользователя, находившегося в системе во время инцидента.
Тип	Тип пользователя.
Сканер	Тип сканера.
Детали	Состояние отправки клиентского журнала.

3.4.8 Вкладка «Мобильный журнал»

На этой вкладке отображаются подробные журналы из мобильных устройств, подключенных к серверу ERA Server.

Атрибут	Описание
ID мобильного устройства	Сетевой идентификатор мобильного устройства
Имя клиента	Имя клиента, на котором было выполнено действие.
Имя компьютера	Имя рабочей станции/сервера (имя хоста).
MAC-адрес	MAC-адрес (сетевой адаптер).
Главный сервер	Имя сервера ERA Server, с которым клиент ведет обмен данными.
Дата получения	Время регистрации данного события сервером ERAS.
Дата обнаружения	Время выполнения события на клиенте.
Уровень	Уровень предупреждения.
Тип журнала	Тип журнала (например, журнал аудита безопасности, журнал защиты от спама в SMS).
Событие	Описание события.
Тип объекта	Объект, к которому имеет отношение событие (например, SMS, файл и т. п.).
Имя объекта	Конкретный объект, к которому имеет отношение событие (например, номер телефона отправителя SMS, путь к файлу и т. п.).
Действие	Действие, выполненное во время события (или возникшая ошибка).

3.4.9 Вкладка «Карантин»

На этой вкладке отображено все содержимое карантина в сети.

Атрибут	Описание
ID в карантине	Идентификатор помещенного в карантин объекта (номер увеличивается в порядке возникновения).
Хэш	Хэш файла.
Дата получения	Время регистрации события сканирования на сервере ERAS.
Первое обнаружение	Время, которое прошло с момента первого обнаружения объекта, помещенного в карантин.
Последнее обнаружение	Время, которое прошло с момента последнего обнаружения объекта, помещенного в карантин.
Имя объекта	Как правило, это папка, в которой обнаружено заражение.
Имя файла	Имя файла, помещенного в карантин.
Расширение	Тип расширения файла, помещенного в карантин.
Размер	Размер файла, помещенного в карантин.
Причина	Причина помещения в карантин; как правило, это описание типа угрозы.
Количество клиентов	Количество клиентов, которые поместили объект в карантин.
Всего	Количество операций помещения объекта в карантин.
Файл	Показывает, была ли запрошена загрузка объекта на сервер.

3.4.10 Вкладка «Задачи»

Предназначение этой вкладки описано в разделе «Задачи». На ней доступны перечисленные ниже атрибуты.

Атрибут	Описание
Статус	Статус задачи (активная — находится в стадии применения, завершенная — доставка на клиенты осуществлена).
Тип	Тип задачи.
Имя	Название задачи.
Описание	Описание задачи.
Дата развертывания	Дата и время выполнения задачи.
Дата получения	Время регистрации данного события сервером ERAS.
Детали	Состояние отправки журнала задач.
Примечание	Краткое описание клиента (вводится администратором).

3.4.11 Вкладка «Отчеты»

На этой вкладке представлены функции для архивирования результатов работы сети за определенные периоды времени. Вкладка **«Отчеты»** позволяет организовать представление статистических данных в виде графиков или диаграмм. Дополнительные сведения см. в разделе Отчеты 78.

3.4.12 Вкладка «Удаленная установка»

На этой вкладке представлены параметры различных способов удаленной установки приложений ESET Smart Security или ESET NOD32 Antivirus на клиентские компьютеры. Дополнительные сведения см. в разделе Удаленная установка 38.

3.5 Настройка консоли ERA Console

ERAC настраивается в меню **«Служебные программы»** > **«Настройки консоли...»**.

3.5.1 Вкладка «Подключение»

Эта вкладка предназначена для настройки подключения консоли ERAC к серверу ERAS. Дополнительные сведения см. в разделе Подключение к серверу ERAS 21.

3.5.2 Вкладка «Отобразить/скрыть столбцы»

На этой вкладке можно задать список атрибутов (столбцов), отображаемых на других вкладках. Изменения отражаются в пользовательском режиме просмотра (вкладка **«Клиенты»**). Внести изменения в других режимах просмотра нельзя.

3.5.3 Вкладка «Цвета»

На этой вкладке можно назначать разные цвета конкретным системным событиям, что позволяет обращать внимание на проблемные клиенты (т. н. условное выделение). Например, клиенты с несколько устаревшей базой данных сигнатур вирусов **«Клиенты: предыдущая версия»**) могут отличаться от клиентов с полностью устаревшей БД (**«Клиенты: устаревшая версия или н/д»**).

3.5.4 Вкладка «Пути»

На этой вкладке можно задать каталог, в который консоль ERAC будет сохранять отчеты, загружаемые с сервера ERAS. По умолчанию отчеты сохраняются в следующем каталоге:

%ALLUSERSPROFILE%\Application Data\Eset\ESET Remote Administrator\Console\reports

3.5.5 Вкладка «Дата/время»

Формат столбцов со значениями даты и времени.

- **«Точное»**
  Время в консоли отображается в абсолютном формате (например, *"14:30:00"*).
- **«Относительное»**
  Время в консоли отображается в относительном формате (например, *"2 недели назад"*.)
- **«Региональное»**
  Время в консоли отображается в соответствии с региональными настройками Windows.
- **«Расчет времени в UTC (местное время)»**
  Установка этого флажка приводит значения времени к местному часовому поясу. В противном случае отображаются значения времени в формате GMT – UTC.

3.5.6 Вкладка «Другие настройки»

- **«Настройки фильтра»** > **«Автоматически применять изменения»**
  Если эта функция включена, фильтры на различных вкладках формируют новые выходные данные при каждом изменении своих параметров. В противном случае фильтрация будет выполняться только после нажатия кнопки **«Применить изменения»**.

- **«Обновления удаленного администрирования»**
  В этом разделе включается проверка новых версий ESET Remote Administrator. Рекомендуется использовать значение по умолчанию **«Ежемесячно»**. При обнаружении новой версии в консоли ERAC в момент запуска программы отображается соответствующее уведомление.

- **«Другие настройки»** > **«Автоматическое обновление»**
  Если эта функция включена, данные на различных вкладках автоматически обновляются через заданные интервалы времени.

- **«Другие настройки»** > **«Показать сетку»**
  Этот параметр включает отображение сетки, разделяющей рабочее пространство на всех вкладках на отдельные ячейки.

- **«Другие настройки»** > **«Отображать клиента как "Сервер/Имя" вместо "Сервер/Компьютер/MAC"»**
  Задает режим отображения клиентов в некоторых диалоговых окнах (например, в окне «Новая задача»). Этот параметр влияет только на внешний вид.

- **«Другие настройки»** > **«Использовать значок в системном лотке»**
  Включает отображение значка консоли ERA Console в области уведомлений Windows.

- **«Другие настройки»** > **«Показывать в панели задач»**
  Окно консоли ERAC в свернутом виде будет доступно в панели задач Windows.

- **«Другие настройки** > **«Изменять значок в системном лотке при наличии проблем на клиенте**
  Включите этот параметр в сочетании с кнопкой «Изменить», чтобы определит события, которые будут приводить к изменению цвета значка ERAC в области уведомлений.

Если консоль ERAC на компьютере администратора будет постоянно подключена к серверу ERAS, рекомендуется установить флажок **«Показывать на панели задач»** и сворачивать ее, когда она неактивна. При возникновении проблемы значок в области уведомлений окрасится красным цветом, что послужит сигналом для вмешательства администратора. Также рекомендуется настроить параметр **«Изменять значок в системном лотке при наличии проблем на клиенте»** и задать список событий, вызывающих изменение цвета значка консоли ERAC. При этом, однако, консоль ERAC будет отключаться, если на сервере включено сжатие базы данных.

- **«Другие настройки»** > **«Подсказки»**
  Включение («Включить все») или отключение («Отключить все») всех информационных сообщений.

3.6 Режимы отображения

В консоли ERAC доступно два режима отображения:

- режим администратора;
- режим только для чтения.

В режиме администратора в консоли ERAC пользователю предоставляется полный контроль над всеми функциями и параметрами, а также возможность администрировать все подключенные клиентские рабочие станции.

Режим только для чтения предназначен для просмотра состояния решений ESET на клиентских машинах, подключенных к серверу ERAS; создание задач для клиентских рабочих станций, создание пакетов установки и удаленная установка запрещены. Диспетчеры лицензий, политик и уведомлений также недоступны. В режиме только для чтения администратору не разрешено менять настройки консоли ERAC и создавать отчеты.

Режим отображения выбирается при каждом запуске консоли в раскрывающемся меню **«Доступ»**, а пароль для подключения к серверу ERAS можно установить в любом режиме отображения. Возможность настройки

пароля особенно полезна в ситуации, когда необходимо, чтобы часть пользователей имела полный доступ к серверу ERAS, а остальные — доступ только для чтения. Для установки пароля выберите команду **«Служебные программы»** > **«Настройки сервера...»** > **«Безопасность»** и нажмите кнопку **«Изменить...»** напротив параметра «Пароль для консоли (доступ с правами администратора)» или «Пароль для консоли (доступ только для чтения)».

3.7 ESET Configuration Editor

ESET Configuration Editor является важным компонентом консоли ERAC и служит для выполнения нескольких задач. Вот некоторые наиболее важные из них:

- создание предопределенных конфигураций установочных пакетов;
- создание конфигураций или политики, отправляемых на клиенты в виде задач;
- создание общего конфигурационного XML-файла.

Configuration Editor является частью консоли ERAC и представлен в основном файлами *cfgedit.**.

Configuration Editor позволяет администратору удаленно настраивать множество параметров продуктов безопасности компании ESET (в частности, продукты, установленные на клиентских рабочих станциях). Он также позволяет администратору экспортировать конфигурации в XML-файлы, которые затем можно будет использовать в различных целях (например, для создания задач в консоли ERAC, локального импортирования конфигураций в ESET Smart Security и т. п.).

В Configuration Editor используется структура *XML*-шаблона, в котором конфигурация хранится в виде древовидной структуры. Этот шаблон находится в файле *cfgedit.exe*. Именно поэтому рекомендуется регулярно обновлять сервер ERAS и консоль ERAC.

Предупреждение. Configuration Editor позволяет изменять *XML*-файлы. Не изменяйте и не перезаписывайте исходный файл *cfgedit.xml*.

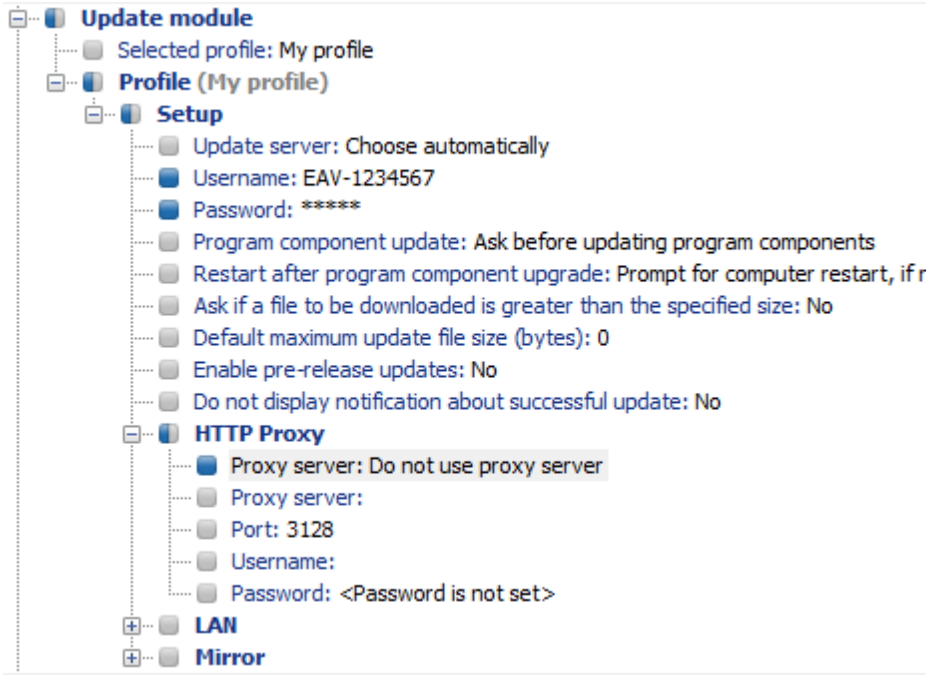
Для работы Configuration Editor необходимы следующие файлы: *eguiEpfw.dll*, *cfgeditLang.dll*, *eguiEpfwLang.dll* и *eset.chm*.

3.7.1 Иерархическое представление конфигурации

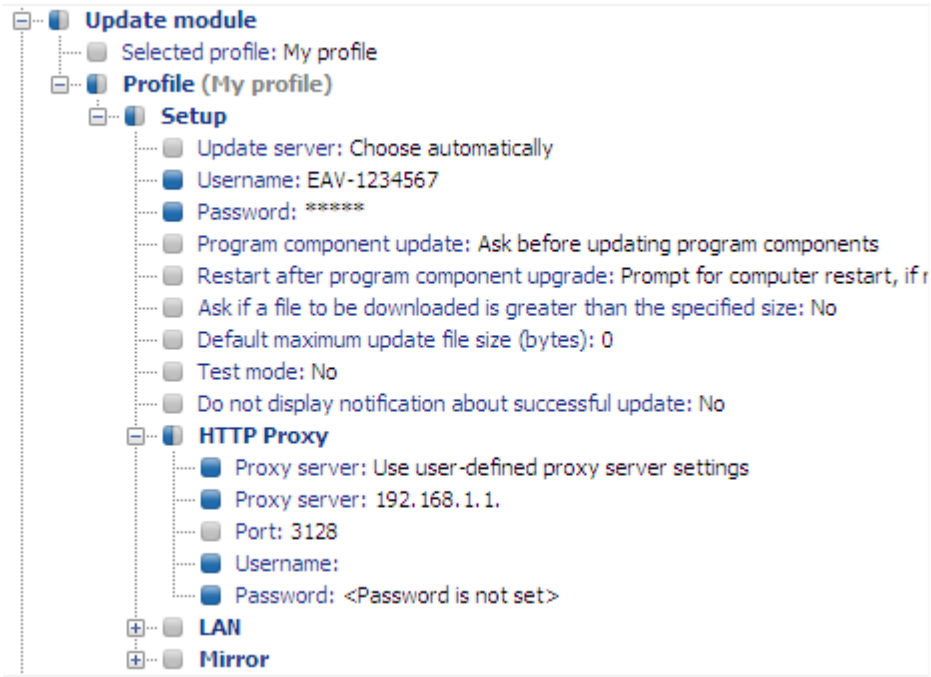
При изменении значения в Configuration Editor это значение отмечается синим символом . Запись, обозначенная серым значком , не менялась и не будет записана в выходную конфигурацию в формате *XML*.

При применении конфигурации к клиентам применяются только те изменения, которые были сохранены в выходном *XML*файле конфигурации (), а все остальные элементы () останутся в прежнем состоянии. Такой подход позволяет последовательно применить несколько разных конфигураций без отмены предыдущих изменений.

На рисунке ниже показан пример. В этой конфигурации вставляются имя пользователя *EAV-12345678* и пароль и запрещается использование прокси-сервера.



Вторая отправляемая клиентам конфигурация (рис. 3—8) гарантирует сохранение предыдущих изменений, включая имя пользователя *EAV-12345678* и пароль. В этой конфигурации также разрешается использование прокси-сервера и задается его адрес и порт.



3.7.2 Основные элементы конфигурации

В этом разделе описано несколько основных элементов конфигурации продуктов ESET Smart Security и ESET NOD32 Antivirus, настраиваемых в ESET Configuration Editor:

- **ESET Smart Security**, **ESET NOD32 Antivirus** > **«Ядро ESET»** > **«Настройка»** > **«Удаленное администрирование»**
  Здесь можно активировать обмен данными между клиентскими компьютерами и сервером ERAS (**«Подключиться к ESET Remote Administrator Server»**). Введите имя или IP-адрес сервера ERAS (**«Адрес сервера»**). Значение параметра **«Интервал между подключениями к серверу»** оставьте значение по умолчанию (5 мин.). При выполнении проверок это значение можно уменьшать до 0, в каковом случае соединение будет устанавливаться каждые десять секунд. Если установлен пароль, воспользуйтесь паролем, заданным на сервере ERAS. Дополнительные сведения о параметре **«Пароль для клиентов»** см. в разделе Вкладка «Безопасность» 82. В данном разделе также доступны дополнительные сведения о настройке пароля.

- **«Ядро ESET»** > **«Настройка»** > **«Лицензионные ключи»**
  На клиентских компьютерах не требуется ни добавлять лицензионные ключи, ни управлять ими. Лицензионные ключи необходимы только для серверных продуктов.

- **«Ядро ESET»** > **«Настройка»** > **ThreatSense.Net**
  В этом разделе задается режим работы системы быстрого оповещения ThreatSense.Net, позволяющей отправлять подозрительные файлы на анализ в лаборатории компании ESET. При развертывании решений ESET в большой сети параметры **«Передача подозрительных файлов»** и **«Разрешить передачу анонимной статистической информации»** играют особую роль: если для них установлено значение **«Не отправлять»** или **«Нет»** соответственно, система ThreatSense.Net полностью отключается. Для автоматической отправки файлов без вмешательства пользователя выберите значения **«Передавать, не спрашивая»** и **«Да»** соответственно. При использовании для подключения к Интернету прокси-сервера задайте параметры соединения в меню **«Ядро ESET» > «Настройка» > «Прокси-сервер»**.
  По умолчанию клиентские продукты отправляют подозрительные файлы на сервер ERAS, который передает их на серверы компании ESET. Поэтому необходимо правильно настроить прокси-сервер на сервере ERAS (**«Служебные программы» > «Настройки сервера...» > «Дополнительно» > «Изменить дополнительные параметры» > ERA Server > «Настройка» > «Прокси-сервер»**).

- **«Ядро»** > **«Настройка»** > **«Защита установочных параметров»**
  Позволяет администратору защитить параметры настройки паролем. Если пароль установлен, он будет запрашиваться при доступе к параметрам настройки на клиентских рабочих станциях. Однако он не используется при внесении изменений в конфигурацию из консоли ERAC.

- **«Ядро»** > **«Настройка»** > **«Расписание/Планировщик»**
  В этом разделе представлены параметры планировщика, с помощью которых администратор может планировать регулярные проверки на вирусы и т. п.

Примечание. По умолчанию в состав всех решений по обеспечению безопасности ESET входит ряд предопределенных задач (в том числе регулярное автоматическое обновление и автоматическая проверка важных файлов при запуске). В большинстве случаев изменять эти задачи или добавлять новые не требуется.

- **«Ядро ESET»** > **«Настройка»** > **«Значения интерфейса пользователя по умолчанию»**
  Параметры в разделе «Значения интерфейса пользователя по умолчанию» (например, **«Показывать заставку при запуске»**/**«Не показывать заставку при запуске»**) применимы только к параметрам по умолчанию клиента. Параметрами клиента можно управлять на основе каждого пользователя и их нельзя изменить удаленно. Чтобы можно было удаленно изменить параметра, для параметра **«Переопределить параметры пользователя»** необходимо установить значение **«Да»**. Параметр **«Переопределить параметры пользователя»** доступен только для клиентов с продуктами безопасности ESET версии 4.0 и старше.

- **«Обновление»**
  В этом разделе Configuration Editor задаются способы применения профилей обновления в обычном режиме. Для этого нужно только внести изменения в предопределенный профиль **«Мой профиль»** и изменить параметры **«Сервер обновлений»**, **«Имя пользователя»** и **«Пароль»**. Если для параметра «Сервер обновлений» задано значение **«Выбирать автоматически»**, все обновления будут загружаться с серверов обновлений компании ESET. В этом случае укажите для параметров **«Имя пользователя»** и **«Пароль»** значения, предоставленные вам при покупке продукта. Дополнительные сведения о настройке получения обновлений от локального сервера (зеркало) на клиентских рабочих станциях см. в разделе Сервер зеркала 83. Дополнительные сведения об использовании планировщика см. в разделе Планировщик 98.

Примечание. На портативных устройствах, таких как ноутбуки, можно настроить два профиля, один из которых будет предназначен для загрузки обновлений с сервера зеркала, а другой — непосредственно с серверов ESET. Дополнительные сведения см. в разделе Комбинированное обновление для ноутбуков 102 в конце этого документа.

4. Установка клиентских решений компании ESET

Эта глава посвящена установке клиентских решений ESET в операционных системах Microsoft Windows. Установку можно выполнять непосредственно на рабочих станциях или удаленно с сервера ERAS. В этой главе также кратко описаны альтернативные способы удаленной установки.

Примечание. Хотя это и возможно чисто технически, не рекомендуется выполнять удаленную установку продуктов ESET на серверы (используйте этот способ только для рабочих станций).

4.1 Непосредственная установка

При непосредственной установке администратор заходит на компьютер, на который нужно установить продукт безопасности ESET. Этот способ не требует никакой дополнительной подготовки и предназначен для небольших компьютерных сетей или сценариев, в которых средства ERA не используются.

Эту задачу можно существенно упростить с помощью предопределенной конфигурации в формате XML. После установки нет необходимости указывать сервера обновлений (имя пользователя, пароль, путь к серверу зеркала и т. п.), настраивать автоматический режим, расписание проверок и т. п.

Отличия в применении конфигурации в формате XML к клиентским решениям ESET версий 3.x и 2.x заключаются в следующем.

- Версия 4.x: загрузите установочный файл (например *ess_nt32_enu.msi*) с веб-сайта *eset.com* и создайте свой собственный установочный пакет в **редакторе установочных пакетов**. Измените или выберите конфигурацию, которую нужно связать с эти пакетом, нажмите кнопку **«Копировать...»** рядом с полем **«Пакет для XX-разрядных систем Windows NT»** и сохраните пакет как **«MSI-файл установки ESET с конфигурацией (*.msi)»**.

  Примечание. При добавлении конфигурации в установочный *MSI*-файл цифровая подпись этого файла больше не будет действительной.

  Кроме того, шаги для версии 3.x применимы также для версии 4.x.

- Версия 3.x: Загрузите установочный файл (например, *ess_nt32_enu.msi*) с веб-сайта *eset.com*. Скопируйте файл конфигурации (*cfg.xml*) в каталог, в котором находится установочный файл. При запуске программа установки автоматически воспользуется конфигурацией из *XML*-файла конфигурации. Если *XML*-файла конфигурации имеет другое имя или он находится в другом месте, можно использовать параметр *ADMINCFG ="genm_r_xml-файлу"* (например, *ess_nt32_enu.msi ADMINCFG ="\\server\xml\settings.xml"* для применения конфигурации, которая хранится на сетевом диске).

- Версия 2.x: Загрузите установочный файл (например, *ndntenst.exe*) с веб-сайта *eset.com*. Извлеките загруженный файл в папку с помощью программы распаковки (например, WinRAR). Папка будет содержать установочные файлы, включая *setup.exe*. Скопируйте файл конфигурации *nod32.xml* в папку. Запустите файл *setup.exe*. При этом автоматически применяется конфигурация из файле *nod32.xml*. Если *XML*-файл конфигурации имеет другое имя или находится в другом месте, используйте параметр */cfg ="путь_к_xml-файлу"*. (например, командная строка *setup.exe /cfg ="\\server\xml\settings.xml"* предписывает использовать конфигурацию, хранящуюся на сетевом диске).

4.2 Удаленная установка

Приложение ERA позволяет выполнять удаленную установку несколькими способами. Рассылку установочных пакетов на целевые рабочие станции можно выполнить одним из следующих методов:

- удаленная автоматическая установка;
- удаленная установка с помощью сценария входа;
- удаленная установка по электронной почте;
- обновление.

Удаленная установка средствами ERA состоит из трех этапов:

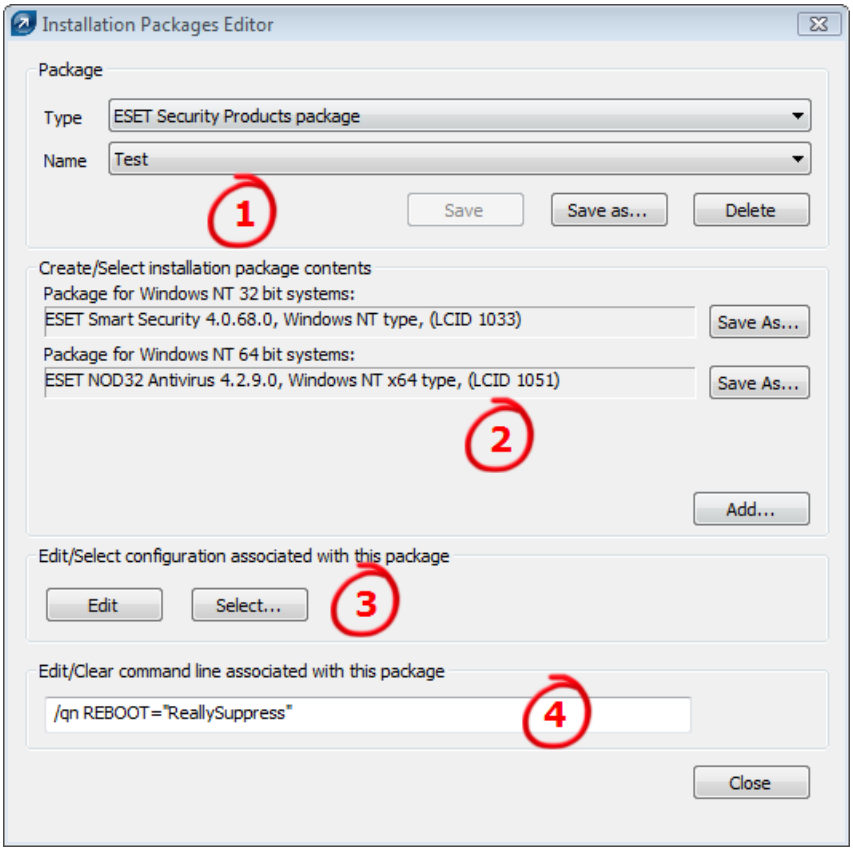
- создание установочных пакетов;
- рассылка пакетов на клиентские рабочие станции (посредством автоматической установки, с помощью

сценария входа, электронной почты, обновления, стороннего решения).

Первый этап инициируется из консоли ERAC, но сам установочный пакет находится на сервере ERAS в следующем каталоге:

%ALLUSERSPROFILE%\Application Data\Eset\ESET Remote Administrator\Server\packages

Для запуска установочных пакетов из консоли ERAC откройте вкладку **«Удаленная установка»**, перейдите на вкладку **«Компьютеры»** и щелкните правой кнопкой мыши любое содержимое в ней. Выберите в контекстном меню команду **«Управление пакетами»**.



Каждый пакет установки имеет свое название (см. (1) на рисунке выше). Остальные разделы диалогового окна связаны с содержимым пакета, которое применяется после его успешной доставки на целевую рабочую станцию. В состав каждого пакета входят такие компоненты:

- установочные файлы клиентского решения ESET (2);
- Конфигурационный *XML*-файл для клиентских решений ESET (3).
- параметры командной строки для запуска данного пакету (4).

Раскрывающееся меню **«Тип»** в разделе (1) предоставляет доступ к дополнительным возможностям ERA. Клиентские решения ESET можно не только удаленно устанавливать, но и удаленно удалять с помощью функции **«Удаление продуктов безопасности ESET и NOD32 версии 2»**. Можно также удаленно установить внешнее приложение, выбрав пункт **Пользовательский пакет**. Это особенно полезно, если нужно запускать различные сценарии и исполняемые файлы на удаленной машине, в том числе средства для удаления сторонних продуктов безопасности или автономные средства очистки. С помощью меню **«Входной файл пакета»** можно указать пользовательские параметры командой строки. Дополнительные сведения см. в разделе Установка продуктов сторонних производителей с помощью программы ERA 103.

Каждому пакету автоматически присваивается удаленный установщик ESET — агент, который облегчает установку и обмен данными между целевыми рабочими станциями и сервером ERAS. Файл агента удаленной установки ESET называется *einstaller.exe*. Он содержит имя сервера ERAS, а также имя и тип пакета, к которому относится. Подробнее этот агент описан в следующих главах.

На процесс установки могут влиять несколько параметров. Их можно использовать как при выполнении администратором непосредственной установки на рабочей станции, так и для удаленной установки. При удаленной установке значения параметров задаются в процессе формирования установочных пакетов, а затем автоматически применяются на целевых клиентах. После имени установочного *MSI*-пакета можно вводить дополнительные параметры для ESET Smart Security и ESET NOD32 Antivirus (например, *eav_nt64_ENU.msi /qn*):

- **/qn**
  Режим автоматической установки — диалоговые окна не показываются.
- **/qb!**
  Вмешательство пользователя невозможно, но ход установки отображается на индикаторе в процентах.
- **REBOOT ="ReallySuppress"**
  Подавление перезагрузки после установки программы.
- **REBOOT ="Force"**
  Автоматическая перезагрузка после установки.
- **REBOOTPROMPT =""**
  После установки открывается диалоговое окно, предлагающее перезагрузить компьютер (этот параметр нельзя использовать вместе с параметром */qn*).
- **ADMINCFG ="путь_к_xml-файлу"**
  Во время установки к продуктам безопасности ESET применяются параметры, заданные в указанных XML-файлах. Этот параметр не требуется при удаленной установке. В установочных пакетах содержится собственная *XML*-конфигурация, применяемая автоматически.
- **PASSWORD="пароль"**
  Этот параметр необходимо добавить, если настройки ESS/EAV защищены паролем.

Параметры для ESET NOD32 Antivirus 2.x необходимо вводить после имени файла *setup.exe*, извлекаемого вместе с другими файлами из установочного пакета (например, *setup.exe /silentmode*):

- **/SILENTMODE**
  Режим автоматической установки — диалоговые окна не показываются.
- **/FORCEOLD**
  Установка старой версии поверх уже установленной новой.
- **/CFG ="путь_к_xml-файлу"**
  Во время установки к клиентским решениям ESET применяются параметры, заданные в указанных *XML*-файлах. Этот параметр не требуется при удаленной установке. В установочных пакетах содержится собственная *XML*-конфигурация, применяемая автоматически.
- **/REBOOT**
  Автоматическая перезагрузка после установки.
- **/SHOWRESTART**
  После установки открывается диалоговое окно, предлагающее перезагрузить компьютер. Этот параметр можно использовать только вместе с параметром *SILENTMODE*.
- **/INSTMFC**
  Установка библиотек MFC для операционной системы Microsoft Windows версии 9x, необходимых для правильной работы программы ERA. Этот параметр можно использовать всегда -даже если библиотеки MFC доступны.

В разделе **«Создание/выбор содержимого пакета установки»** (2) администратор может создать автономный установочный пакет с предопределенной конфигурацией из уже существующего и сохраненного установочного пакета (кнопка **«Сохранить как...»**). Такие установочные пакеты запускаются на клиентской рабочей станции, на которую нужно установить программу. Пользователю необходимо только запустить пакет, после чего продукт устанавливается автоматически без подключения к серверу ERAS во время установки.

Примечание. При добавлении конфигурации в установочный *MSI*-файл цифровая подпись этого файла больше не будет действительной.

Внимание! В системах Microsoft Windows Vista и старше настоятельно рекомендуется выполнять автоматическую удаленную установку (с параметром */qn*, */qb*). В противном случае взаимодействие с пользователем может привести к сбою удаленной установки из-за превышения интервала ожидания.

4.2.1 Требования

Основным требованием для удаленной установки является правильно настроенная сеть TCP/IP, обеспечивающая надежную связь между клиентом и сервером. При установке клиентского решения с помощью программы ERA к клиентской рабочей станции предъявляются более строгие требования, чем при непосредственной установке. Для удаленной установки должны выполняться следующие требования:

- включен клиент сети Microsoft;
- включена служба «Общий доступ к файлам и принтерам»;
- открыты порты общего доступа к файлам (445, 135-139);
- активирован протокол TCP/IP;
- включен административный общий ресурс ADMIN$;
- клиенты могут отвечать на PING-запросы;
- существует возможность обмена данными между сервером ERAS и консолью ERAC (открыты порты 2224-2224);
- для клиентских рабочих станций существуют имя пользователя и пароль учетной записи администратора (имя пользователя не может быть пустым);
- отключена служба «Простой общий доступ к файлам»;
- включена служба «Сервер»;
- включена служба «Удаленный реестр».

ПРИМЕЧАНИЕ.: В последних версиях ОС Microsoft Windows (Windows Vista, Windows Server 2008 и Windows 7) используются политики безопасности, ограничивающие разрешения учетной записи локального пользователя, то есть пользователь может быть не в состоянии выполнять определенные сетевые действия. Если служба ERA работает в учетной записи локального пользователя, в некоторых конфигурациях сети могут возникнуть проблемы с запуском установки (например, при удаленной установке из домена в рабочей группе). В системах Windows Vista, Windows Server 2008 или Windows 7 рекомендуется запускать службу ERA с достаточными разрешениями доступа к сети. Чтобы указать учетную запись пользователя, от имени которой будет выполняться служба ERA, выберите команду **«Пуск»** → **«Панель управления»** → **«Административные задачи»** → **«Службы»**. Выберите службу ESET Remote Administrator Server в списке и щелкните вкладку **«Вход от имени»**. ESET Remote Administrator 4 встраивает этот параметр в сценарии расширенной установки, поэтому во время установки необходимо выбрать **«Дополнительно»** → **«Полностью настраиваемая установка»**. При автоматической установке на целевых рабочих станциях под управлением Windows Vista, Windows Server 2008 или Windows 7 убедитесь в том, что они и сервер ERA Server находятся в домене.

Перед установкой настоятельно рекомендуется проверить все требования, особенно если в сети есть несколько рабочих станций (на вкладке **«Удаленная установка»** щелкните вкладку **«Компьютеры»**, щелкните правой кнопкой мыши соответствующий клиент и выберите в контекстном меню пункт **«Диагностика автоустановки»**).

4.2.2 Настройка среды удаленной установки

Перед установкой продуктов безопасности ESET на сетевые компьютеры администратор должен надлежащим образом подготовить среду, чтобы не допустить сбоев при установке.

В разделе **«Вид сети»** на вкладке **«Удаленная установка»** представлен настраиваемый вид сети. Существует два способа просмотра сети.

Консоль

В представлении **«Консоль»** доступен стандартный поиск NetBios с компьютера, на котором установлена консоль ERAC. В нем отображаются все доступные домены и рабочие группы, которые можно выбрать (или отменить выбор) для фильтрации вида.

Сервер

В представлении **«Сервер»** доступны дополнительные параметры фильтрации. Помимо поиска NetBios можно просматривать компьютеры в каталоге Active Directory, существующих клиентов ERA, а также создавать собственные пользовательские фильтры.

Пользовательские фильтры содержат два элемента — **«Пользовательский список»** и **Поиск IP**, — которые позволяют вручную создавать свои группы.
В **пользовательском списке** можно вручную добавлять компьютеры в группу, указав их имена в разделе **«Компьютеры в группе»** или путем импорта их из *TXT*-файла. В обоих случаях имена компьютеров должны

быть указаны в виде списка один за одним.
Раздел **«Поиск IP»** позволяет создавать диапазоны IP-адресов компьютеров и группы IP-адресов компьютеров, где диапазон IP служит критерием фильтрации.

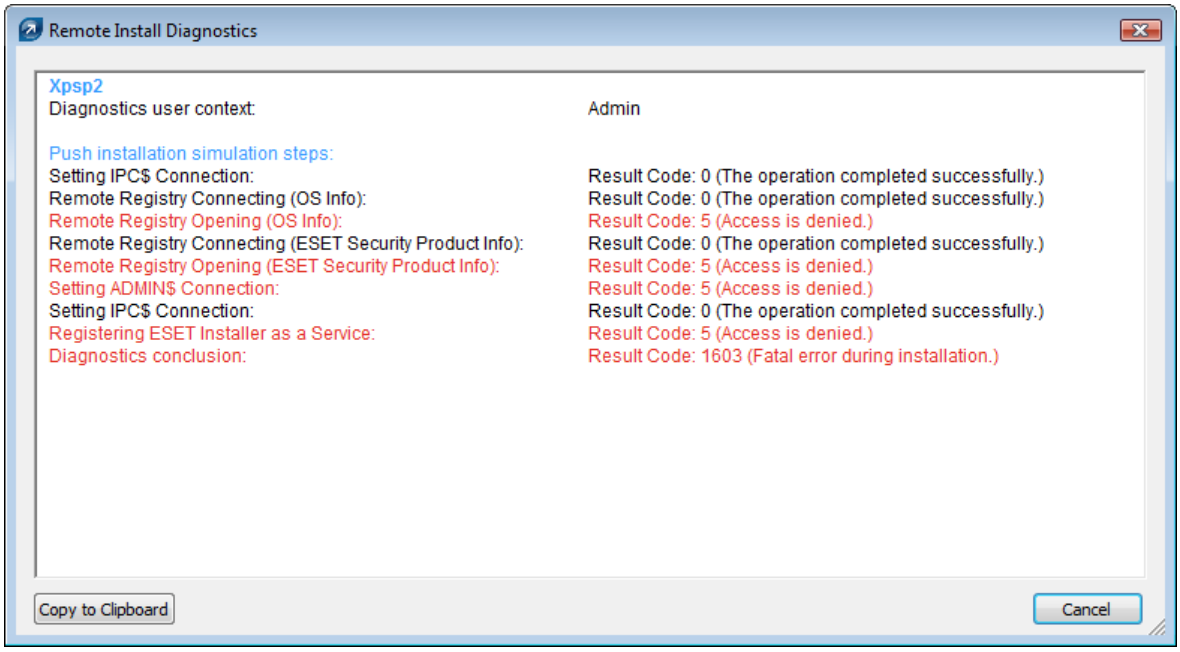
Примечание. Ветки Консоль/Сервер определяют, откуда просматриваются компьютеры — из ERAS ил ERAC. Это рекомендуется учитывать при подключении к серверу ERAS из другой сети.

Раздел **«Параметры фильтрации»** содержит два дополнительных параметра фильтрации:

«Незарегистрированные компьютеры» — отображение компьютеров, не указанных в базе данных текущего сервера;

«Клиенты с предупреждением о последнем подключении» — отображение компьютеров, указанных в базе данных текущего сервера, и для которых есть предупреждение о последнем подключении.

После настройки всех необходимых условий в разделах **«Вид сети»** и **«Параметры фильтрации»** в правой части окна на вкладке **«Компьютеры»** можно просмотреть список рабочих станций, подходящих для установки клиентского решения. Можно запустить диагностику удаленной установки на компьютерах, которые были обнаружены и отображаются в списке, щелкнув правой кнопкой мыши нужный компьютер и выбрав в контекстном меню пункт **«Диагностика автоустановки»**. Диагностика помогает проверить требования к установке и определить возможные проблемы.



4.2.3 Удаленная автоматическая установка

При использовании этого способа удаленной установки клиентские решения ESET передаются на удаленные компьютеры. Удаленные компьютеры должны находиться в сети во включенном состоянии. Если все рабочие станции включены, наиболее эффективным является метод автоматической установки является. Перед началом автоматической установки необходимо загрузить с веб-узла ESET установочные файлы с расширением для ESET Smart Security или ESET NOD32 Antivirus и создать пакет установки. Можно создать XML-файл конфигурации, который будет применяться автоматически при запуске данного пакета. Перед установкой прочтите раздел Требования 41.

Для запуска автоматической установки выполните перечисленные ниже действия.

1) После подготовки компьютеров к удаленной установке на вкладке **«Компьютеры»** выберите все или несколько компьютеров и запустите задачу автоматической установки, щелкнув окно правой кнопкой мыши и выбрав в контекстном меню пункт **«Автоматическая установка»**.

2) Укажите учетные данные для компьютеров в списке (**«Задать»**, **«Задать все»**). Это должно быть сделано с использованием учетной записи с правами администратора. На этом этапе можно еще добавить клиентов в список с помощью функции **«Специальное добавление клиентов»**.

3) Выберите установочный пакет, который нужно отправить на рабочие станции.

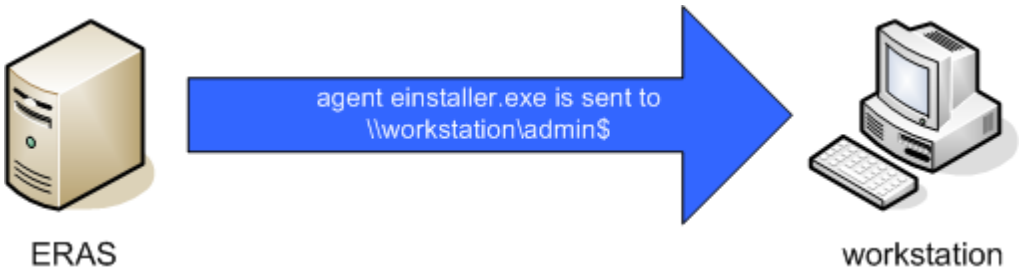
4) Задайте время запуска задачи и нажмите кнопку **«Готово»**.

Состояние задачи автоматической установки отображается на вкладке **«Задачи установки»**. Для просмотра более подробных результатов диагностики выберите нужное задание и нажмите клавишу F4. В окне **«Свойства»** есть вкладка **«Детали**, в которой можно просмотреть результаты диагностики удаленной установки, нажав кнопку **«Просмотреть выбранные журналы/Просмотреть все журналы»**.

Примечание. Максимальное количество одновременных потоков автоустановки по умолчанию равно 20. При отправке задачи автоматической установки на несколько компьютеров, превышающих этот предел, дополнительные компьютеры будут поставлены в очередь, ожидая освобождения потока. Не рекомендуется увеличивать это значение, чтобы не снизилось быстродействие. Однако при необходимости это ограничение можно изменить в редакторе конфигураций (**ESET Remote Administrator** > **ERA Server** > **«Настройка»** > **«Удаленная установка»**).

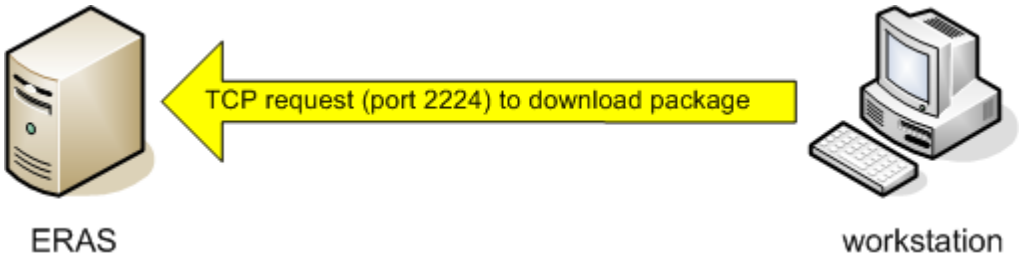
Ниже подробно описан процесс удаленной установки.

5) Сервер ERAS отправляет агент *einstaller.exe* на рабочую станцию с использованием административного общего ресурса admin$.

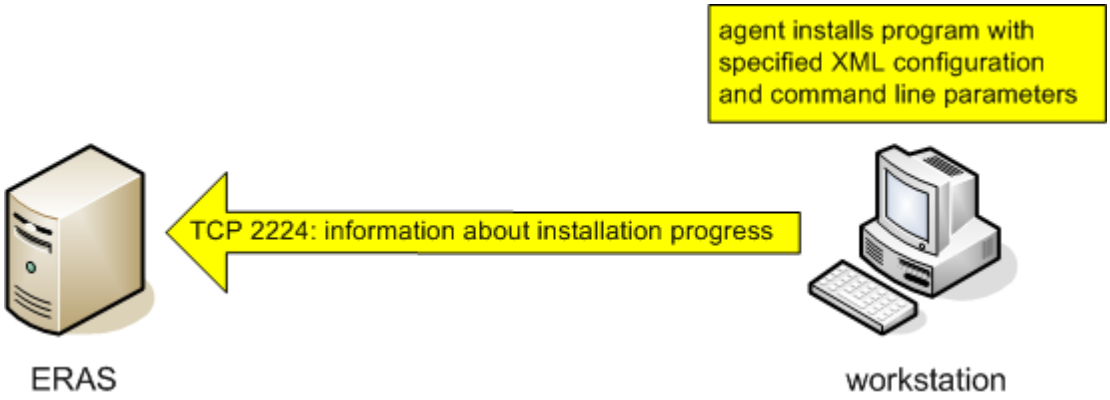


6) Агент запускается как служба с правами учетной записи системы.

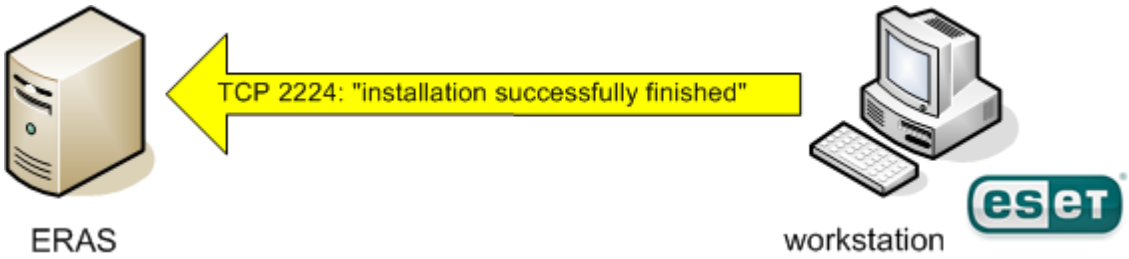
7) Агент устанавливает соединение с «родительским» сервером ERAS и загружает соответствующий установочный пакет по TCP-порту 2224.



Агент устанавливает пакет с учетной записью администратора, выбранной на шаге 2. При этом также применяется соответствующая *XML*-конфигурация и параметры командной строки.



9) Завершив установку, агент немедленно отправит сообщение на сервер ERAS. Некоторые продукты безопасности ESET предлагают в случае необходимости перезагрузить компьютер.



В контекстном меню (вызываемом щелчком правой кнопкой мыши) вкладки **«Компьютеры»** доступны указанные ниже команды.

- **«Управление пакетами»**
  Запускает **редактор установочных пакетов**. Дополнительные сведения см. в разделе Удаленная установка 38.

- **«Обновление клиента»**
  Запускает задачу обновления. Используйте эту команду, если необходимо установить новую версию ESS/EAV поверх старой.

- **«Диагностика автоустановки»**
  Проверка доступности клиентов и служб, которые будут использоваться в ходе удаленной установки. Дополнительные сведения см. в разделе Настройка среды удаленной установки 41.

- **«Автоматическая установка»**
  Запускает задачу автоматической установки.

- **«Экспорт в папку или в сценарий входа»**
  Дополнительные сведения см. в разделе Удаленная установка с использованием сценария входа или электронной почты 45.

- **Отправка по электронной почте**
  Дополнительные сведения см. в разделе Удаленная установка с использованием сценария входа или электронной почты 45.

- **Установить вход по умолчанию**
  Открывает окно **Вход по умолчанию**, где можно указать имя и пароль учетной записи администратора для целевых компьютеров.

- **Свойства**
  Открывает окно **Свойства клиента**, содержащее важные сведения о клиенте.

Описание других команд контекстного меню см. в разделе Контекстное меню 24.

4.2.4 Удаленная установка с использованием сценария входа или электронной почты

Эти способы удаленной установки очень похожи. Единственным отличием является способ отправки агента *einstaller.exe* на клиентские рабочие станции. Программа ERA позволяет запускать агент с помощью сценария входа или по электронной почте. Агент *einstaller.exe* также можно использовать отдельно и запускать другими способами (дополнительные сведения см. в разделе Пользовательская удаленная установка 47).
Установка с использованием сценария входа хорошо подходит для ноутбуков, которые часто находятся за пределами локальной сети. Установка происходит после их входа в домен. Для этих устройств рекомендуется применять сценарии входа.

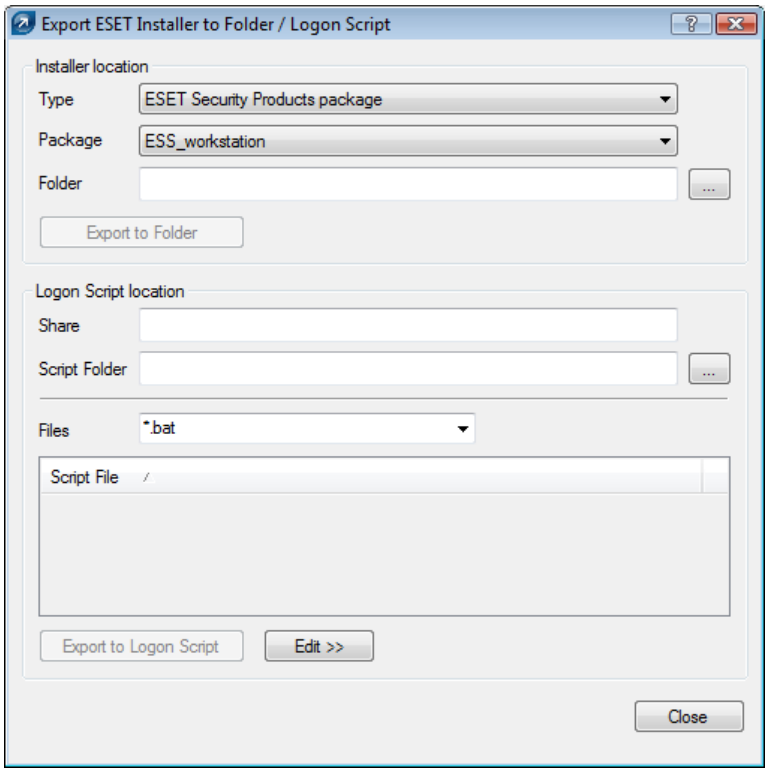
Сценарий входа выполняется автоматически при входе в систему, а для удаленной установки с помощью электронной почты требуется вмешательство пользователя, который должен запустить агент einstaller.exe, содержащийся во вложении в письмо При повторном запуске агент einstaller.exe не инициирует повторную установку клиентского решения ESET. Дополнительные сведения см. в разделе Как избежать повторных установок 48.

Команду вызова агента *einstaller.exe* из сценария входа можно вставить с помощью текстового редактора или другой подходящей программы. Аналогичным образом, агент *einstaller.exe* можно отправлять в виде вложения с помощью почтового клиента. Вне зависимости от используемого способа убедитесь в том, что используется правильный файл *einstaller.exe*.

Для запуска агента *einstaller.exe* вошедшему в систему пользователю не обязательно иметь права администратора. Агент получает требуемые имя пользователя, пароль и домен учетной записи администратора с сервера ERAS. Дополнительные сведения см. в конце этой главы.

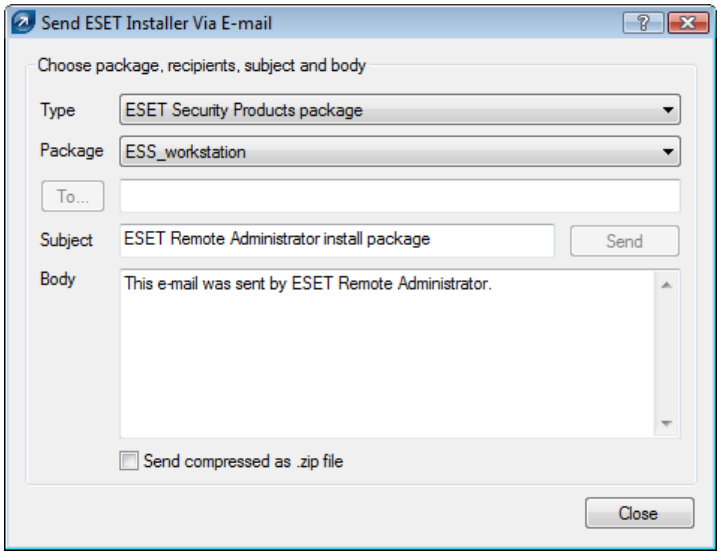
Укажите в сценарии входа путь к файлу *einstaller.exe*.

1) На вкладке **«Удаленная установка»**нажмите кнопку **«Экспорт в папку или в сценарий входа»** и выберите **тип** и название **пакета**, который нужно установить.
2) Нажмите кнопку «...» справа от поля **«Папка»** и выберите каталог, в котором будет находиться и будет доступен в сети файл *einstaller.exe*, и нажмите кнопку **ОК**.
3) Убедитесь в том, что в поле **«Общий доступ»** указан правильный путь; при необходимости исправьте его.
4) Нажмите кнопку **...** справа от поля **«Папка сценария»**, чтобы выбрать папку, в которой находится сценарий, и при необходимости измените маску (**«Файлы»**).
5) В разделе **«Файлы»** выберите файл, в который нужно вставить строку, вызывающую файл *einstaller.exe*.
6) Нажмите кнопку **«Экспорт в сценарий входа»**, чтобы вставить строку.
7) Местонахождение строки можно изменить, нажав кнопку **«Изменить >>»** и сохранив файл с помощью кнопки **«Сохранить»**.

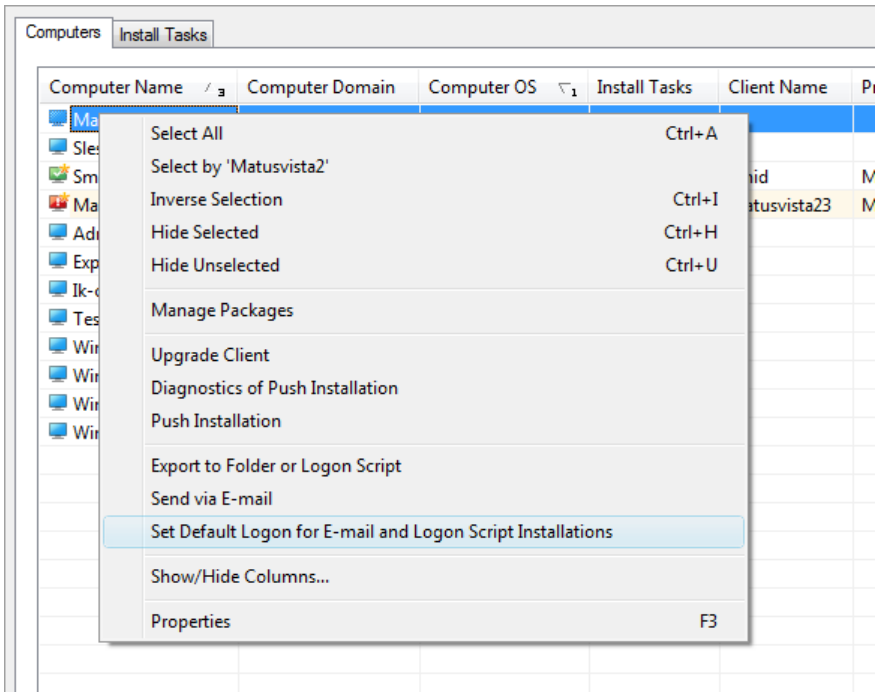


Вложение агента (*einstaller.exe*) в сообщение электронной почты

1) На вкладке **«Удаленная установка»** нажмите кнопку **«Электронная почта»** и выберите **тип** и название **пакета** для установки.
2) Нажмите кнопку **Кому**, чтобы выбрать адреса из адресной книги (или введите адреса вручную).
3) Введите **тему** в соответствующем поле.
4) Введите текст сообщения в поле **«Текст»**.
5) Установите флажок **«Отправить файл, сжатый в формате .zip»**, чтобы отправить агент в сжатом ZIP-архиве.
6) Нажмите кнопку **«Отправить»**, чтобы отправить сообщение.



В ходе удаленной установки устанавливается обратное подключение к серверу ERAS и агент (*einstaller.exe*) использует параметры, заданные на вкладке «Удаленная установка» в разделе **«Установить вход по умолчанию для электронной почты и сценария входа»**.



Имя пользователя и пароль учетной записи, с использованием которой будет установлен пакет, должны принадлежать учетной записи администратора локального компьютера или домена. После каждой перезагрузки службы сервера ERAS значения, введенные в диалоговое окно **«Вход по умолчанию...»**, теряются.

4.2.5 Пользовательская удаленная установка

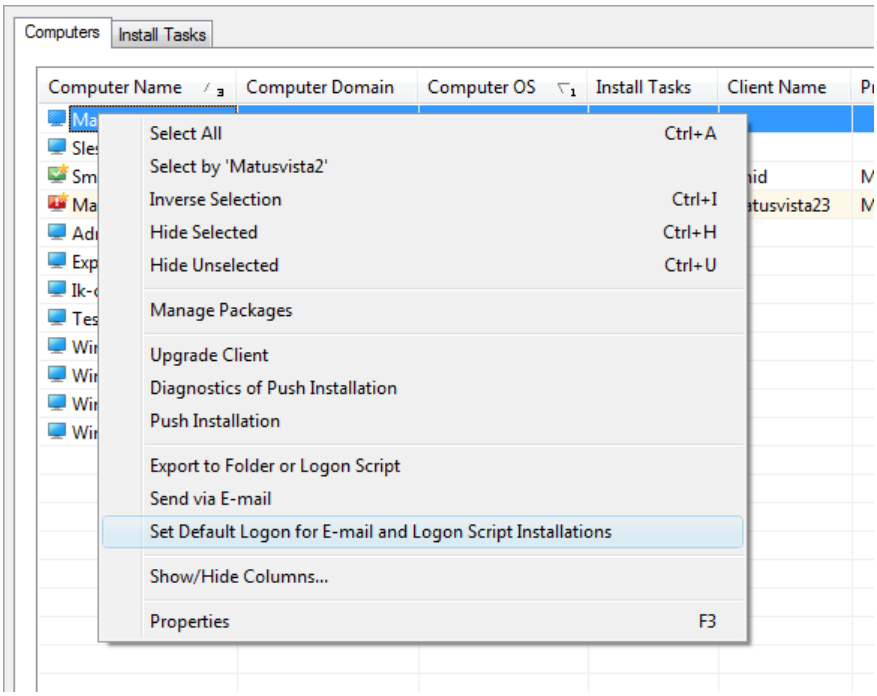
Для удаленной установки клиентских решений ESET не обязательно использовать средства ERA. В конечном итоге самым важным аспектом является доставка и запуск файла *einstaller.exe* на клиентских рабочих станциях.

Для запуска агента *einstaller.exe* вошедшему в систему пользователю не обязательно иметь права администратора. Агент получает требуемые имя пользователя, пароль и домен учетной записи администратора с сервера ERAS. Дополнительные сведения см. в конце этой главы.

Файл *einstaller.exe* можно получить следующим образом.

- На вкладке **«Компьютеры»** (на вкладке **«Удаленная установка»**) щелкните правой кнопкой мыши пустое место, в контекстном меню **«Экспорт в папку или в сценарий входа»** выберите пункт **«Тип»** и имя **пакета** для установки.
- Нажмите кнопку **...** рядом с полем **«Папка»** и выберите каталог, в который будет экспортирован файл *einstaller.exe*.
- Нажмите кнопку **«Экспорт в папку»**.
- Используйте распакованный файл *einstaller.exe*.

Примечание. *Прямая установка с предопределенной XML-конфигурацией* используется в ситуациях, когда для установки можно получить права администратора. *MSI*-пакет запускается с параметрами */qn* (версия 4.x и 3.x) или */silentmode* (версия 2.x). Эти параметры позволяют выполнять установку без соответствующего интерфейса пользователя.



Имя пользователя и пароль учетной записи, с использованием которой будет установлен пакет, должны принадлежать учетной записи администратора локального компьютера или домена.

В ходе удаленной установки устанавливается обратное подключение к серверу ERAS и агент (*einstaller.exe*) использует параметры, заданные в разделе **«Установить вход по умолчанию для электронной почты и сценария входа»**.

Если агент *einstaller.exe* запускается на целевой рабочей станции вручную, удаленная установка выполняется следующим образом.

- Агент *einstaller.exe* отправляет запрос на сервер ERAS (TCP-порт 2224).
- Сервер ERAS запускает новый сеанс автоматической установки (с новым агентом) соответствующего пакета (отправляемого через общий ресурс *admin$*). Агент ожидает ответа от сервера ERAS (отправки пакета в общий ресурс *admin$*). При отсутствии ответа агент попытается загрузить установочный пакет (через TCP/IP-порт 2224). В этом случае имя пользователя и пароль учетной записи администратора, указанные в разделе **«Удаленная установка» > «Вход...»** на сервере ERAS, не передаются, поэтому агент пытается установить пакет с использованием учетной записи текущего пользователя. В операционных системах Microsoft

Windows 9x/Me нельзя использовать общий административный ресурс, поэтому агент автоматически устанавливает прямое подключение к серверу по протоколу TCP/IP. Затем новый агент начинает загрузку пакета с сервера ERAS по протоколу TCP/IP.

При запуске установки пакета применяются параметры из XML-файла под учетной записью, указанной на сервере ERAS (кнопка **«Установить вход по умолчанию»**).

4.2.6 Обновление

Этот тип установки предназначен для клиентов с ESS/EAV версии 4.2 и выше. Начиная с версии 4.2, в ERA был реализован новый механизм обновления, который позволяет запускать процесс обновления на стороне клиента без агента *einstaller.exe*. Этот механизм работает по аналогии с обновлением компонентов программы (PCU), при котором клиенты обновляются до более новой версии программы. Для клиентов ESS/EAV версии 4.2 и старше настоятельно рекомендуется использовать этот тип обновления.

Примечание. Если для установочного пакета был определен пользовательский файл конфигурации, он будет игнорировать во время обновления.

4.2.7 Как избежать повторных установок

Сразу после завершения удаленной установки агент помечает удаленный клиент флажком, запрещающим повторно использовать тот же самый установочный пакет. Этот флажок записывается в следующий ключ реестра:

HKEY_LOCAL_MACHINE\Software\ESET\ESET Remote Installer

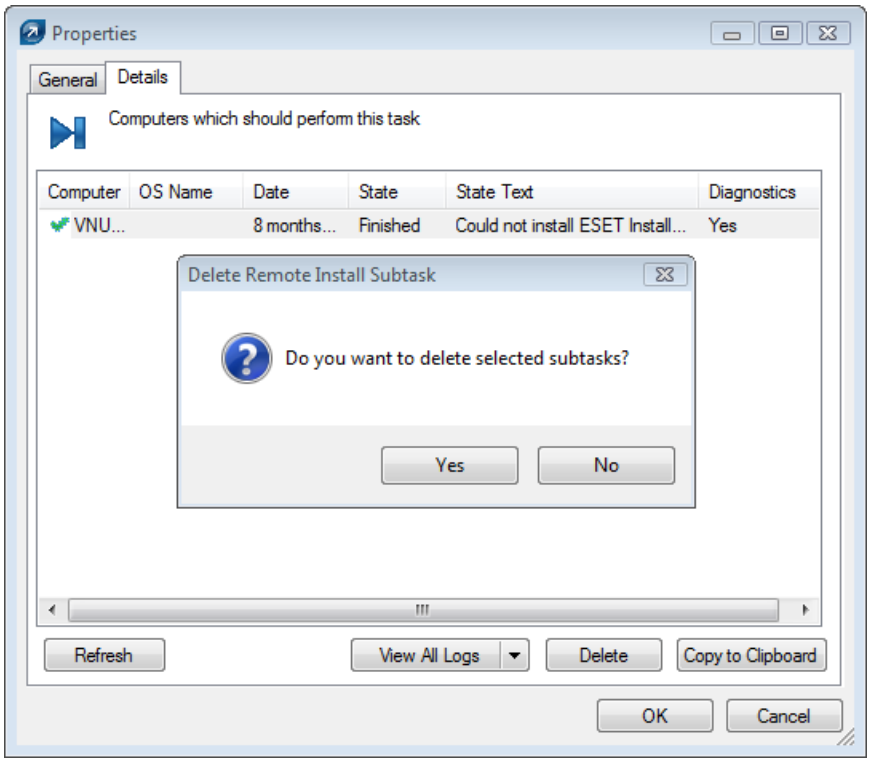
Если тип и название пакета, заданные в агенте *einstaller.exe*, совпадают с данными в реестре, установка не выполняется. Это предотвратит повторные установки на целевых рабочих станциях.

Примечание. При удаленной автоматической установке содержимое этого раздела реестра не принимается во внимание.

Сервер ERAS обеспечивает дополнительный уровень защиты от повторных установок, реализуемый в момент установки программой обратного соединения с сервером ERAS (TCP 2224). При выводе сообщения об ошибке, связанного с данной рабочей станцией, или после успешного завершения установки дополнительные попытки установки отклоняются.

Агент записывает следующую ошибку в журнал установщика *%TEMP%\einstaller.log*:

Программа установки ESET получила сообщение от сервера „X:2224" о выходе;



чтобы предотвратить отклонение повторных установок сервером ERAS, необходимо удалить соответствующие записи на вкладке **«Данные задачи удаленной установки»**. Чтобы удалить запись, выделите ее, нажмите кнопку **«Удалить»** и подтвердите действие, нажав кнопку **«Да»**.

4.3 Установка в корпоративной среде

При развертывании программ в больших сетях важно использовать средство, способное выполнять удаленную установку программ на всех компьютерах в сети.

Установка с использование групповой политики

В среде Active Directory эту задачу можно хорошо решить посредством установки с использованием групповой политики. Во время установки используется MSI-установщик, который непосредственно рассылается на все компьютеры, подключенные к домену с использованием групповой политики.

Чтобы настроить в контроллере домена автоматическую установку приложений ESET Smart Security или ESET NOD32 Antivirus на всех рабочих станциях после входа в систему, выполните следующие действия.

1) Создайте общую папку в контроллере домена. Все рабочие станции должны иметь к ней доступ для чтения.

2) Скопируйте установочный *MSI*-пакет ESET NOD32 Antivirus или ESET Smart Security в эту папку.

3) Переместите в эту папку *XML*-файл конфигурации, который нужно применить к данной программе. Файл должен называться *cfg.xml*. Для создания файла конфигурации можно использовать ESET Configuration Editor. Дополнительные сведения см. в разделе ESET Configuration Editor 34.

4) Выберите команду **«Пуск** > **«Программы** > **«Администрирование** > **«Пользователи и компьютеры службы Active Directory»**.

5) Щелкните правой кнопкой мыши имя домена и выберите команду **«Свойства»** > **«Политика группы»** > **«Изменить»** > **«Конфигурация пользователя»**.

6) Щелкните правой кнопкой мыши пункт **«Настройка ПО»** и выберите команду **«Новый»** > **«Пакет»**.

7) В окне **«Открыть»** укажите путь в формате UNC к общему установочному пакету, то есть *имя_компьютера**путь**установочный_пакет.msi* и нажмите кнопку **«Открыть»**. Не используйте параметр **«Обзор»** для поиска установочного пакета, потому что в этом случае он будет отображаться как путь в локальной сети, а не как UNC-путь.

8) В следующем диалоговом окне выберите параметр **«Присвоено»**. Нажмите кнопку **ОК**, чтобы закрыть окно.

С помощью этих действий установочный пакет можно устанавливать на все компьютеры, которые входят в домен. Для установки пакета на подключенных компьютерах необходимо их отключить и снова подключить.

Если пользователям нужно дать возможность принятия или отклонения установки пакета, выберите **«Опубликовать»** вместо **«Присвоено»** на шаге 8. При следующем входе в систему пакет будет добавлен в раздел **«Панель управления»** > **«Установка и удаление программ»** > **«Установка новой программы»** > **«Установка программ из сети»**. В этом случае в будущем этот пакет можно будет устанавливать из данного места.

5. Управление клиентскими компьютерами

5.1 Задачи

Для настройки и администрирования клиентских рабочих станций, которые надлежащим образом подключены к серверу ERAS и отображаются на консоли ERAC, можно использовать различные типы задач.

Общий рабочий процесс, показанный ниже, применяется ко всем задачам, описанным в следующих подразделах, за исключением подраздела Интерактивная задача 54 (см. в разделе описание рабочего процесса).

Этап I. **«Новая задача»**

Задачи можно применять к нескольким клиентам либо к одной или нескольким группам клиентов.

1) Чтобы применить задачу к одной или нескольким клиентским рабочим станциям, щелкните их правой кнопкой мыши на панели **«Клиенты»**.

2) Нажмите кнопку **«Новая задача»** и выберите вид задачи, которую нужно выполнить.

   Примечание. Кроме того, мастер задач можно запустить с помощью команды главного меню консоли ERAC **«Действия» > «Новая задача»**.

Этап II. Выберите одну из следующих задач:

3) После выбора нужной задачи необходимо выполнить действия, описанные в каждом из разделов (см. по ссылкам выше).

Этап III. **«Выбор клиентов»**

4) После настройки задачи в появившемся окне **«Выбор клиентов»** можно изменить выбор клиентов. Выбор клиентов можно изменить путем добавления клиентов из дерева **«Все элементы»** (в левой половине окна) в список **«Выбранные элементы»** (в правой половине окна) или путем удаления клиентов, которые уже есть в списке.

   Примечание. Нажмите кнопку **«Добавить специальное...»**, чтобы открыть новое окно, в котором можно добавить клиентов с панели **«Клиенты»** или **«Сервер»** и/или **«Группы»**.

Этап IV. **«Отчет по задаче, Готово»**

5) Последнее диалоговое окно (**«Отчет по задаче»**) предназначено для предварительного просмотра задачи конфигурации. Введите название или описание задачи (необязательно). Параметр **«Применить в»** позволяет назначить запуск задачи на указанное время или дату. Параметр **«Очищать задачи автоматически при успешном выполнении»** удаляет все задачи, которые были успешно доставлены на конечные рабочие станции.

6) Нажмите кнопку **«Готово»**, чтобы поместить задачу на исполнение.

В следующих подразделах дается краткое описание отдельных типов задач для клиентских рабочих станций, каждый из которых сопровождается образцом сценария.

5.1.1 Задача конфигурации

Задачи конфигурации используются для изменения настроек защиты на клиентских рабочих станциях. Эти задачи доставляются на клиентские рабочие станции в конфигурационных пакетах, содержащих параметры изменений. *XML*-файлы, созданные в ESET Configuration Editor или экспортированные из клиентов, также совместимы с задачами конфигурации. Ниже приведен пример создания задачи конфигурации, изменяющей имя пользователя и пароль на целевых компьютерах. Все переключатели и параметры, не использующиеся в этом примере, будут описаны в конце этой главы.

Сначала выберите рабочие станции, на которые необходимо доставить задачу. Отметьте эти рабочие станции на панели **«Клиенты»** в консоли ERAC.

1) Щелкните правой кнопкой мыши по любой из выделенных рабочих станций и выберите в контекстном меню пункт **«Новая задача»** > **«Задача конфигурации»**.

2) Откроется окно **«Конфигурация для клиентов»**, которое является мастером задачи конфигурации. Чтобы указать источник конфигурации, нажмите кнопку **«Создать»**, **«Выбрать»** или **«Создать из шаблона...»**.

3) Нажмите кнопку **«Создать**, чтобы открыть ESET Configuration Editor, и выберите применяемую конфигурацию. Выберите в меню **ESET Smart Security**, **ESET NOD32 Antivirus** > **«Модуль обновления»** > **«Профиль»** > **«Настройка»** > **«Имя пользователя»** и **«Пароль»**.

4) Введите предоставленные компанией ESET имя пользователя и пароль и нажмите находящуюся справа кнопку **«Консоль»** для возврата в мастер задачи. В поле **«Создать/Выбрать конфигурацию»** отобразится путь к пакету.

5) Если уже имеется файл с необходимыми изменениями, нажмите кнопку **«Выбрать»**, найдите файл и назначьте его задаче конфигурации.

6) Также можно нажать кнопку **«Создать из шаблона»**, выбрать *XML*-файл и внести необходимые изменения.

7) Нажмите кнопку **«Просмотр»** или **«Изменить»** для просмотра или изменения только что созданного или измененного файла конфигурации.

8) Нажмите кнопку **«Далее»** для перехода в окно **«Выбор клиентов»**, содержащем список рабочих станций, на которые будет доставлена задача. На этом этапе можно добавить добавить клиенты (или из выбранных серверов или групп). Нажмите кнопку **«Далее»** для перехода к следующему этапу.

9) Последнее диалоговое окно (**«Отчет по задаче»**) предназначено для предварительного просмотра задачи конфигурации. Введите название или описание задачи (необязательно). Параметр **«Применить в»** позволяет назначить запуск задачи на указанное время или дату. Параметр **«Очищать задачи автоматически при успешном выполнении»** удаляет все задачи, которые были успешно доставлены на конечные рабочие станции.

10) Нажмите кнопку **«Готово»**, чтобы поместить задачу на исполнение.

5.1.2 Задача сканирования по требованию

В контекстном меню **Новая задача** есть два варианта сканирования по требованию. В первом варианте — **Сканирование по требованию (очистка отключена)** — просто создается журнал, а зараженные файлы остаются без изменений. Второй вариант — **Сканирование по требованию (очистка включена)**.

В окне **Сканирование по требованию** для обоих вариантов доступны одни и те же настройки по умолчанию, за исключением параметра **Сканировать без очистки**. Этот параметр включает или отключает очистку зараженных файлов при сканировании. Ниже приведен пример создания задачи «Сканирование по требованию».

1) В раскрывающемся меню **Раздел конфигурации** можно выбрать тип продукта ESET, для которого назначается задача сканирования по требованию. Следует выбирать только продукты, установленные на целевых рабочих станциях.

   Примечание. Параметр **Исключить этот раздел из сканирования по требованию** отключает все настройки в окне для выбранного типа продуктов — они не будут применяться на рабочих станциях с продуктом, указанным в разделе **Конфигурация**. Таким образом, все клиенты с указанным продуктом

исключаются из списка получателей задачи. Если администратор отмечает клиентов как получателей и исключает продукт с помощью этого параметра, задача завершается неудачей с уведомлением о том, что ее не удалось применить. Во избежание этого администратору всегда следует указывать клиенты, которым назначается соответствующая задача.

2) В поле **Название профиля** можно выбрать профиль сканирования, который нужно применить к задаче.

3) В разделе **Диски** выбираются типы дисков, проверяемых на клиентских компьютерах. Если предлагаемый выбор слишком общий, можно указать точный путь к проверяемым объектам. Для этого используется поле **Путь** или кнопка **Добавить путь**. Параметр **Очистить историю** позволяет восстановить исходный список проверяемых дисков.

4) Нажмите кнопку **Далее**, чтобы перейти к окнам **Выбор клиентов** и **Отчет по задаче**, которые подробно описаны в разделе Задачи 50.

5) После выполнения задачи на клиентских рабочих станциях результаты отправляются обратно серверу ERAS и отображаются в ERAC на панели **Журнал сканирования**.

5.1.3 Задача «Обновить сейчас»

Предназначением этой задачи является принудительное обновление рабочих станций (обновляется база данных сигнатур вирусов и программные компоненты).

1) На вкладке **Клиенты** щелкните правой кнопкой мыши по любой рабочей станции и выберите команду **Новая задача** > **Обновить сейчас**.

2) Если нужно исключить из задачи определенные виды продуктов безопасности ESET, выберите их в раскрывающемся меню **Раздел конфигурации** и установите параметр **Исключить данный раздел из задачи обновления**.

3) Чтобы использовать для задачи **Обновить сейчас** определенный профиль обновления, установите флажок **Выбрать название профиля** и выберите необходимый профиль. Также можно установить флажок **Пользовательское имя профиля** и ввести название профиля. Кнопка **Очистить историю** возвращает значение поля по умолчанию.

4) Нажмите кнопку **Далее**, чтобы перейти к диалоговым окнам **Выбор клиентов** и **Отчет по задаче**. Описание этих окон см. в разделе Задачи 50.

5.1.4 Задача «Сценарий SysInspector»

Задача «Сценарий SysInspector» позволяет запускать сценарии на конечных компьютерах. Он предназначен для удаления из системы нежелательных объектов. Дополнительную информацию см. в справке по ESET SysInspector 104.

1) После выполнения первого и второго этапов, описанных в разделе Задачи 50, нажмите кнопку **«Выбрать»**, чтобы выбрать сценарий для запуска на целевой рабочей станции.

2) Чтобы настроить сценарий, нажмите кнопку **«Просмотреть и изменить»**.

3) Нажмите кнопку **«Далее»**, чтобы перейти к окнам **«Выбор клиентов»** и **«Отчет по задаче»**, которые подробно описаны в разделе Задачи 50.

4) По окончании выполнения задачи на рабочей станции данные отобразятся в столбце **«Состояние»** на панели **«Задачи»**.

Примечание. Задачи сценариев SysInspector поддерживаются только в продуктах ESET Smart Security/ESET NOD32 Antivirus версии 4.0 и выше.

5.1.5 Задача «Восстановить или удалить из карантина»

С помощью этой задачи можно восстанавливать или удалять помещенные в карантин объекты с помощью клиента.

1) После открытия окна **Восстановление или удаление из карантина** (см. раздел Задачи 50) щелкните переключатель **Восстановить/Удалить** в зависимости от типа действия, выполняемого для изолированного объекта.

   Примечание. При восстановлении изолированного объекта, который по-прежнему определяется как угроза, возможно потребуется также установить флажок **Добавить исключение**, потому что противном случае антивирус может заблокировать действие или добавить объект обратно в карантин.

2) Выберите условие, чтобы указать изолированные объекты, которые нужно восстановить или удалить, и нажмите кнопку «Далее».

   Примечание. Если диалоговое окно «Восстановление или удаление из карантина» открыто из окна карантина щелчком правой кнопкой мыши непосредственно на вкладке «Карантин» (и с выбором параметра **Задача «Восстановить или удалить из карантина»**), вам не нужно указать условия (параметр **По хэшу** будет автоматически выбран, а в качестве идентификатора будет использован хэш изолированного файла).

3) Выберите клиентов для операции восстановления или удаления (см. раздел. Задачи 50) и нажмите кнопку **Далее**.

4) Проверьте параметры в окне **Отчет по задаче**, дайте название задаче, укажите время применения задачи и задайте параметры очистки (если необходимо) и нажмите кнопку **Готово** для подтверждения. Дополнительные сведения см. в разделе Задачи 50.

5.1.6 Задача «Создать журнал аудита безопасности»

Данная задача применима только к ESET Mobile Security.

Проверки безопасности: заряд аккумулятора, состояние Bluetooth, свободное место на диске, видимость устройства, домашняя сеть и выполняемые процессы. Будет создан подробный отчет, показывающий, не опустилось ли значение элемента ниже установленного порога или может ли это представлять потенциальную угрозу безопасности (например, устройство стало видимым и т.д.).

Включение аудита безопасности на телефоне
1) Щелкните правой кнопкой мыши имя клиента на панели **«Клиенты»** и выберите в контекстном меню команду **«Новая задача»** > **«Создать журнал аудита безопасности»**.
2) Затем нажмите кнопку **«Далее»**, чтобы перейти к диалоговым окнам **«Выбор клиентов»** и **«Отчет по задаче»** . Описание этих окон см. в разделе Задачи 50.

5.1.7 Задача «Показать уведомление»

Данная задача применима только к ESET Mobile Security.

Отправка уведомления (например, предупреждения) на телефон:
1) Щелкните правой кнопкой мыши имя клиента на панели **«Клиенты»** и выберите в контекстном меню команду **«Новая задача»** > **«Показать уведомление»**.
2) Введите **заголовок** уведомления и **текст** сообщения в соответствующих полях и установите уровень **детализации** уведомления.
3) Затем нажмите кнопку **«Далее»**, чтобы перейти к диалоговым окнам **«Выбор клиентов»** и **«Отчет по задаче»** . Описание этих окон см. в разделе Задачи 50.

5.1.8 Интерактивная задача

Эта задача отличается от других описанных здесь задач способом выполнения и используемым приложением.

На вкладке **Клиенты** отображается столбец **Текст состояния защиты** с данными состояния защиты всех подключенных клиентов ESET. Пустое поле означает, что для состояния защиты конкретного клиента установлен уровень **Максимальная степень защиты**. Если уровень защиты клиента меньше максимального, в столбце **Текст состояния защиты** (например, **Персональный файервол ESET отключен**) появится предупреждение о состоянии защиты красного или оранжевого цвета.

ERA позволяет администратору контролировать эти параметры на вкладке **Клиенты**.

1) Щелкните дважды запись клиента на вкладке **Клиент**.

2) В окне **Свойства** щелкните вкладку **Состояние защиты**.

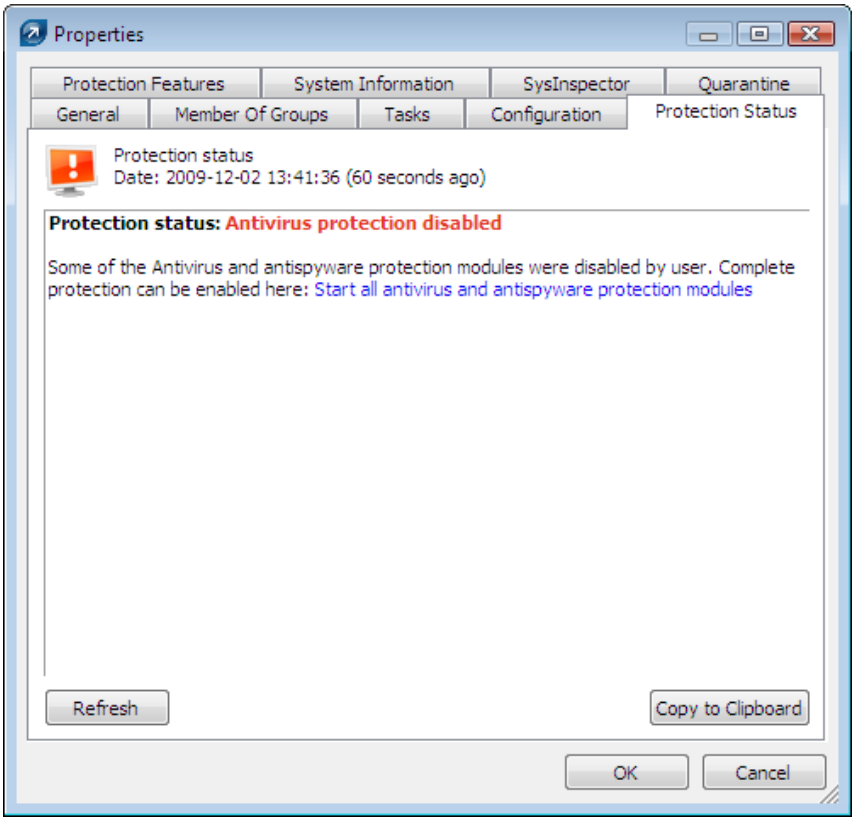


Рисунок: выбор предложенного текста решения для отправки интерактивной задачи клиенту.

3) В поле **Состояние защиты** будет показано одно или несколько предупреждений. Щелкните текст предлагаемого решения голубого цвета в конце сообщения.

4) Нажмите кнопку **Да** для подтверждения выполнения интерактивной задачи.

5) После повторения шагов 3 и 4 для каждого показанного сообщения несколько раз нажмите кнопку **Обновить**, чтобы проверить, исчезло ли сообщение о состоянии.

После успешного устранения проблемы текст состояния защиты изменится на **Состояние защиты: Система в безопасности**.

Примечание. Функция интерактивной задачи поддерживается в продуктах ESET Smart Security/ESET NOD32 версии 3 и старше.

5.2 Диспетчер групп

Диспетчер группы представляет собой функциональный инструмент для управления клиентами, позволяющий разделить их на отдельные группы и применить к ним различные параметры, задачи, ограничения и т. д. Диспетчер легко вызывается из меню **«Служебные программы» > «Диспетчер групп»** или клавишами **CTRL+G**. Группы независимы для каждого сервера ERAS и не реплицируются.
Можно создавать собственные группы с учетом текущий потребностей сети компании или просто синхронизировать группы клиентов ERAC с каталогом Microsoft Active Directory с помощью шаблона **«Синхронизация Active Directory»** прямо в главном окне диспетчера групп.

Группы клиентов могут быть двух типов:
- Статические группы
- Параметрические группы

Статические и параметрические группы можно использовать в различных частях ERA, что существенно расширяет возможности в области управления клиентами.

5.2.1 Статические группы

Статические группы создаются для объединения клиентов в сети в именованные группы и подгруппы. Например, можно создавать группу «Маркетинг», в которой будут собраны всю клиенты маркетинга, а также создать специализированные подгруппы — «Местные продажи», «Руководство EMEA» и т. п.

Главное окно статических групп разделено на две части. В левой части отображается иерархия существующих группы и подгрупп. Клиенты, являющиеся членами выбранной группы, отображаются в правой части окна. По умолчанию отображаются только клиенты из выбранной группы. Чтобы отображались клиенты, входящие в подгруппы выбранной группы, установите флажок **«Показывать клиенты в подгруппах»**.

Чтобы создать новую группу, нажмите кнопку **«Создать»** и введите название группы. Новая группа будет создана как подгруппа выбранной в данный момент родительской группы. Если нужно создать основную группу, выделите корень иерархического дерева — **«Статические группы»**. Поле родительской группы содержит имя родительской группы для новой созданной группы (например, "/" для корневой группы). Рекомендуется использовать названия, обозначающие местонахождение компьютеров (например, *Бухгалтерия*, *Технический отдел* и т. п.). В поле «Описание» можно задавать дополнительное описание группы (например, *«Компьютеры в центральном офисе»*, *«Компьютеры дизайнеров»* и т. п.). Кроме того, свойства созданных и настроенных групп можно изменить позже.

Примечание. Если задача отправлена в родительскую группу, все станции, принадлежащие ее подгруппе, также примут эту задачу.

Кроме того, можно создать пустую группы для последующего использования.

Нажмите кнопку **OK**, чтобы создать группу. Слева появится название и описание группы. Кроме того, станет активной кнопка **«Добавить/удалить»**. Эта кнопка предназначена для добавления клиентов в группу (дважды щелкните по клиенту или перетащите его из левой части в правую). Чтобы найти и добавить клиента, полностью или частично введите его имя в поле **«Быстрый поиск»**: в результате появится список всех клиентов, в названии которых есть введенная строка. Чтобы отметить всех клиентов, нажмите кнопку **«Выбрать все»**. Для проверки наличия новых клиентов, подключившихся к серверу, нажмите кнопку **«Обновить»**.

Если выбор клиентов вручную не подходит, нажмите кнопку **«Добавить специальное...»**, чтобы вызвать окно с дополнительными параметрами.

Параметр **«Добавить клиенты»** на панели клиентов позволяет добавить все клиенты, отображенные в разделе клиентов; кроме того, доступен параметр **«Только выбранные»**. Чтобы добавить клиенты, уже относящиеся к другому серверу или группе, выделите их в списках слева и справа и нажмите кнопку **«Добавить»**.

Для возврата в главное окно редактора статических групп нажмите в окне **«Добавить/удалить»** кнопку **OK**. В результате отобразится новая группа с соответствующими клиентами.

Для добавления или удаления клиентов из групп предназначена кнопка **«Добавить/удалить»**, а для удаления целых групп — кнопка **«Удалить»**. Для копирования списков клиентов и групп используется кнопка **«Копировать в буфер»**. Для обновления клиентов группы нажмите кнопку **«Обновить»**.

Клиентов выбранной группы можно также **импортировать/экспортировать** в *XML*.

5.2.2 Параметрические группы

В дополнение к статическим группам доступны параметрические группы. Клиентские станции динамически присваиваются определенной параметрической группе при соответствии условиям данной группы. Преимущество параметрических групп заключается в том, что их можно использовать для различных целей: в фильтрах, политиках, отчетах и уведомлениях.

Главное окно параметрический группы состоит из четырех частей. В разделе **«Параметрические группы»** перечислены созданные родительские группы и подгруппы. После выбора определенной группы в разделе «Параметрические группы» принадлежащие этой группе клиенты отображаются в разделе **«Выбранная группа»**.
Примечание. Если выбрана родительская группа, список будет также содержать членов подгруппы.

Параметры, установленные для выбранной группы, отображаются в разделе **«Параметры»** данного окна. Для изменения или добавления параметров предназначена кнопка **«Изменить...»**.

В разделе **«Состояние синхронизации»** отображается ход выполнения синхронизации.

Чтобы создать новое правило, нажмите кнопку **«Создать...»**. Новая группа будет создана как подгруппа выбранной в данный момент родительской группы. Если нужно создать основную группу, выделите корень иерархического дерева — **«Параметрические группы»**. Поле родительской группы содержит имя родительской группы для новой созданной группы (например, "/" для корневой группы). Введите **имя** и небольшое **описание** новой группы. Следующим шагом является создание **параметров фильтрации клиентов**. Это можно сделать с помощью кнопки **«Изменить...»**. Если установлен флажок **«Закрепить»**, клиенты будут автоматически добавляться в эту группу, если отвечают ее условиям (при этом автоматическое удаление не выполняется). Содержимое закрепленной группы можно сбросить вручную на уровне корневого каталога.

Примечание. Этот параметр можно установить только при создании новой группы.

Чтобы изменить существующую группу, просто выберите ее в списке параметрических групп и нажмите кнопку **«Изменить...»** в нижней части окна. Чтобы удалить группу, выберите нужную группу и нажмите кнопку **«Удалить»**.
Список групп можно обновить вручную с помощью кнопки **«Обновить»**. Чтобы импортировать группу из файла, выберите в разделе **«Параметрические группы»** группу, в которую нужно импортировать новую группу, и нажмите кнопку **«Импорт...»**. Подтвердите выбор, нажав кнопку **«Да»**. Найдите файл для импорта и нажмите кнопку **«Открыть»**. Группы (и все ее подгруппы) будут импортированы в выбранное место. Чтобы экспортировать группу (и ее подгруппы), выберите ее в разделе **«Параметрические группы»**, щелкните стрелку кнопки **«Импорт...»** и выберите команду **«Экспорт...»** Подтвердите действие, нажав кнопку **«Да»**, выберите имя экспортируемого файла, укажите место для его экспорта и нажмите кнопку **«Сохранить»**.

Примечание. Группы в разделе **«Параметрические группы»** можно перетаскивать с помощью мыши.

5.2.3 Синхронизация Active Directory

При синхронизации Active Directory группы (с соответствующими клиентами) создаются автоматически на базе структуры Active Directory. Это позволяет администратору распределить клиентов по группам (при условии, что имя клиента совпадает с объектом *компьютер* на стороне Active Directory (AD) и входит в группы AD).

Есть два основных параметра, которые определяют порядок синхронизации.

Параметр **«Синхронизировать группы»** позволяет выбрать группы AD для синхронизации. Параметр **«Все группы»** выполняет синхронизацию всей древовидной структуры AD независимо от того, есть ли в группах AD клиенты ERA. Следующие два параметра (**«Только группы с клиентами сервера ERA Server»** и **«Только группы с клиентами главного сервера ERA»**) обеспечивают строгую синхронизацию, то есть синхронизацию только групп с уже существующими клиентами ERA.

Параметром **«Тип синхронизации»** определяется, будут ли синхронизируемые группы AD добавлены в существующие группы AD (значение **«Импорт групп AD»**) или существующие группы AD будут полностью заменены синхронизируемыми (значение **«Синхронизация групп AD»**).

Параметр **«Синхронизировать»** позволяет запланировать синхронизацию AD на определенное время.

Подробная настройка синхронизации Active Directory выполняется в редакторе Configuration Editor (**ESET Remote Administrator** > **ERA Server** > **«Настройка»** > **«Группы»** > **«Параметры синхронизации Active Directory»**). По умолчанию синхронизируются только **группы защиты компьютера и организационные единицы компьютера**. Однако можно добавить и другие объекты Active Directory, установив соответствующие флажки.

Примечание. Для синхронизации ERAS с Active Directory сервер ERAS не обязательно должен быть установлен на контроллере домена. Достаточно того, чтобы контроллер домена был доступен с компьютера, на котором находится сервер ERAS. Чтобы настроить аутентификацию для контроллера домена, выберите в меню следующую команду: **«Служебные программы»** > **«Настройки сервера...»** > **«Дополнительно»** > **«Изменить дополнительные настройки...»** > **ESET Remote Administrator** > **ERA Server** > **«Настройка»** > **Active Directory**. Имя сервера задается в формате *LDAP://имя_сервера* или *GC://имя_сервера*. Если этот параметр не задан, используется глобальный каталог (GC).

5.3 Политики

Политики напоминают задачи конфигурирования с тем отличием, что не являются разовыми задачами, отправляемыми на одну или несколько рабочих станций. Вместо этого политики предназначены для постоянного обслуживания конфигурационных настроек продуктов безопасности ESET. Другими словами, политика — это конфигурация, которая принудительно устанавливается для клиента.

5.3.1 Основные принципы применения и действия

Диспетчер политик вызывается с помощью команды меню **«Служебные программы»** > **«Диспетчер политик»**. В дереве политик слева перечислены политики, присутствующие на отдельных серверах. Правая часть состоит из четырех областей — **«Параметры политики»**, **«Конфигурация политики»**, **«Действие политики»** и **«Глобальные настройки политики»**, — параметры в которых позволяют администратору управлять политиками и настраивать их.

Основными функциями диспетчера политик являются создание, изменение и удаление политик. Клиенты получают политики с сервера ERAS. На сервере ERAS может использоваться несколько политик, которые наследуют настройки друг от друга или с сервера верхнего уровня.

Система копирования политик с сервера верхнего уровня называется *наследованием*; политики, созданные в результате наследования, называются *объединенными политиками*. Наследование основано на принципе «Родитель — ребенок», то есть дочерняя политика наследует настройки родительской политики.

5.3.2 Создание политик

При установке по умолчанию реализована только одна политика — «Политика сервера». Это название можно изменить в поле **«Название политики»** раздела **«Параметры политики»**. Сама политика настраивается в редакторе конфигураций ESET Configuration Editor: нажмите кнопку **«Изменить»** и задайте параметры для выбранного продукта безопасности ESET (или клиента). Все параметры упорядочены в обширную структуру, а все элементы в редакторе обозначены значками. Для клиентов можно применять только активные параметры (они отмечены голубым значком). Все неактивные параметры (серого цвета) остаются на целевых компьютерах без изменений. Тот же принцип действует для унаследованных и объединенных политик: дочерняя политика наследует из родительской политики только активные параметры.

На серверах ERA Server можно использовать несколько политик (**«Добавить новую дочернюю политику»**). Для новых политик доступны следующие параметры: название политики, связь с **родительской политикой** и конфигурация (конфигурация может быть пустой, скопированной из существующей политики или из *XML*-файла конфигурации). Политики можно создавать только на сервере, к которому подключена консоль ERAC. Для создания политик на подчиненном сервере необходимо подключиться к этому серверу.

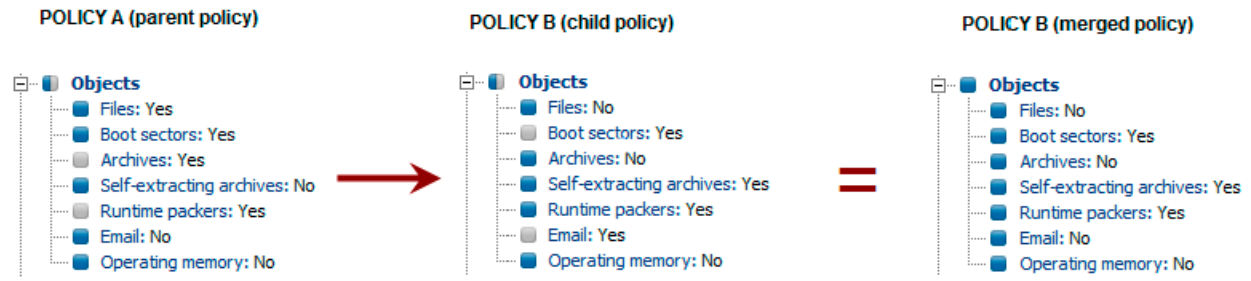
У каждой политики есть два базовых атрибута: **«Переопределить все дочерние политики»** и **«Реплицируемая вниз политика»**. Эти атрибуты определяют наследование дочерними клиентами активных параметров конфигурации.

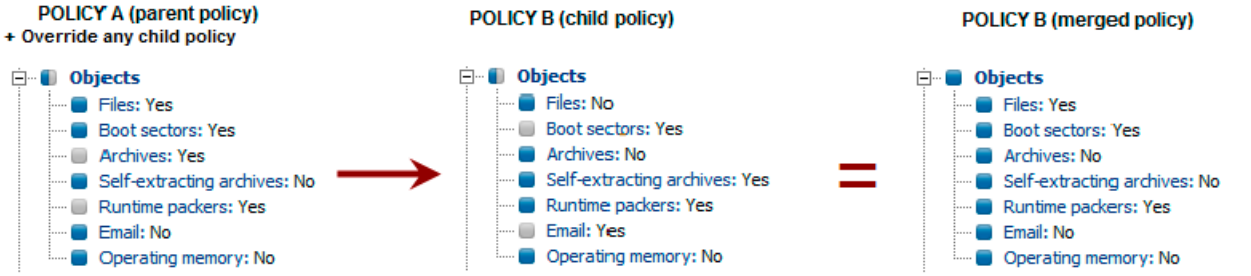
«Переопределить все дочерние политики» — принудительно изменяет все активные параметры в унаследованных политиках. Если в дочерней политике имеются отличия, объединенная политика будет содержать все активные параметры из родительской политики (даже если для дочерней политики включен параметр **«Переопределить все дочерние политики»**). Все неактивные параметры из родительской политики перейдут в дочернюю политику. Если атрибут **«Переопределить все дочерние политики»** не включен, в объединенной политике настройки дочерней политики будут иметь более высокий приоритет, чем настройки

родительской политики. Такие объединенные политики применяются к другим политикам, если они связаны с ними как родительские.

«Реплицируемая вниз политика — включает репликацию на дочерние политики, т. е. может служить политикой по умолчанию для подчиненных серверов, а также назначаться клиентам, подключенным к подчиненным серверам.

Политики также можно импортировать из *XML*-файла и экспортировать в него, а также импортировать из групп. Дополнительные сведения см. в разделе Импорт и экспорт политик 60.





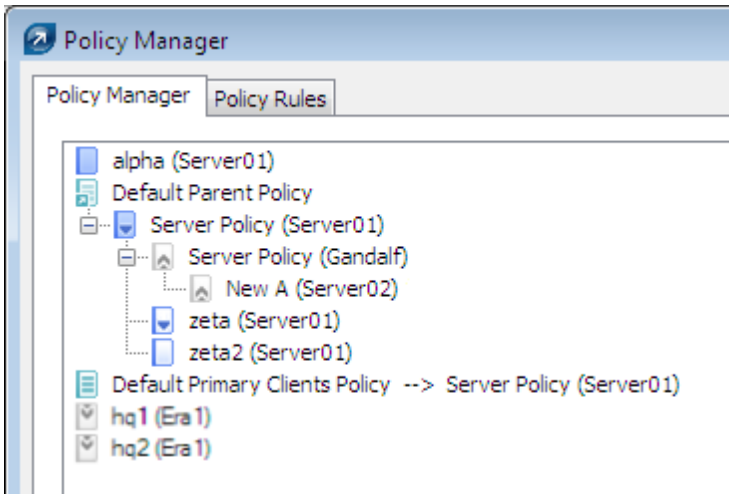
5.3.3 Виртуальные политики

В дополнение к созданным и реплицированным с других серверов политикам (см. раздел Вкладка «Репликация» 87) в дереве политик также есть родительская политика по умолчанию и политика по умолчанию для основных клиентов, которые называются виртуальными политиками.

Родительская политика по умолчанию находится на сервере более высокого уровня в глобальных настройках политик и выбирается как **«Политика по умолчанию для подчиненных серверов»**. Если сервер не реплицируется, политика является пустой (этот момент подробнее разъясняется далее).

Политика по умолчанию для основных клиентов находится на заданном сервере (не на сервере более высокого уровня) в глобальных настройках политик и выбирается как «Политика по умолчанию для основных клиентов». Она автоматически применяется к новым (основным) клиентам, подключившимся к данному серверу ERAS, независимо от того, применялась ли к ним другая политика из правил политик (дополнительные сведения см. в разделе Назначение политик клиентам 60. Виртуальные политики являются ссылками на другие политики, находящиеся на том же сервере.

5.3.4 Роль и назначение политик в древовидной структуре политик



Каждая политика в дереве политик обозначается значком слева. Значение этих значков описано ниже.

1) Политики, обозначенные синими значками, используются на данном сервере. Существует три разновидности синих значков.

Значки с белой серединой — политика создана на данном сервере. Кроме того, она не реплицируется вниз, т. е. не назначается клиентам серверами нижнего уровня, а также не является родительской политикой для дочерних серверов. Такие политики можно использовать только на данном сервере — для клиентов, подключенных к этому серверу. Она также может быть родительской политикой для другой политики на том же самом сервере.

Значки с синей серединой — политика также создана на данном сервере, но при этом включен параметр **«Переопределить все дочерние политики»** (дополнительные сведения см. в разделе Создание политик 57).

Значки со стрелкой «Вниз» — эти политики реплицируются, т. е. включен параметр **«Реплицируемая вниз политика»** включен. Эти политики можно использовать на данном сервере или на его дочерних серверах.

2) Политики, обозначенные серыми значками, созданы на других серверах.

Значки со стрелкой «Вверх» — эти политики реплицированы с дочерних серверов. Их можно только просмотреть или удалить с помощью функции **«Удалить ветвь политики»**. Сама политика при этом не удаляется, она будет удалена только из дерева политик. Поэтому такие политики могут снова появляться после репликации. Чтобы не отображать политики с подчиненных серверов, воспользуйтесь параметром **«Скрыть неиспользуемые политики чужого сервера в дереве политик»**.

Значки со стрелкой «Вниз» — эти политики реплицированы с серверов верхнего уровня. Их можно использовать в качестве родительских для других назначенных политик, назначать клиентам (**«Добавить клиенты»**) или удалять (**«Удалить политику»**). В этом случае удаляется только сама эта политика — она снова появится после репликации с сервера верхнего уровня (если на сервере верхнего уровня для нее не отключен атрибут **«Реплицируемая вниз политика»**).

Примечание. Чтобы переместить или назначить политику в рамках структуры, можно либо выбрать ей родительскую политику, либо перетащить ее с помощью мыши.

Существующие правила политик можно импортировать и экспортировать из/в *XML*-файл(а) с помощью кнопки **«Импорт.../Экспорт...»**. Конфликты имен при импорте (существующая и импортированная политика с одинаковыми названиями) решаются путем добавления случайной строки после названия импортируемой политики.

5.3.5 Просмотр политик

Политики в дереве политик можно просматривать прямо в Configuration Editor с помощью кнопки **«Просмотр...»** или **«Показать объединенные...»**.

«Показать объединенные» — отображение объединенной политики, созданной в результате наследования (в ходе наследования применяются настройки родительской политики). Этот параметр отображается по умолчанию, поскольку действующая политика уже является объединенной.

«Просмотр» — отображение исходной политики до ее слияния с родительской.

На серверах нижнего уровня политикам, унаследованным от серверов верхнего уровня, доступны следующие параметры.

«Показать объединенные» — см. выше.

«Просмотреть обязательную часть» — эта кнопка применяется только к политикам с атрибутом «Переопределить все дочерние политики». Этот параметр позволяет просматривать только принудительно заданную часть политики, т. е. ту ее часть, которая имеет приоритет над другими настройками дочерних политик.

«Просмотреть необязательную часть» — имеет значение, противоположное параметру «Просмотреть обязательную часть», т. е. отображает только активные элементы, к которым параметр «Переопределить...» не применяется.

5.3.6 Импорт и экспорт политик

Диспетчер политик позволяет импортировать и экспортировать политики и правила политик. Существующие политики можно импортировать и экспортировать из/в *XML*-файл(а) с помощью кнопки **«Импорт политики.../ Экспорт политики...»**. Кроме того, политики можно импортировать из групп с помощью кнопки **«Импорт из групп...»**. Правила политик можно импортировать и экспортировать с помощью кнопки **«Импорт.../ Экспорт...»**, а также их можно создавать в **мастере правил политик**.

Конфликты имен при импорте (существующая и импортированная политика с одинаковыми названиями) решаются путем добавления случайной строки после названия импортируемой политики. Если конфликт не может быть решен таким образом (как правило, из-за того, что новое имя слишком длинное) импорт заканчивается с предупреждением *Конфликт неразрешенного имени политики*. Решением является переименование или удаление конфликтующей политики или правил политики.

5.3.7 Назначение политик клиентам

Ниже описаны два основных правила назначения политик клиентам.

1. Локальным (основным) клиентам можно назначить любую локальную политику или любую политику, реплицированную с серверов более высокого уровня.

2. Клиентам, реплицированным с серверов более низкого уровня, можно назначить любую локальную политику с атрибутом **«Реплицируется вниз»** или любую политику, реплицированную с серверов более высокого уровня. Этим клиентам нельзя принудительно назначить политику с их собственного главного сервера (для этого необходимо подключиться к этому серверу с помощью консоли ERAC).

Важным моментом является то, что каждому из клиентов назначается какая-нибудь политика (клиентов без политики не существует). Кроме того, политику клиента нельзя удалить — ее можно только заменить другой. Чтобы не применять к клиенту конфигурацию ни из одной политики, создайте пустую политику.

5.3.7.1 Политика по умолчанию для основных клиентов

Одним из методов назначения политик является автоматическое применение политики по умолчанию для основных клиентов — виртуальной политики, которая конфигурируется в глобальных настройках политики. Эта политика применяется к основным клиентам — к клиентам, которые напрямую подключены к серверу ERAS. Дополнительную информацию см. в разделе Виртуальные политики 58.

5.3.7.2 Назначение вручную

Назначить политику вручную можно двумя способами: щелкнуть правой кнопкой мыши по панели **«Клиенты»** и выбрать в контекстном меню пункт **«Добавить политику** или выбрать в диспетчере политик команду **«Добавить клиенты** > **«Добавить/удалить»**.

После выбора команды **«Добавить клиенты»** в диспетчере политик откроется диалоговое окно **«Добавление и удаление»**. Список клиентов находится слева в виде «Сервер/Клиент». Если выбран параметр **«Реплицируется вниз»**, в окне также будут перечислены клиенты, реплицированные с подчиненных серверов. Выберите клиенты для политики посредством перетаскивания или с помощью кнопки **>>**, перемещающей их в список **выбранных**. Новые выбранные клиенты помечаются желтой звездочкой; их можно удалить из списка **выбранных** с помощью кнопки **<<** или клавиши **C**. Нажмите кнопку **OK**, чтобы подтвердить выбор.

Примечание. Если после подтверждения повторно открыть окно **«Добавление и удаление»**, клиентов уже нельзя будет удалить из списка **выбранных**. Политику для них можно будет только заменить.

Клиенты также можно добавлять с помощью функции **«Добавить специальное»**, которая добавляет все клиенты сразу, только выбранные клиенты или клиенты из выбранных серверов или групп.

5.3.7.3 Правила политик

Инструмент **«Правила политик»** позволяет администратору автоматически назначать политики клиентским рабочим станциям более удобным способом. Правила применяются сразу после подключения клиента к серверу. Они имеют более высокий приоритет, чем у **политики по умолчанию для основных клиентов** или при назначении вручную. **«Политика по умолчанию для основных клиентов»** применяется только в случае, если клиент не подпадает под текущие правила. Аналогичным образом, если применяется вручную назначенная политика, конфликтующая с правилами политик, приоритет будет иметь конфигурация, принудительно примененная правилами политик.

Для правил политик в диспетчере политик есть отдельная вкладка, на которой можно создавать правила и управлять ими. Процесс создания и применения правил очень похож на аналогичный процесс в почтовых клиентах: каждое правило содержит один или несколько критериев; чем выше правило в списке, тем оно важнее (их можно перемещать вверх и вниз).

Чтобы создать новое правило, нажмите кнопку **«Создать...»**. Затем укажите значения параметров **«Название»**, **«Описание»**, **«Фильтр клиентов»** и **«Политика»** (политика, которая применяется ко всем клиентам, удовлетворяющим указанному критерию).

Для настройки критерия фильтрации нажмите кнопку **«Изменить»**.

Доступные критерии:

«(НЕ) С главного сервера» — клиент (не) находится на главном сервере;
«(НЕ) ЯВЛЯЕТСЯ новым клиентом» — клиент (не) является новым;
«(НЕ) УСТАНОВЛЕН флаг „Новый“» — применяется к клиентам с флагом «Новый клиент» или без него;
«Главный сервер (НЕ) содержит (указать)» — имя главного сервера (не) содержит указанную строку;
«В ГРУППАХ ERA (указать)» — клиент относится к указанным группам;
«НЕ В ГРУППАХ ERA (указать)» — клиент не относится к указанным группам;
«(НЕ) В ДОМЕНЕ/РАБОЧЕЙ ГРУППЕ (указать)» — клиент (не) относится к указанному домену;
«Маска имени компьютера (указать)» — имя компьютера соответствует указанному значению;
«СОДЕРЖИТ маску IP (указать)» — клиент относится к группе, определяемой указанными IP-адресом и маской;
«СОДЕРЖИТ диапазон IP (указать)» — клиент относится к группе, определяемой указанными диапазоном IP-адресов;
«(НЕ) СОДЕРЖИТ запрещенную политику (указать)» — клиент (не) наследует указанную политику;
«Название продукта (НЕ) содержит» — название продукта содержит указанную строку;
«Версия продукта (НЕ)» — версия продукта соответствует указанной;
«Маска прочих данных клиента (НЕ) содержит» — прочие данные клиента содержат указанное значение;

«(НЕ) установлено состояние защиты (указать)» — для клиента установлено указанное состояние защиты;
«Версия БД сигнатур вирусов (НЕ)» — версия БД сигнатур вирусов соответствует указанной;
«Последнее подключение (НЕ) старше чем (указать)» — последнее подключение старше указанного времени;
«Ожидание перезапуска (НЕТ)» — клиент находится в ожидании перезапуска;

Правила политик можно импортировать из *XML*-файл и экспортировать в него. Кроме того, их можно создавать автоматически с помощью **мастера правил политики**, который позволяет сформировать структуру политики на основе структуры существующей группы и сопоставлять созданные политики группам путем создания соответствующих правил политики. Дополнительные сведения об импорте и экспорте правил политики см. в разделе Импорт и экспорт политик 60.

Чтобы удалить политику, нажмите кнопку **«Удалить»** в окне **диспетчера политик**. Чтобы немедленно применить все правила, нажмите кнопку **«Запустить сейчас правила политики»**.

5.3.8 Удаление политик

Как и создание правил, их удаление возможно только для политик, находящихся на сервере, с которым установлено соединение. Для удаления политик на других серверах к ним необходимо подключиться с помощью консоли ERAC.

Примечание. Политика может быть связана с другими серверами или политиками (как родительская политика, как политика по умолчанию для подчиненных серверов, как политика по умолчанию для основных клиентов и т. п.), поэтому в некоторых случаях ее придется заменить, а не удалить. Для просмотра параметров удаления и замены нажмите кнопку **«Удалить политику»**. Описанные ниже параметры могут быть доступны или недоступны в зависимости от положения заданной политики в иерархии политик.

«Новая политика для главных клиентов с удаленной политикой»: позволяет выбрать новую политику для основных клиентов в качестве замены для удаляемых. Основные клиенты могут принимать **политику по умолчанию для основных клиентов**, а также другие политики с того же сервера (назначенные вручную с помощью кнопки **«Добавить клиенты»** или принудительно **правилами политик**). В качестве замены можно использовать любую политику с заданного сервера или реплицированную политику.

«Новая родительская политика для дочерних политик удаленной политики (если существуют)»: если удаляемая политика является родительской для других дочерних политик, ее также необходимо заменить. Заменить ее можно политикой с того же сервера, политикой, реплицированной с серверов более высокого уровня, или флагом «н/д», который означает, что дочерним политикам будет назначена незаменяемая политика. Настоятельно рекомендуется назначать замену, даже если дочерних политик не существует. Назначение другим пользователем дочерней политики этой политике в процессе удаления приведет к конфликту.

«Новая политика для реплицированных клиентов с удаленной или измененной политикой»: здесь можно выбрать новую политику для клиентов, реплицированных с серверов более низкого уровня, которые были связаны с удаляемой политикой. В качестве замены можно использовать любую политику с заданного сервера или реплицированную политику.

«Новая политика по умолчанию для подчиненных серверов»: если удаленная политика является виртуальной (см. раздел **«Глобальные настройки политики»**), ее необходимо заменить другой политикой (дополнительную информацию см. в разделе Виртуальные политики 58). В качестве замены можно использовать любую политику с заданного сервера или флаг «н/д».

«Новая политика по умолчанию для главных клиентов»: если удаленная политика является виртуальной (см. раздел **«Глобальные настройки политики»**), ее необходимо заменить другой политикой (дополнительную информацию см. в разделе Виртуальные политики 58). Для замены можно использовать политику с того же сервера.

Если отключить параметр политики **«Реплицируется вниз»** и нажать кнопку **«ОК, Применить»** или выбрать в дереве политик другую политику, появится такое же диалоговое окно. При этом будут включены параметры **«Новая политика для реплицированных клиентов с удаленной или измененной политикой»** или **«Новая политика по умолчанию для подчиненных серверов»**.

5.3.9 Специальные настройки

Еще две политики находятся не в диспетчере политик, а в разделе **«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные настройки»** > **ESET Remote Administrator** > **ERA Server** > **«Настройка» > «Политики»**.

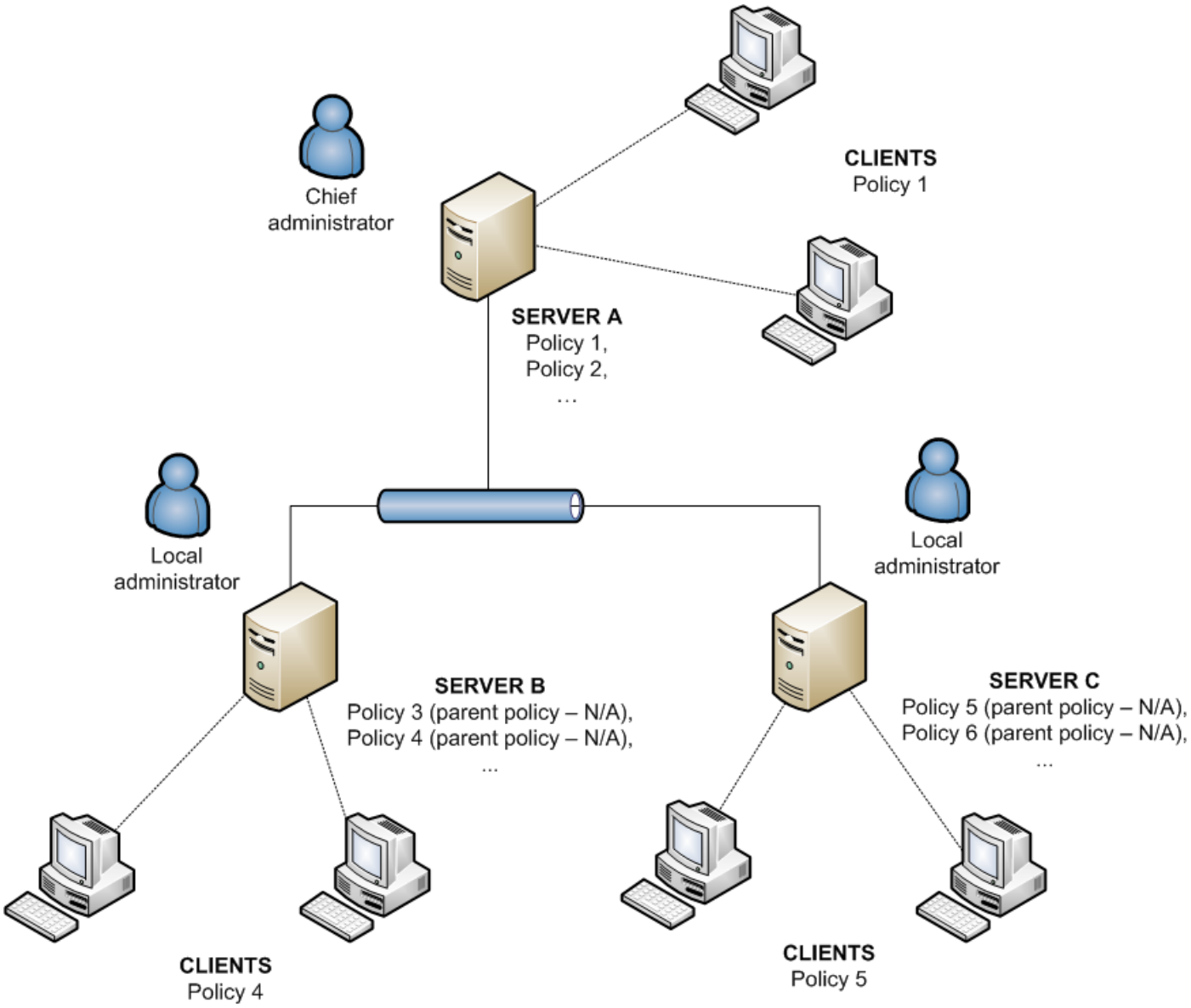
«Интервал принудительного применения политики (мин)»:
данная функция применяется к политикам в течение выбранного интервала времени. Рекомендуется оставлять значение по умолчанию.

«Отключить использование политики»:
этот параметр позволяет отменять применение политик на серверах. Рекомендуется использовать этот параметр в случае возникновения проблем с политикой. Если к некоторым клиентам не нужно применять политику, лучшим решением является назначение пустой политики.

5.3.10 Сценарии развертывания политик

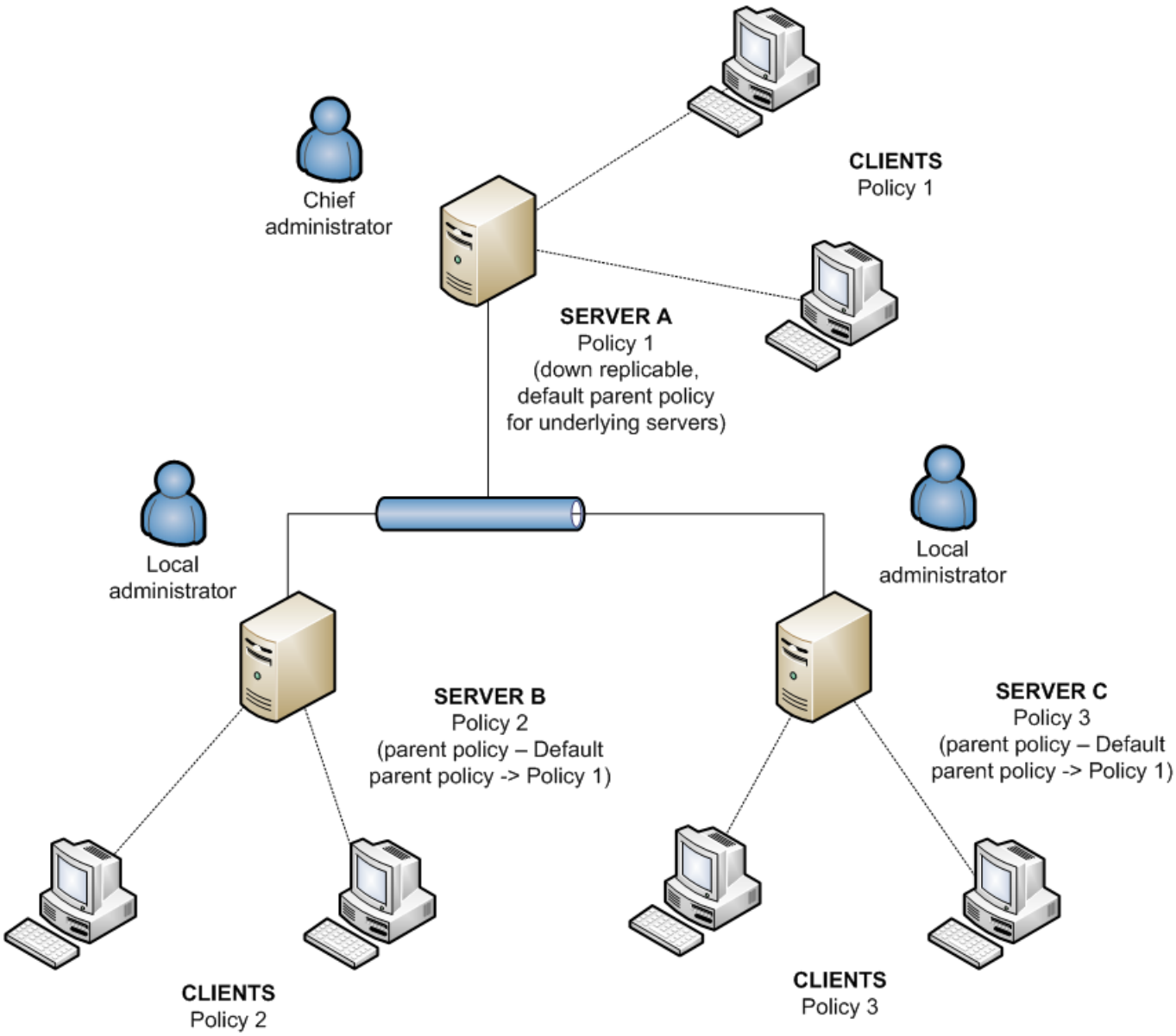
5.3.10.1 Каждый сервер является автономной единицей, политики определяются локально

Этот сценарий предназначен для небольших сетей с одним главным и двумя подчиненными серверами. У каждого сервера есть несколько клиентов. На каждом из серверов создано не менее одной политики. Подчиненные серверы находятся в филиалах; оба сервера обслуживаются локальными администраторами. Каждый из администраторов сам решает, какие политики применяются к различным клиентам его сервера. Главный администратор не изменяет конфигурации, созданные локальными администраторами, и не назначает политики клиентам подчиненных серверов. С точки зрения политики сервера это означает, что у сервера А отсутствует **политика по умолчанию для подчиненных серверов**. Это также означает, что у сервера Б и сервера В для родительской политики установлен флаг «н/д» или другая локальная политика (отдельно от **родительской политики по умолчанию**). (Например, у серверов Б и В отсутствуют родительские политики, назначенные с главного сервера.)


Chief
administrator
CLIENTS
Policy 1
SERVER A
Policy 1,
Policy 2,
…
Local
administrator
Local
administrator
SERVER B
Policy 3 (parent policy – N/A),
Policy 4 (parent policy – N/A),
…
SERVER C
Policy 5 (parent policy – N/A),
Policy 6 (parent policy – N/A),
…
CLIENTS
Policy 4
CLIENTS
Policy 5

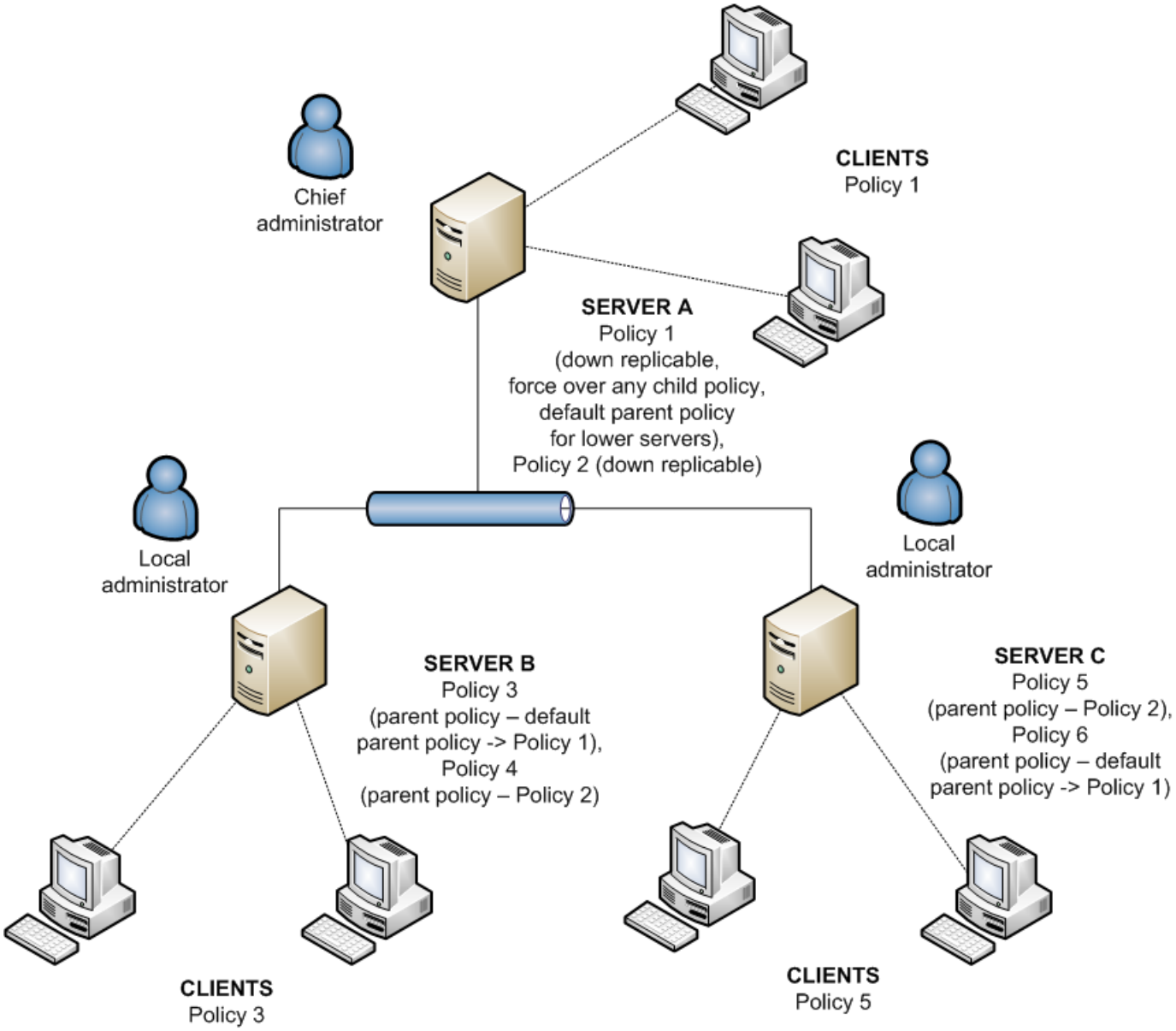
5.3.10.2 Каждый сервер обслуживается отдельно, политики управляются локально, но родительская политика по умолчанию наследуется с сервера верхнего уровня.

Конфигурация из предыдущего сценария применима также и к этому сценарию. Однако при этом для сервера A включен параметр «Политика по умолчанию для подчиненных серверов», а политики на подчиненных серверах наследуют с основного сервера конфигурацию родительской политики по умолчанию. В этом сценарии локальные администраторы имеют достаточно прав для настройки политик. Хотя дочерние политики на подчиненных серверах могут наследовать родительскую политику по умолчанию, локальные администраторы все-таки могут изменять ее своими собственными политиками.



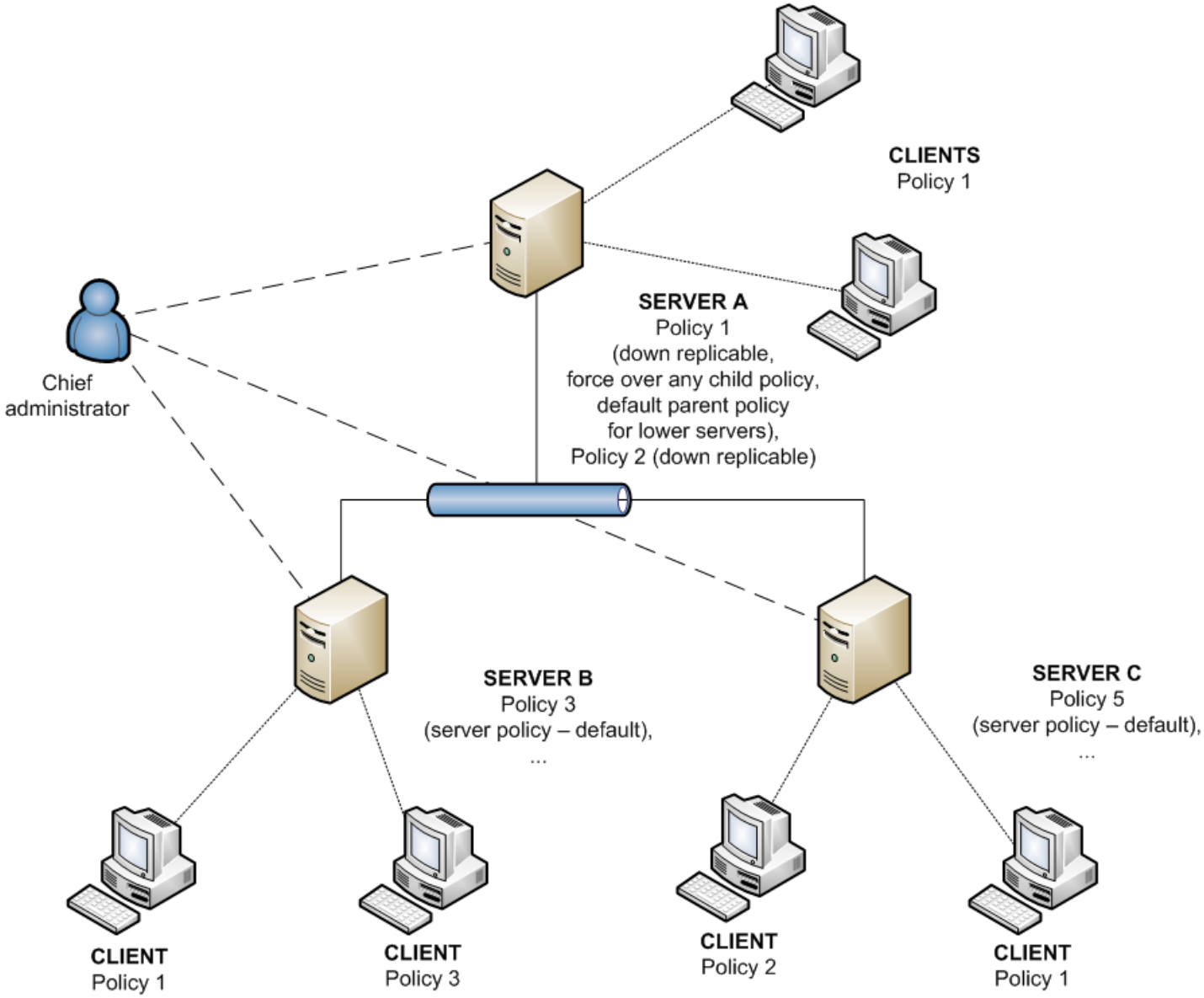
5.3.10.3 Наследование политик с сервера верхнего уровня

Сетевая модель этого сценария та же самая, что и в предыдущих двух сценариях. Кроме того, основной сервер с родительской политикой по умолчанию содержит другие политики, которые реплицируются на уровень ниже и служат родительскими политиками для подчиненных серверов. Для политики 1 (см. рисунок ниже) активирован атрибут **«Применить поверх любых дочерних политик»**. У локального администратора остается достаточно прав, но главный администратор определяет, как и какие политики реплицируются вниз и какие из них служат родительскими для локальных политик. Атрибут **«Переопределить...»** означает, что конфигурации, установленные в выбранных политиках, переопределяют эти настройки на локальных серверах.



5.3.10.4 Назначение политик только с сервера верхнего уровня

Данный сценарий соответствует централизованной системе управления политиками. Политики для клиентов создаются, изменяются и назначаются только на главном сервере, а у локальных администраторов нет прав на их изменение. У всех подчиненных серверов есть только одна базовая политика, которая является пустой (по умолчанию она называется «Политика сервера»). Эта политика служит родительской политикой по умолчанию для основных клиентов.



5.3.10.5 Использование правил политик

В примере ниже рассматриваются автоматически назначаемые политики, основанные на правилах политик. Этот метод является дополнительным, и его следует использовать не в качестве отдельного сценария, а в сочетании со сценариями, описанными ранее.

Если все серверы обслуживаются локальными администраторами, каждый администратор может создавать для своих клиентов отдельные правила политик. В этом сценарии важно, чтобы правила политик не конфликтовали: например, сервер верхнего уровня назначает клиентам политику, основанную на правилах политик, а подчиненный сервер в то же время назначает отдельные политики, основанные на правилах локальных политик.

Кроме того, централизованная система значительно снижает вероятность возникновения конфликтов, поскольку весь процесс управления происходит на главном сервере.

5.3.10.6 Использование групп

В некоторых ситуациях назначение политик группам клиентов служит дополнением к ранее использовавшимся сценариям. Группы можно создавать вручную или с помощью параметра **«Синхронизация Active Directory»**.
Клиентов можно добавлять в группы вручную (**«Статические группы»**) или автоматически — по свойствам группы (**«Параметрические группы»**). Дополнительные сведения см. в разделе Диспетчер групп 55.
Чтобы назначить политику для группы клиентов, можно использовать параметр разового назначения **«Диспетчер групп»** (**«Добавить клиентов» > «Добавить специальное»**), или доставить политики напрямую через **правила политик**.

Ниже показан один из возможных сценариев.

Администратору нужно назначить различные политики для клиентов, принадлежащих различным группам AD, и автоматически изменять политики клиента, когда клиент перемещается в другую группу AD.

1) Сначала необходимо настроить **синхронизацию Active Directory** в **диспетчере групп** согласно своим потребностям. Здесь важно правильно запланировать синхронизацию AD (возможные варианты: каждый час, ежедневно, каждую неделю, каждый месяц).
2) После первой удачной синхронизации группы AD появятся в разделе **«Статические группы»**.
3) Создайте новое правило политики и установите **«Группы ERA В»** и/или **«Группы ERA НЕ В»** как условие правила.
4) Укажите группы AD, которые нужно добавить в условие.
5) В следующем шаге определите политику, которая будет применяться к клиентам, соответствующим условиям правил(а) и нажмите кнопку **ОК**, чтобы сохранить правило.

ПРИМЕЧАНИЕ.: Шаги 3–5 можно заменить, используя **мастер правил политики**, который позволяет создать структуру политики но основе структуры существующей группы и сопоставлять созданные политики группам путем создания соответствующих правил политики.

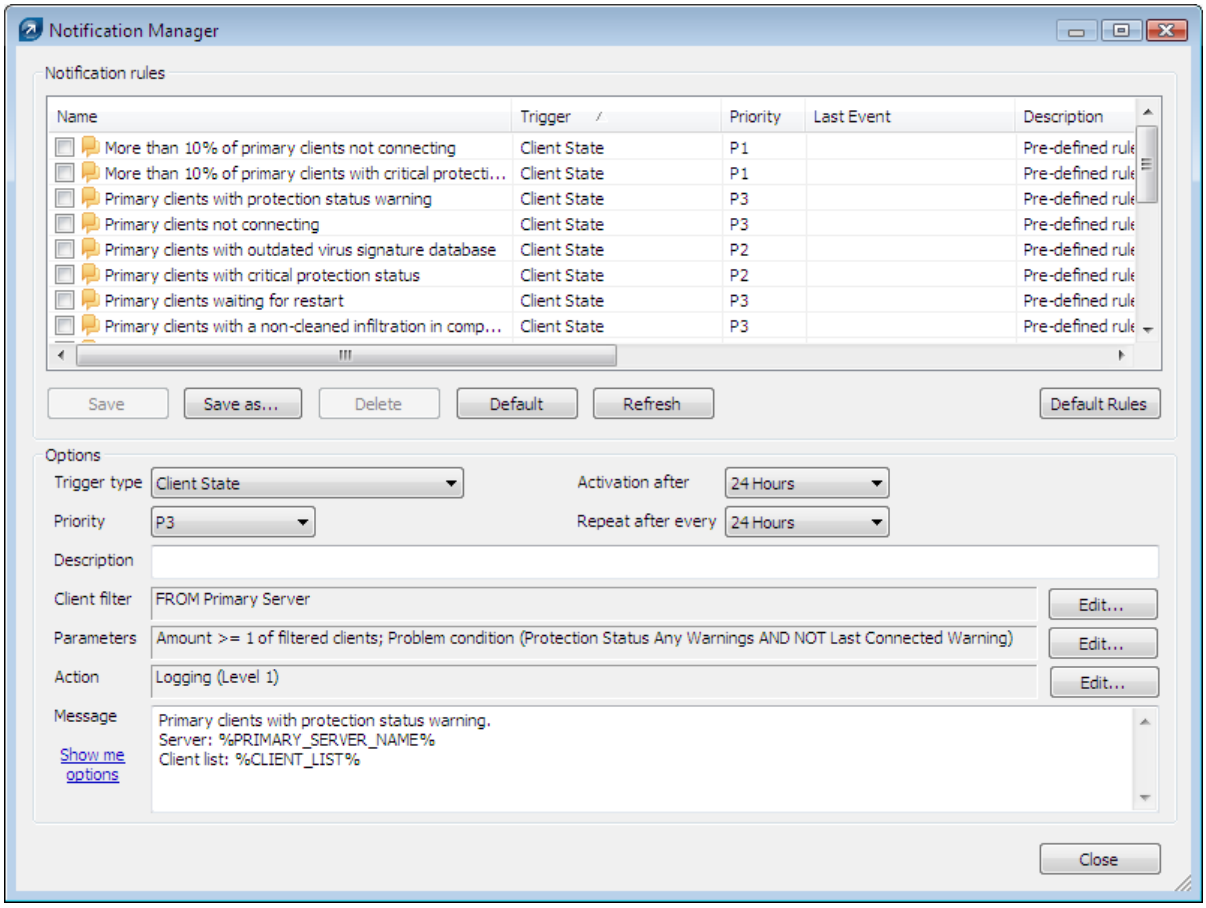
Таким образом можно определить конкретное правило политики для каждой группы AD. Присвоение конкретной политики определенным клиентам теперь зависит от членства клиента в определенной группе AD. Поскольку синхронизация AD выполняется регулярно, все изменения членства клиента в группах AD обновляются и учитываются при применении правила политики. Другими словами, политики применяются к клиентам автоматически в зависимости от их группы AD. После полного определения правил и политик администратору больше не нужно заниматься применением политик.
Основным преимуществом такого подхода является прямое автоматическое связывание членства в группах AD с присвоением политики.

5.4 Уведомления

Возможность уведомлять системных и сетевых администраторов о важных событиях является важной составляющей системы защиты и обеспечения целостности сети. Ранее предупреждение об ошибке или вредоносной программе может предотвратить потерю огромного количества времени и денег для устранения проблемы на более поздней стадии. В следующих трех разделах описаны возможности функции уведомлений, реализованной в программе удаленного администрирования ESET.

5.4.1 Диспетчер уведомлений

Чтобы открыть главное окно **диспетчера уведомлений**, выберите команду **«Служебные программы»** > **«Диспетчер уведомлений»**.



Главное окно разделено на две области. В верхней части окна в разделе **правил уведомления** перечислены существующие (предварительно определенные или определенные пользователем) правила. Для создания уведомлений необходимо выбрать правило из списка. По умолчанию уведомления включены. Поэтому рекомендуется проверить, включены ли правила.

Функциональные кнопки в списке правил: **«Сохранить»** (сохранение изменений в правиле), **«Сохранить как...»** (сохранение изменений в правиле с новым именем), **«Удалить»**, **«По умолчанию»** (восстановление параметров по умолчанию для выбранного типа триггера), **«Обновить»** и **«Правила по умолчанию»** (обновление списка правил по умолчанию).

В разделе **«Параметры»** в нижней части окна отображается информация о выбранном в данный момент правиле. Все поля и параметры из этого раздела описаны в демонстрационном правиле в разделе Создание правила 74.

Для каждого правила можно указать критерий, называемый триггером и активирующий данное правило. Доступны следующие триггеры:

- **«Состояние клиента»** — правило применяется при возникновении проблем на клиентах;
- **«Состояние сервера»** — правило применяется при возникновении проблем на серверах;
- **«Событие „Завершенная задача“»** — правило запускается после завершения указанной задачи;
- **«Событие „Новый клиент“»** — правило выполняется при подключении к серверу нового клиента (в том числе реплицированного);
- **«Новое событие в журнале»** — правило выполняется при обнаружении указанного события в журналах.

В зависимости от типа триггера активируются или деактивируются и другие параметры правил, поэтому при создании новых правил рекомендуется сначала создавать триггеры.

С помощью раскрывающегося меню **«Приоритет»** можно установить приоритет правила. **P1** означает самый высокий приоритет, а **P5** — самый низкий. Приоритет никак не влияет на функциональность правил. Для

назначения приоритета уведомлениям можно использовать переменную *%PRIORITY%*. Под меню **«Приоритет»** находится поле **«Описание»**. Рекомендуется задавать для каждого правила осмысленное описание, например *«правило, предупреждающее об обнаружении вируса»*.

Как только система обнаруживает срабатывание события для определенного клиента или клиентов и находит правило, подлежащее выполнению, применяется фильтр клиентов. Фильтр можно назначать любым правилам, в которых задействованы клиенты. Для настройки фильтра клиента в разделе **«Фильтр клиентов»** нажмите кнопку **«Изменить»**. В открывшемся окне настраиваются параметры фильтрации. При применении правила учитываются только те клиенты, которые удовлетворяют критериям фильтрации клиентов. Критерии фильтрации:

- **«С основного сервера»** — только клиенты с главного сервера; кроме того, можно использовать отрицание этого условия (т. е. «НЕ С»);
- **«ВКЛЮЧИТЬ главный сервер»** — включить в выходные данные главный сервер;
- **«УСТАНОВЛЕН флаг „Новый“»** — клиенты с флагом *«Новый»* (можно использовать отрицание «НЕ УСТАНОВЛЕН»);
- **«Группы ERA B»** — клиенты, относящиеся к указанной группе;
- **«В домене/рабочей группе»** — клиенты, относящиеся к указанному домену или рабочей группе;
- **«Маска имени компьютера»** — клиенты с указанным именем компьютера;
- **«СОДЕРЖИТ маску IP»** — клиенты, соответствующие указанной маске IP-адреса;
- **«СОДЕРЖИТ диапазон IP»** — клиенты, относящиеся к указанному диапазону IP-адресов;
- **«ИМЕЕТ заданную политику»** — клиенты с назначенной им указанной политикой (можно использовать отрицание «НЕ ИМЕЕТ»).

Задав для правила уведомлений фильтр клиентов, нажмите кнопку **OK** и переходите к параметрам правила. Параметры клиента определяют, какому условию должен удовлетворять клиент или группа клиентов для запуска действия уведомления. Чтобы просмотреть доступные параметры, нажмите кнопку **«Изменить...»** в разделе **«Параметры»**.

Доступность параметров зависит от выбранного типа триггера. Ниже приведен полный список параметров, зависимых от типа триггера.

Для триггеров типа «Состояние клиента» доступны следующие параметры:

- **«Состояние защиты: любые предупреждения»** — в элементе «Состояние защиты» обнаружено какое-либо предупреждение;
- **«Состояние защиты: критические предупреждения»** — в элементе «Состояние защиты» обнаружено критическое предупреждение;
- **«Версия БД сигнатур вирусов»** — проблема с базой данных сигнатур вирусов (этот параметр может принимать 6 значений);
  - **«Предыдущая»** — базы данных сигнатур вирусов на одну версию старше текущей;
  - **«Более старая или н/д»** — база данных сигнатур вирусов старше текущей на несколько версий;
  - **«Устарела на 5 версий или Н/Д»** — база данных сигнатур вирусов старше текущей более чем на 5 версий;
  - **«Устарела на 10 версий или Н/Д»** — база данных сигнатур вирусов старше текущей более чем на 10 версий;
  - **«Устарела на 7 дней или Н/Д»** — база данных сигнатур вирусов старше текущей более чем на 7 дней;
  - **«Устарела на 14 дней или Н/Д»** — база данных сигнатур вирусов старше текущей более чем на 14 дней;

- **«Предупреждение о последнем подключении»** — последнее соединение было установлено до указанного периода времени;
- **«Имеется запись об угрозе»** — в столбце «Угроза» имеется предупреждение об угрозе;
- **«Имеется запись о событии»** — в столбце «Последнее событие» имеется запись;
- **«Имеется запись о событии файервола»** — в столбце «Событие файервола» имеется запись о событии файервола;
- **«Установлен флаг „Новый“»** — для клиента установлен флаг «Новый»;
- **«Ожидание перезапуска»** — клиент находится в ожидании перезапуска;
- **«При последнем сканировании обнаружена угроза»** — на клиенте при последнем сканировании обнаружены угрозы в указанном количестве;
- **«При последнем сканировании угроза не была устранена»** — на клиенте при последнем сканировании обнаружены неустраненные угрозы в указанном количестве.

Для всех параметров можно использовать отрицание, но не все отрицания имеет смысл использовать.

Отрицание имеет смысл только для параметров с двумя логическими значениями: истина и не истина. Например, параметр **«Установлен флаг „Новый“»** охватывает только клиенты, отмеченные флагом *«Новый»*. Обращенный параметр будет охватывать все клиенты без этого флага.

Все вышеперечисленные условия можно логически комбинировать и инвертировать. Раскрывающееся меню **«Правило применяется, когда»** содержит два пункта:

- **«все параметры совпадают»** — правило применяется в случае, если соблюдены **все** указанные условия;
- **«любой из параметров совпадает»** — правило применяется в случае, если соблюдено хотя бы **одно**условие.

Для триггеров типа «Состояние сервера» доступны указанные ниже параметры.

- **«Сервер обновлен»** — сервер находится в актуальном состоянии.

- **«Сервер не обновлен»** — сервер не обновлялся дольше, чем предусмотрено значением параметра.

- **«Журналы сервера»** — ниже перечислены различные виды записей в журнале сервера.

  - **«Ошибки»** — сообщения об ошибках.
  - **«Ошибки и предупреждения»** — сообщения об ошибках и предупреждениях.
  - **«Ошибки, предупреждения и информация»** — сообщения об ошибках, предупреждениях и информационные сообщения.
  - **«Фильтровать записи в журнале по типу»** — включив этот параметр, можно указать, какие записи об ошибках и предупреждениях в журнале нужно отслеживать. Обратите внимание на то, что для правильной работы функции уведомлений необходимо установить соответствующий уровень детализации журнала (**«Служебные программы» > «Настройки сервера» > «Ведение журнала»**). В противном случае для правила уведомления в журнале сервера не обнаружится соответствующий ему триггер. В журнал заносятся следующие записи:

- **ADSI_SYNCHRONIZE** — синхронизация групп Active Directory;
- **CLEANUP** — задачи очистки сервера;
- **CREATEREPORT** — создание отчета по запросу;
- **DEINIT** — завершение работы сервера;
- **INIT** — запуск сервера;
- **INTERNAL 1** — внутреннее сообщение сервера;
- **INTERNAL 2** — внутреннее сообщение сервера;
- **LICENSE** — управление лицензиями;
- **MAINTENANCE** — задачи обслуживания сервера;
- **NOTIFICATION** — управление уведомлениями;
- **PUSHINST** — автоматическая установка;
- **RENAME** — переименование внутренней структуры;
- **REPLICATION** — репликация сервера;
- **POLICY** — управление политиками;
- **POLICYRULES** — правила политик;
- **SCHEDREPORT** — автоматически созданные отчеты;
- **SERVERMGR** — управление внутренними потоками сервера;
- **SESSION** — сетевые соединения сервера;
- **SESSION_USERACTION** — различные действия пользователя;
- **THREATSENSE** — отправка статистической информации ThreatSense.Net;
- **UPDATER** — обновление сервера и создание зеркала.

К примеру, параметр UPDATER предписывает отправлять уведомления, когда диспетчер уведомлений находит в журнале сервера проблему, связанную с обновлением и созданием зеркала.

- **«Срок действия лицензии»** — срок действия лицензии истекает через указанное число дней либо уже истек. Параметр **«Предупреждать, только если это приведет к падению числа клиентов в лицензии ниже фактического числа клиентов на сервере базы данных»** предписывает отправлять уведомления только в случае, если истечение срока действия лицензии приведет к падению разрешенного количества клиентов ниже числа клиентов, подключенных в данный момент.

- **«Ограничение лицензии»** — процентная доля свободных слотов клиентов опускается ниже указанного значения.

Для триггеров типа «Новое событие в журнале» доступны указанные ниже параметры.

- **«Тип журнала»** — журнал событий, журнал угроз или журнал файервола.
- **«Уровень журнала»** — уровень детализации записей в заданном журнале:
  — **«Уровень 1 — критические предупреждения»** — только критические ошибки;
  — **«Уровень 2 — То же + предупреждения»** — то же, что и уровень 1, плюс предупреждения;
  — **«Уровень 3 — То же + норма»** — то же, что и уровень 2, плюс информационные сообщения;
  — **«Уровень 4 — То же + диагностика»** — то же, что и уровень 3, плюс сообщения диагностики.

- **«1000 событий за 60 минут»**: введите количество событий и выберите период времени, чтобы установить частоту событий, необходимую для отправки уведомления. По умолчанию частота составляет 1000 событий в час.

- **«Количество»** — количество клиентов (абсолютное или в процентах).

Другие триггеры не имеют никаких специальных параметров.

При возникновении условий, заданных в правиле, автоматически выполняется действие, указанное администратором. Для настройки действий предназначена кнопка **«Изменить...»** в разделе **«Действия»**. Ниже описаны варианты, доступные в редакторе действий.

- **«Электронная почта»** — программа отправляет текст уведомления для данного правила на указанный адрес электронной почты; в поле **«Тема»** можно указать тему сообщения, а кнопка **«Кому»** открывает адресную книгу.
- **«SNMP-ловушка»** — создание и отправка SNMP-уведомления.
- **«Выполнить (на сервере)»** — выбрав этот вариант, укажите приложение для запуска на сервере.
- **«Записывать в файл (на сервере)»** — в указанном файле журнала создаются записи. Также можно настроить **степень детализации** журнала.
- **«Также записывать сообщение»** — в журнал также записывается текст сообщения.
- **«Записывать в системный журнал»** — включает запись уведомлений в журнал сервера; также можно настроить степень детализации уведомлений.
- **«Ведение журнала»** — включает запись уведомлений в журнал сервера; также можно настроить **степень детализации** уведомлений. Для правильной работы этой функции необходимо включить ведение журнала на сервере ERA Server (**«Служебные программы»** > **«Настройки сервера»** > **«Ведение журнала»**).

Формат уведомлений настраивается в поле **«Сообщение»** в нижней части окна диспетчера уведомлений. В тексте можно использовать специальные переменные вида *%ИМЯ_ПЕРЕМЕННОЙ%*. Чтобы просмотреть список доступных переменных, нажмите кнопку **«Показать параметры»**.

- **Server_Last_Updated** — последнее обновление сервера;
- **Primary_Server_Name** — имя главного сервера;
- **Rule_Name** — имя правила уведомления;
- **Rule_Description** — описание правила уведомления;
- **Client_Filter** — параметры фильтрации клиентов;
- **Client_Filter_Short** — параметры фильтрации клиентов (краткая форма);
- **Client_List** — список клиентов;
- **Triggered** — дата последнего отправленного уведомления (без учета повторений);
- **Triggered_Last** — дата последнего отправленного уведомления (с учетом повторений);
- **Priority** — приоритет правила уведомления;
- **Log_Text_Truncated** — текст записи в журнале, для которой сработало уведомление (усеченный вид);
- **Task_Result_List** — список завершенных задач;
- **Parameters** — параметры правила;
- **Last_Log_Date** — дата последнего журнала;
- **License_Info_Merged** — информация о лицензии (сводка);
- **License_Info_Full** — информация о лицензии (полностью);
- **License_Days_To_Expiry** — количество дней, оставшихся до истечения срока действия лицензии;
- **License_Expiration_Date** — ближайшая дата срока истечения лицензии;
- **License_Clients_Left** — количество свободных слотов для подключения клиентов к серверу согласно текущей лицензии;
- **License_Customer** — покупатель лицензии (объединено);
- **Actual_License_Count** — количество клиентов, подключенных к серверу в данный момент;
- **Virus_Signature_DB_Version** — последняя версия базы данных сигнатур вирусов;
- **Pcu_List** — список последних обновлений компонентов программы.

Кроме того, нужно указать время и дату. Активацию правила можно отложить на период от одного часа до трех месяцев. Если нужно активировать правило как можно скорее, выберите в меню **«Активировать через»** пункт **«Как можно скорее»**. По умолчанию диспетчер уведомлений активируется каждые 10 минут, поэтому если выбрать пункт **«Как можно скорее»**, задача будет запущена в пределах 10 минут. Если в меню выбрать конкретный период, действие будет автоматически выполнено по истечении этого времени (в том случае, если будет соблюдено условие правила).

В меню **«Повторять каждые...»** можно выбрать интервал повторения действия. При этом, однако, для активации правила все равно должно быть соблюдено его условие. В меню **«Сервер»** > **«Дополнительно»** > **«Изменить дополнительные настройки»** > **ESET Remote Administrator** > **«Сервер»** > **«Настройка»** > **«Уведомления»** > **«Интервал обработки уведомлений (мин.)»** можно задать интервал времени, по истечении которого сервер будет проверять и выполнять активные правила.

Значение по умолчанию — 10 минут. Не рекомендуется уменьшать это значение, поскольку это может привести к замедлению работы сервера.

По умолчанию в окне диспетчера уведомлений представлен список предопределенных правил. Чтобы активировать правило, установите напротив него флажок. Ниже перечислены доступные правила уведомлений. Если они включены, при соблюдении условий конкретного правила в журнале создается запись.

- **«Нет соединения с более чем 10 % основных клиентов»** — к серверу в течение более одной недели не подключалось более десяти процентов основных клиентов. Правило выполняется в режиме «как можно скорее».
- **«Более 10 % клиентов с критическим состоянием защиты»** — для более чем десяти процентов клиентов было выдано предупреждение о критическом состоянии защиты, причем ни один из этих клиентов не подключался к серверу более одной недели. Правило выполняется в режиме «как можно скорее».
- **«Предупреждения о состоянии защиты у основных клиентов»** — есть хотя бы один клиент с предупреждением о состоянии защиты, который не подключался к серверу в течение одной и более недель.
- **«Основные клиенты не подключаются»** — есть хотя бы один клиент, который не подключался к серверу в течение одной и более недель.
- **«Устаревшая база данных сигнатур вирусов у основных клиентов»** — есть клиент с базой данных сигнатур вирусов на две или более версий младше, чем текущая, который не отключался от сервера в течение более чем одной недели.
- **«Критическое состояние защиты у основных клиентов»** — есть клиент с предупреждением о критическом состоянии защиты, который не отключался от сервера в течение более чем одной недели.
- **«У основных клиентов более новая база данных сигнатур вирусов, чем на сервере»** — есть клиент с базой данных сигнатур вирусов более новой, чем на сервере, который при этом не отключался от сервера в течение более чем одной недели.
- **«Основные клиенты ожидают перезагрузки»** — есть ожидающий перезагрузки клиент, который не отключался от сервера в течение более чем одной недели.
- **«У основных клиентов остались неочищенные после сканирования вирусы»** — есть клиент, компьютер которого при сканировании не удалось очистить от не менее одного вируса, который при этом не отключался от сервера в течение более чем одной недели.
- **«Завершенная задача»** — на клиенте была завершена задача. Правило выполняется в режиме «как можно скорее».
- **«Новые основные клиенты»** — к серверу подключился новый клиент. Правило выполняется в режиме «как можно скорее».
- **«Новые реплицированные клиенты»** — в списке клиентов появился новый реплицированный клиент.
- **«Возможная активность вируса»** — частота записей в журнале угроз на клиенте превысила 1000 критических предупреждений в час на более чем 10 % всех клиентов.
- **«Возможная сетевая атака** — частота записей в журнале персонального файервола ESET на клиенте превысила 1000 критических предупреждений в час на более чем 10 % всех клиентов.
- **«Сервер обновлен»** — сервер был обновлен.
- **«Сервер не обновлен»** — сервер не обновлялся в течение пяти дней или более. Правило выполняется в режиме «как можно скорее».
- **«Ошибка в журнале сервера»** — в журнале сервера имеется запись с ошибкой.
- **«Срок действия лицензии»** — срок действия текущей лицензии истекает через 20 дней, после чего максимальное количество слотов для клиентов станет меньше текущего числа клиентов. Правило выполняется в режиме «как можно скорее».
- **«Ограничение лицензии»** — количество свободных слотов клиентов снижается до 10 % от числа всех доступных слотов клиентов.

Если не указано иное, все правила выполняются и повторяются через 24 часа и применяются к главному серверу и основным клиентам.

5.4.1.1 Уведомления с использованием SNMP-ловушки

Протокол SNMP (простой протокол управления сетью) — это простой и широко распространенный протокол управления, предназначенный для отслеживания и идентификации сетевых проблем. Одним из действий этого протокола является «Ловушка», отправляющая отправляются определенные данные. В ERA функция «Ловушка» используется для отправки уведомлений.

Для эффективной работы функции «Ловушка» необходимо надлежащим образом установить и настроить протокол SNMP на компьютере с сервером ERAS (**«Пуск»** > **«Панель управления»** > **«Установка и удаление программ»** > **«Установка и удаление компонентов Windows»**). Службу SNMP необходимо настроить так, как описано в статье по адресу http://support.microsoft.com/kb/315154. На сервере ERAS необходимо активировать правило уведомлений протокола SNMP. На сервере ERAS необходимо активировать правило уведомлений протокола SNMP.

Уведомления можно просматривать в диспетчере протокола SNMP, подключенному к серверу SNMP, на который импортирован файл конфигурации *eset_ras.mib*. Этот файл является стандартным компонентом установочного пакета ERA и обычно находится в папке *C:\Program Files\ESET\ESET Remote Administrator\Server\snmp*.

5.4.2 Создание правила

В следующих пунктах показано создание правила для отправки администратору уведомлений по электронной почте в случае возникновения проблем с состоянием защиты на какой-либо клиентской рабочей станции. Это уведомление также сохраняется в файл *log.txt*.

1) В раскрывающемся меню **«Тип триггера»** выберите пункт **«Состояние клиента»**.

2) Оставьте для параметров **«Приоритет, Активация через»** и **«Повторять через»** имеющиеся значения. Правилу будет автоматически назначен приоритет 3, и оно будет активировано через 24 часа.

3) В поле **«Описание»** введите **уведомление о состоянии защиты для клиентов головного офиса»**.

4) В разделе **«Фильтр клиентов»** выберите команду **«Изменить...»** и активируйте только условие **«Группы ERA B»**. В нижней части окна щелкните ссылку **«указать»** и введите *Центральный офис* в новом окне. Нажмите кнопку **«Добавить»** и дважды нажмите **OK** для подтверждения. Это означает, что правило применяется только к клиентам, входящим в группу головного офиса.

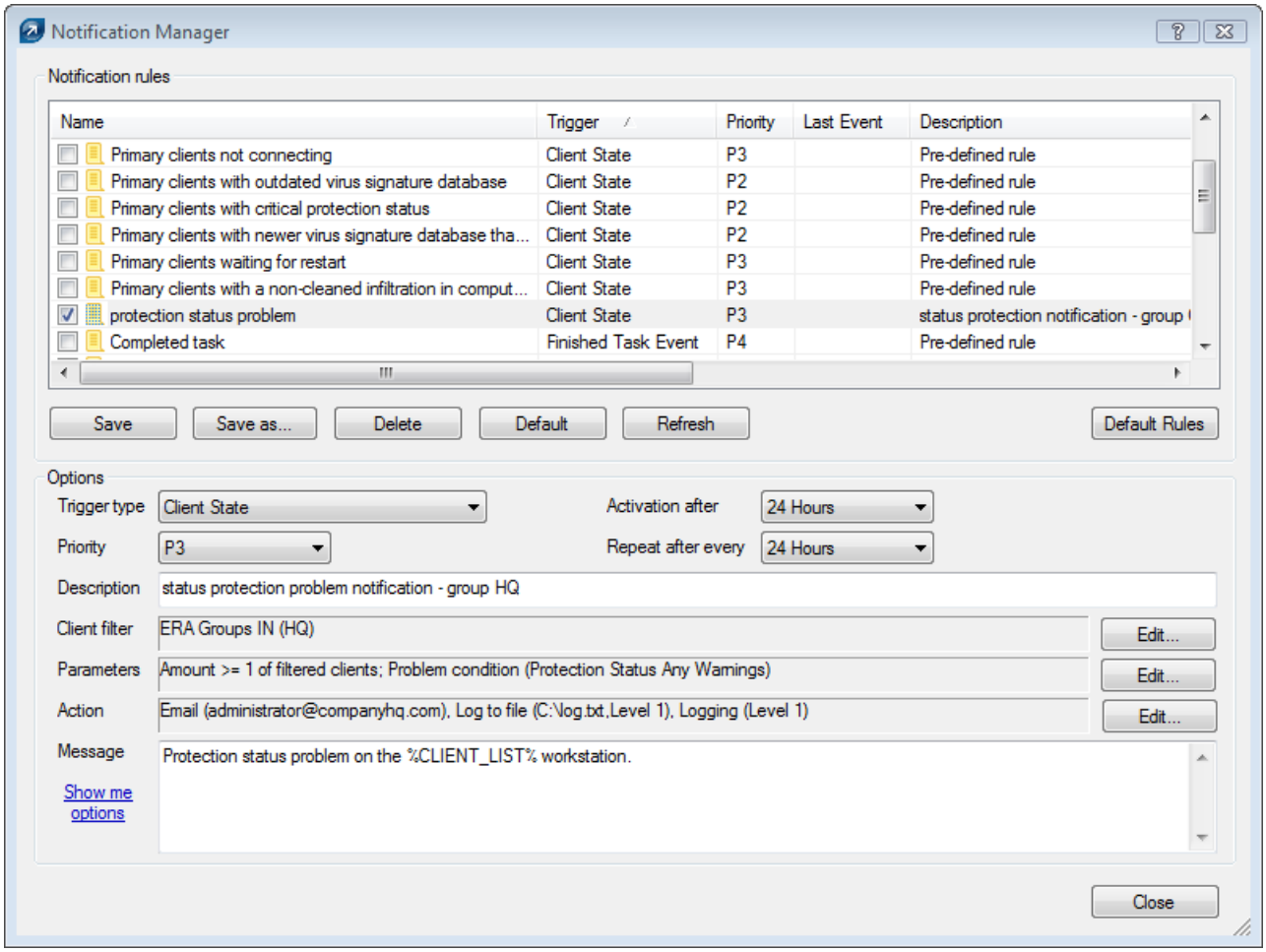
5) В меню **«Параметры» > «Изменить...»** укажите другие параметры для правила. Снимите все флажки кроме **«Состояние защиты: любые предупреждения»**.

6) Перейдите в раздел **«Действие** и нажмите кнопку **«Изменить...»**. В окне **«Действие»** выберите параметр **«Электронная почта»**, укажите получателя (поле **«Кому...»**) и **тему** письма. Затем установите флажок **«Журнал в файл»** и введите имя и путь к создаваемому журналу. Дополнительно для файла журнала можно указать уровень **детализации**. Для сохранения действия нажмите кнопку **OK**.

7) В поле **«Сообщение»** введите текст сообщения, отправляемого при срабатывании данного правила. Пример *«Клиент %CLIENT_LIST% сообщает о проблеме с состоянием защиты»*.

8) Нажмите кнопку **«Сохранить как...»**, укажите имя правила (например, *«проблемы с состоянием защиты»*) и выберите правило в списке правил уведомлений.

Готовое правило должно выглядеть примерно так, как показано на рисунке ниже.



Теперь правило активно. Оно применяется при обнаружении проблемы с защитой на клиенте из группы головного офиса. Администратор получит уведомление по электронной почте с вложением, содержащим название проблемного клиента. Нажмите кнопку **«Закрыть»**, чтобы выйти из диспетчера уведомлений.

5.5 Подробные сведения о клиентах

Приложение ERA позволяет получать сведения о выполняемых процессах и программах, запущенных на клиентских рабочих станциях. Эти сведения можно получать с помощью средства ESET SysInspector, которое встроено в сервер ERAS. Помимо других своих полезных функций, средство ESET SysInspector тщательно анализирует операционную систему и создает системные журналы. Чтобы открыть эту программу, выберите команду **«Служебные программы»** > **ESET SysInspector** в главном меню ERAC.

Если на определенном клиенте есть проблемы, можно запросить журнал ESET SysInspector с данного клиента. Для этого щелкните правой кнопкой мыши по клиенту на панели **«Запросить данные»** — **«Запрос данных SysInspector**. Журналы можно получать только с продуктов поколения 4.x; более ранние версии не поддерживают эту функцию. Откроется окно со следующими параметрами:

- **«Создать снимок (с записью результатов в журнал на клиенте)»** — копия журнала сохраняется на клиентском компьютере.

- **«Включить сравнение в последний снимок до указанного времени»** — отображается журнал сравнения. Журналы сравнения создаются путем слияния текущего журнала с доступным предыдущим журналом. Приложение ERA выберет первый из журналов, созданных до указанной даты.

Нажмите кнопку **OK**, чтобы получить выбранные журналы и сохранить их на сервере. Чтобы открыть и просмотреть журналы, выполните указанные ниже действия.

Параметры ESET SysInspector для отдельных клиентских рабочих станций находятся на вкладке **«Свойства клиента»** — **SysInspector**. Это окно разделено на три области; в верхней области отображается список последних журналов данного клиента. Чтобы загрузить последние сведения, нажмите кнопку **«Обновить»**.

Средний раздел окна **«Запрос параметров»** практически идентичен окну, появляющемуся при запросе требуемых журналов на клиентских рабочих станциях. Кнопка **Запрос** предназначена для получения с клиента журнала ESET SysInspector.

В нижней части окна есть следующие три кнопки.

- **«Вид»** — открытие журнала, указанного в верхнем разделе ESET SysInspector.
- **«Сохранить как...»** — сохранение текущего журнала в файл. Если включен параметр «С последующим просмотром файла в приложении ESET SysInspector», содержимое журнала автоматически отобразится после его сохранения (как при нажатии кнопки **«Вид»**).

Создание и просмотр новых журналов иногда может замедляться локальным клиентом из-за размера журнала и скорости передачи данных. Дата и время, назначенные журналу в разделе **«Свойства клиента»** > **SysInspector** отображают дату и время доставки на сервер.

5.6 Централизованный карантин

Централизованный карантин является мощным средством, которое позволяет администраторам легко работать с файлами, помещенными в карантин. Это упрощает выполнение таких действий, как просмотр, удаление, восстановление изолированных файлов и исключение их от дальнейших проверок. Карантин доступен в окне **«Карантин»** на главной панели консоли или в свойствах клиента. В главном окне карантина отображаются все сведения о файле, название угрозы, хэш, дата и время первого и последнего обнаружения, размер файла и количество заражений.

Примечание. Обратите внимание, что в полях **«Имя объекта»**, **«Имя файла»** и **«Расширение»** отображаются только первые три объекта. Для получения дополнительных сведений откройте окне свойств или нажмите клавишу **F3** или дважды щелкните выбранный элемент.

Централизованный карантин содержит обзор изолированных файлов, которые хранятся локально на клиентах и которые можно запросить для загрузки. Если файл запрошен, он копируется на сервер ERA Server в безопасном зашифрованном виде. По соображениям безопасности расшифровка выполняется перед сохранением файла на диск. Инструкции по работе с изолированными файлами см. в разделе Задача «Восстановить или удалить из карантина» 53.

Примечание. Для работы централизованного карантина на клиентах должен быть установлен EAV/ESS версии 4.2 или выше.

Qua...	Hash	DateReceived	Occurred First	Occurred Last	Object Name	File Name	Extension	Size	Reason	Client Cou...	Hits	File
3	d2726507...	8 days ago	12 months ago	3 months ago	http://www.eicar.o...	eicar_com....	zip	184	Eicar test file	1	32	Ready
2	bec1b52d...	8 days ago	12 months ago	12 months ago	https://secure.eica...	eicarcom2....	zip	308	Eicar test file	1	4	No Data
1	3395856c...	8 days ago	12 months ago	9 months ago	C:\Users\smid\Ap...	eicar.com, ...	com, tx...	68	Eicar test file...	1	14	No Data

6. Мастер объединения правил файервола

Мастер объединения правил файервола позволяет объединять правила для выбранных клиентов. Это особенно полезно, если необходимо создать единую конфигурацию со всеми правилами файервола, которые были собраны клиентами в режиме обучения. Полученную конфигурацию затем модно отправить клиентам посредством задачи конфигурации или применить как политику.

Мастер доступен в раскрывающемся меню **«Служебные программы»** и в контекстном меню на вкладке **«Клиенты»**, если щелкнуть правой кнопкой мыши выбранного клиента (выбранные клиенты затем автоматически добавляются в список выбранных элементов первого этапа).

Примечание. Для успешного выполнения этой операции для всех выбранных клиентов необходимо сохранить (отправить или реплицировать) последние конфигурации на сервере.

Процесс выполняется следующим образом. Сначала необходимо выбрать клиентов или группу клиентов, из которых будут собираться правила файервола для объединения. На следующем этапе будет показан список выбранных клиентов и их состояния конфигурации. Если конфигурация клиента отсутствует на сервере, запросите ее с помощью кнопки **«Запрос»**. На последнем этапе можно выбрать объединенные правила для использования в конфигурации и сохранить их в *XML*-файл.

7. Отчеты

Вкладка «Отчеты» предназначена для разделения статистической информации по графикам или диаграммам. После этого их можно сохранять и обрабатывать в формате значений, разделенных запятыми (CSV), с помощью средств ERA для вывода диаграмм и графиков. По умолчанию сервер ERA сохраняет выходные данные в формате HTML. Большая часть отчетов, связанных с заражением, создается в журнале угроз.

Для просмотра и выбора графических стилей можно воспользоваться раскрывающимся меню **«Стиль»** в разделе **«Отчет»**.

В ERA доступно несколько стандартных отчетов. Для выбора отчета предназначено раскрывающееся меню **«Тип»**.

- **«Клиенты с наибольшим количеством угроз»**
  Список наиболее «активных» клиентских рабочих станций (с наибольшим числом обнаруженных угроз).
- **«Пользователи с наибольшим количеством угроз»**
  Список наиболее «активных» пользователей (с наибольшим числом обнаруженных угроз).
- **«Наиболее часто встречающиеся угрозы»**
  Список угроз, обнаруживаемых чаще всего.
- **«Основные угрозы по распространенности»**
  Список основных угроз по распространенности.
- **«Динамика угроз»**
  Динамика событий, представляющих угрозу (в количественном выражении).
- **«Сравнительная динамика угроз»**
  Динамика представляющих опасность событий, связанных с указанными угрозами (которые отделяются с помощью фильтра), по сравнению с общим числом угроз.
- **«Угрозы по сканерам»**
  Количество сообщений об угрозах, поступивших от отдельных программных модулей.
- **«Угрозы по объектам»**
  Количество сообщений об угрозах, классифицированных по способу проникновения (через электронную почту, через файлы, через загрузочные сектора).
- **«Комбинированный: клиенты с наибольшим количеством угроз/наиболее часто встречающиеся угрозы»**
  Сочетание описанных выше типов.
- **«Комбинированный: наиболее часто встречающиеся угрозы/динамика угроз»**
  Сочетание описанных выше типов.
- **«Комбинированный: наиболее часто встречающиеся угрозы/сравнительная динамика угроз»**
  Сочетание описанных выше типов.
- **«Клиенты групп»**
  Вывод количества клиентов выбранных групп.
- **«Клиенты групп/все клиенты»**
  Вывод процентного отношения количества клиентов выбранных групп к общему количеству клиентов.
- **«Комбинированный: клиенты групп/клиенты»**
  Вывод количества клиентов для выбранных групп и клиентов в каждой группе в таблице (после щелчка по имени группы).
- **«Клиенты с наибольшим количеством сетевых атак»**
  Клиенты с наибольшим количеством сетевых атак
- **«Наиболее часто встречающиеся сетевые атаки»**
  Список наиболее часто встречающихся сетевых атак.
- **«Источники наиболее часто встречающихся сетевых атак»**
  Список источников наиболее часто встречающихся сетевых атак.
- **«Динамика сетевых атак»**
  Отображение динамики сетевых атак.
- **«Комбинированный: клиенты с наибольшим количеством сетевых атак/наиболее часто встречающиеся сетевые атаки»**
  Вывод клиентов с наибольшим количеством сетевых атак и наиболее часто встречающихся сетевых атак для каждого клиента в таблице (при щелчке по имени клиента).
- **«Клиенты с наибольшим количеством SMS-спама»**
  Список клиентов с наибольшим количеством SMS-спама.
- **«Наиболее активные SMS-спамеры»**
  Вывод наиболее активных SMS-спамеров для указанных адресатов.

- **«Динамика SMS-спама»**
  Вывод динамики SMS-спама.
- **«Комбинированный: клиенты с наибольшим количеством SMS-спама/наиболее активные SMS-спамеры»**
  Вывод клиентов с наибольшим объемом SMS-спама и наиболее часто встречающихся SMS-спамеров для каждого клиента в таблице (при щелчке по имени клиента).
- **«Отчет по клиентам»**, **«Отчет по угрозам»**, **«Отчет файервола»**, **«Отчет по событиям»**, **«Отчет по поверкам»**, **«Отчет по задачам»**, **«Мобильный отчет»**, **«Отчет по карантину»**
  Стандартные отчеты, которые можно просматривать на вкладках «Клиенты», «Журнал угроз», «Журнал событий», «Журнал сканирования» и «Задачи».
- **«Общий отчет об угрозах»**
  Сводка по отчетам «Комбинированный: клиенты с наибольшим количеством угроз/Наиболее часто встречающиеся угрозы», «Комбинированный: наиболее часто встречающиеся угрозы/Сравнительная динамика угроз», «Динамика угроз».
- **«Общий отчет о сетевых атаках»**
  Сводка по отчетам «Комбинированный: клиенты с наибольшим количеством сетевых атак/наиболее часто встречающиеся сетевые атаки», «Источники наиболее часто встречающихся сетевых атак», «Динамика сетевых атак».
- **«Общий отчет об SMS-спаме»**
  Сводка по отчетам «Комбинированный: клиенты с наибольшим количеством SMS-спама/наиболее активные SMS-спамеры», «Наиболее активные SMS-спамеры», «Динамика SMS-спама».

В разделе **«Фильтр»** можно с помощью раскрывающихся меню **«Целевые ПК»** или **«Угрозы»** выбрать клиенты, которые нужно включить в отчеты или исключить из них.

Открыть окно настройки других параметров можно с помощью кнопки **«Дополнительные настройки...»**. Эти настройки в основном относятся к данным в заголовке и в типах используемых графических диаграмм. При этом, однако, данные также можно фильтровать по состоянию выбранных атрибутов и выбирать формат для отчета (HTML, CSV).

Вкладка «Интервал» позволяет задавать интервал, за который будет создаваться отчет.

- **«Данное»**
  В отчет включены только события, произошедшие в указанный период — например, если отчет создан а среду, а в качестве интервала установлено значение «Текущая неделя», то в отчет включаются все события, произошедшие в понедельник, вторник и среду.

- **«Завершено»**
  В отчет включаются только события, которые произошли в указанный период (т. е. весь август или вся неделя с понедельника по воскресенье). Если установлен флажок **«Добавить также текущий период»**, в отчет будут включены события за последний завершенный период, включая момент создания.

Пример

Нужно создать отчет, включающий события последней календарной недели с понедельника по воскресенье. Этот отчет должен быть создан в следующую среду (после воскресенья).

На вкладке **«Интервал»** выберите **«Завершено»** и **«1 неделя»**. Снимите флажок **«Добавить также текущий период»**. На вкладке **«Планировщик»** установите для параметра **«Частота»** значение **«Еженедельно»** и выберите пункт **«Среда»**. Остальные параметры можно настроить по своему усмотрению.

- **«С/по»**
  Этот параметр позволяет задать период, для которого создается отчет.

На вкладке **«Планировщик»** можно задавать и настраивать автоматическое создание отчетов в указанное время или в выбранных интервалах (в разделе **«Частота»**).

После занесения отчета в планировщик нажмите кнопку **«Выбрать цель...»**, чтобы указать место для охранения отчета. Отчеты можно сохранять на сервере ERAS (по умолчанию), отправлять по электронной почте по указанному адресу или экспортировать в папку. Последний вариант необходим в том случае, если отчет отправляется в общую папку во внутренней сети организации, где может просматриваться другими работниками.

Для отправки созданных отчетов по электронной почте необходимо ввести адрес сервера SMTP и адрес отправителя в меню **«Служебные программы»** > **«Настройки сервера»** > **«Другие настройки»**.

Чтобы сохранить параметры настроенных отчетов в шаблон, нажмите кнопку **«Сохранить»** или **«Сохранить как...»**. При создании нового шаблона нажмите кнопку **«Сохранить как...»** и введите название шаблона.

В верхней части окна «Консоль» в разделе **«Шаблоны отчетов»** показаны названия созданных шаблонов. Рядом с именами шаблонов отображается время и интервалы, в соответствии с которыми создаются данные отчеты. Кнопка **«Создать сейчас»** (на вкладке **«Параметры»**) позволяет создать отчет в любой момент независимо от расписания.

Существующие шаблоны отчетов можно импортировать и экспортировать из/в *XML*-файл(а) с помощью кнопки **«Импорт.../Экспорт...»**. Конфликты имен при импорте (совпадение имен у существующих и импортируемых шаблонов) решаются путем добавления случайной строки после имени импортируемого шаблона.

Ранее созданные отчеты можно просмотреть на вкладке **«Созданные отчеты»**. Дополнительные параметры отчетов доступны в контекстном меню соответствующих отчетов или групп отчетов, которое вызывается с помощью правой кнопки мыши.

Шаблоны, помещенные в список **«Избранное»**, позднее можно использовать для создания новых отчетов. Чтобы переместить шаблон в «Избранное», щелкните его правой кнопкой мыши и выберите в контекстном меню команду **«Добавить в избранное»**.

7.1 Образец сценария отчета

Чтобы добиться максимальной сетевой безопасности для клиентов, необходимо иметь хорошее представление о состоянии безопасности сети. Можно с легкостью создавать отчеты с подробным описанием угроз, обновлений, версии клиентских продуктов и т. п. (дополнительные сведения см. в разделе Отчеты 78). Как правило, всю необходимую информацию содержит еженедельный отчет. Тем не менее, могут возникнуть ситуации, в которых окажется необходима дополнительная осторожность, например при обнаружении угрозы.

В качестве примера создадим параметрическую группу с названием *«Карантин»*. Эта группа будет содержать только те компьютеры, в которых угроза была обнаружена и устранена во время последней проверки по требованию. Зададим это условие, включив параметр **«При последнем сканировании обнаружена угроза»**. Для создания параметрической группы следуйте инструкциям в разделе Параметрические группы 56.

Примечание. При создании группы *«Карантин»* убедитесь в том, что параметр **«Закрепить»** отключен. Компьютер будет назначен в эту группу динамически и удален, как только условия перестанут выполняться.

Создайте отчет *«Компьютеры в карантине»*. Для создания отчета следуйте инструкциям в разделе Отчеты 78. Ниже указаны конкретные параметры для данного примера.

- Параметры шаблона **«Параметры»**:

«Тип»: **«Подробный отчет по карантину»**
«Вид»: **«Голубая схема»**
«Целевые клиенты»: **«Только выбранные группы»**
«Угроза»: **«н/д»**

- Параметры шаблона **«Интервал»**:

«Данный»: **«День»**

- Параметры шаблона **«Планировщик»**:

«Частота»: **«Ежедневно»**
«Кажд.»: **«1 день»**

Совет. Результаты можно сохранить в базы данных отчетов или указать папку, в которой будут сохранены копии отчетов. Отчеты также можно отправить по электронной почте. Все эти параметры вызываются с помощью кнопки **«Выбрать цель...»**.

Созданные отчеты можно просматривать в разделе **«Отчеты»** в шаблоне **«Общие отчеты»**.

Выводы. Была создана параметрическая группа *Карантин* с компьютерами, на которых была обнаружена

угроза в ходе последней проверки по требованию. Затем был создан автоматизированный отчет, который будет ежедневно информировать нас о том, какие компьютеры принадлежат группе «*Карантин*», что дает хорошее представление о состоянии сетевых клиентов, позволяя держать потенциальную угрозу под контролем.

Совет. Чтобы отобразить данные журнала последней проверки, можете воспользоваться отчетом типа **«Подробный отчет по сканеру»**.

8. Настройка сервера ESET Remote Administrator (ERAS)

8.1 Безопасность

Продукты безопасности ESET версии 3.x (ESET Smart Security и т. п.) поддерживают использование паролей, шифрующих обмен данными между клиентом и сервером ERAS (связь по протоколу TCP через порт 2222).

В более старых версиях (2.x) эта функциональная возможность отсутствует. Для обратной совместимости со старыми версиями должен быть активирован режим **«Включить доступ без аутентификации для клиентов»**.

На вкладке «Безопасность» представлены параметры, позволяющие администратору использовать версии 2.x и 3.x в одной сети.

- **«Пароль для консоли (доступ с правами администратора, доступ в режиме только для чтения)»**
  Позволяет указать пароль для администратора и ограниченного числа пользователей для защиты параметров ERAC от несанкционированного изменения.

- **«Пароль для клиентов (продукты ESET для обеспечения безопасности)»**
  Устанавливает пароль для доступа клиентов к ERAS.

- **«Пароль для репликации»**
  Устанавливает пароль для ERA Server нижнего уровня для репликации на данный сервер ERAS.

- **«Пароль для удаленного установщика ESET (агент)»**
  Устанавливает пароль для доступа агента программы установки к ERAS. Используется при удаленной установке.

- **«Включить доступ без аутентификации для клиентов (продукты ESET для обеспечения безопасности)»**
  Разрешает доступ к ERAS для клиентов с отсутствующим или недействительным паролем (если текущий пароль отличается от пароля для клиентов).

- **«Включить доступ без аутентификации для репликации»**
  Разрешает доступ к серверу ERAS для клиентов сервера ERA Server нижнего уровня, у которых отсутствует или является недействительным пароль для репликации.

- **«Включить доступ без аутентификации для удаленного установщика ESET (агент)»**
  Включает доступ к серверу ERAS для удаленного установщика ESET, в котором не указан действительный пароль.

Примечание. Если аутентификация включена на сервере ERAS и на всех клиентах поколения 3.x, параметр **«Включить доступ без аутентификации для клиентов»** можно отключить.

- **«Использовать аутентификацию Windows или домена»**
  Развешает проверку подлинности Windows/домен и позволяет задать группы администраторов (с полным доступом к ERA Server), а также группы с доступом только для чтения (параметр **«Для всех остальных пользователей доступ только для чтения»**).

8.2 Обслуживание сервера

При условии правильной настройки параметров на вкладке «Обслуживание сервера» для базы данных ERAS будет автоматически производиться обслуживание и оптимизация. По умолчанию записи и журналы старше шести месяцев удаляются, а через каждые пятьдесят дней выполняется задача «Сжатие и восстановление». Все параметры обслуживания сервера доступны в меню **«Служебные программы»** > **«Настройки сервера»** > **«Обслуживание сервера»**.

Ниже перечислены доступные команды.

- **«Удалять клиенты, не подключавшиеся в течение последних X месяцев (дней)»**
  Удаляет все клиенты, которые не подключались к ERAS более указанного числа месяцев (дней).

- **«Удалять журналы угроз старше X месяцев (дней)»**
  Удаляет все инциденты с вирусами старше указанного числа месяцев (дней).

- **«Удалять журналы файервола старше X месяцев (дней)»**
  Удаляет все журналы файервола старше указанного числа месяцев (или дней).

- **«Удалять журналы событий старше X месяцев (дней)»**
  Удаляет все системные события старше указанного числа месяцев (или дней).

- **«Удалять журналы проверки старше X месяцев (дней)**
  Удаляет все журналы модуля сканирования старше указанного числа месяцев (или дней).

- **«Удалять мобильные журналы старше X месяцев (дней)»**
  Удаляет все журналы мобильных устройств старше указанного числа месяцев (или дней).

- **«Удалять записи в карантине без клиентов старше X месяцев (дней)»**
  Удаляет все журналы модуля сканирования старше указанного числа месяцев (или дней).

«Планировщик очистки»
Выполняет выбранные выше действия с периодичностью, равной указанному числу минут.

«Планировщик сжатия и восстановления»
Сжимает базу данных с указанным интервалом в заданное время. При сжатии и восстановлении удаляются несогласованности и ошибки, что ускоряет обмен данными с базой.

8.3 Сервер зеркала

Функция зеркала позволяет создавать локальный сервер обновления. Клиентские компьютеры не загружают обновления сигнатур вирусов с сервера ESET в Интернете, а подключаются к локальному серверу-зеркалу в своей сети. Основным преимуществом этого решения является сокращение нагрузки на внешний канал и уменьшение трафика, поскольку для обновления к Интернету подключается только зеркало, а не сотни клиентских компьютеров. В такой конфигурации важно, чтобы зеркало было постоянно подключено к Интернету.

Предупреждение. В работе зеркала, выполнившего обновление компонентов программы, но еще не перезагруженного, возможны отказы. В этом случае сервер не сможет загружать обновления и рассылать их на клиентские рабочие станции. НЕ ВКЛЮЧАЙТЕ АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ ПРОГРАММНЫХ КОМПОНЕНТОВ ДЛЯ СЕРВЕРНЫХ ПРОДУКТОВ КОМПАНИИ ESET! Это не относится к зеркалу, созданному на сервере ERAS.

Работать с зеркалом можно из двух мест:

- ESET Remote Administrator (зеркало физически работает на сервере ERAS и управляется из консоли ERAC);

- ESET Smart Security Business Edition или ESET NOD32 Antivirus Business Edition (при условии, что пакет Business Edition был активирован с использованием лицензионного ключа).

Администратор выбирает способ активации функции зеркала.

В больших сетях можно создавать несколько зеркал (например, для различных отделений компании) и устанавливать одно из них в качестве центрального (в головном офисе) в каскадной конфигурации — аналогично конфигурации сервера ERAS с несколькими клиентами.

Администратор должен указать лицензионный ключ купленного продукта и ввести имя пользователя и пароль для активации функции зеркала на сервере ERAS. Если администратор использует лицензионный ключ, имя пользователя и пароль для ESET NOD32 Antivirus Business Edition, то при дальнейших обновлениях ESET Smart Security Business Edition исходный лицензионный ключ, имя пользователя и пароль также нужно заменить.

Примечание. Клиенты ESET NOD32 Antivirus могут также обновляться с помощью лицензии ESET Smart Security, но не наоборот.

8.3.1 Работа сервера зеркала

Компьютер, на котором находится сервер зеркала, должен быть постоянно включен и подключен к Интернету или зеркалу верхнего уровня для репликации. Пакеты обновления зеркала можно загружать двумя способами:

1. По протоколу HTTP (рекомендуется).
2. С помощью общего сетевого диска (SMB).

Сервер обновления ESET использует протокол HTTP с аутентификацией. Центральное зеркало должно иметь доступ к серверам обновления по имени пользователя (которое обычно имеет вид *EAV-XXXXXXX*) и пароль.

В сервер зеркала, который является частью ESET Smart Security и ESET NOD32 Antivirus, встроен HTTP-сервер (вариант 1).

Примечание. При использовании встроенного HTTP-сервера (без аутентификации) обеспечьте его недоступность за пределами своей сети (т. е. для клиентов, не охватываемых лицензией). Сервер не должен быть открыть для доступа из Интернета.

По умолчанию встроенный HTTP-сервер подключается через TCP-порт 2221. Не используйте этот порт для других приложений.

Примечание. Если используется HTTP-сервер, рекомендуется использовать не более 400 клиентов для одного зеркала. В крупных сетях с большим количеством клиентов рекомендуется разнести зеркала обновлений на дополнительные серверы ERA (или ESS/EAV). Если зеркало должно быть центральным на одном сервере, рекомендуется использовать HTTP-сервера другого типа, например Apache. В ERA также поддерживаются дополнительные способы аутентификации (например, на веб-сервере Apache используется способ .htaccess).

Второй способ (общая сетевая папка) требует совместного использования (с правами для чтения) папки, в которой содержатся пакеты обновления. В этом сценарии имя пользователя и пароль с правами на чтение папки обновления необходимо вводить на клиентской рабочей станции.

Примечание. Клиентские решения ESET используют учетную запись SYSTEM, поэтому их права доступа отличаются от прав доступа пользователя, находящегося в системе. Аутентификация требуется даже в том случае, если сетевой диск доступен группе пользователей «Все» (Everyone), в том числе текущему пользователю. Кроме того, для задания сетевого пути к локальному серверу следует использовать формат UNC. Не рекомендуется использовать формат *ДИСК*:\.

При использовании общей сетевой папки (вариант 2) рекомендуется создать уникальное имя пользователя (например, NODUSER). Эта учетная запись будет использоваться на всех клиентских компьютерах только для загрузки обновлений. Учетная запись NODUSER должна иметь права для чтения на общую сетевую папку, в которой находятся пакеты обновления.
Для получения доступа к сетевому диску введите полные данные аутентификации: *РАБОЧАЯ ГРУППА\Пользователь* или *ДОМЕН\Пользователь.*.

Помимо данных для аутентификации, необходимо также задать источник обновлений для клиентских решений ESET. Источником обновления может быть URL-адрес локального сервера (*http://имя_сервера_зеркала:порт*) либо UNC-путь к сетевому диску: (*имя_сервера_зеркала\имя_общего_ресурса*).

8.3.2 Типы обновлений

Помимо обновлений БД сигнатур вирусов (которые могут включать обновления ядра программного обеспечения ESET), выполняются также обновления программных компонентов. Обновления программных компонентов добавляют новые функции в продукты безопасности ESET и требуют перезагрузки компьютера.

Сервер зеркала позволяет администратору отключать автоматическую загрузку обновлений программы с серверов обновления ESET (или с зеркала верхнего уровня) и их рассылку на клиенты. Позднее администратор сможет активировать рассылку вручную (например, когда он будет уверен, что это не приведет к конфликту между новой версией и существующими приложениями).

Эта функция особенно необходима, если администратору нужно загружать обновления БД сигнатур вирусов вместе с новой версией программы. При использовании более старой версии программы вместе с последней версией БД сигнатур вирусов программа будет продолжать обеспечивать наилучшую защиту. Однако для получения доступа к новым функциям рекомендуется загружать и устанавливать последние версии программы.

По умолчанию программные компоненты не загружаются автоматически и их загрузку нужно настраивать вручную на сервере ERAS. Дополнительные сведения см. в разделе Включение и настройка зеркала 85.

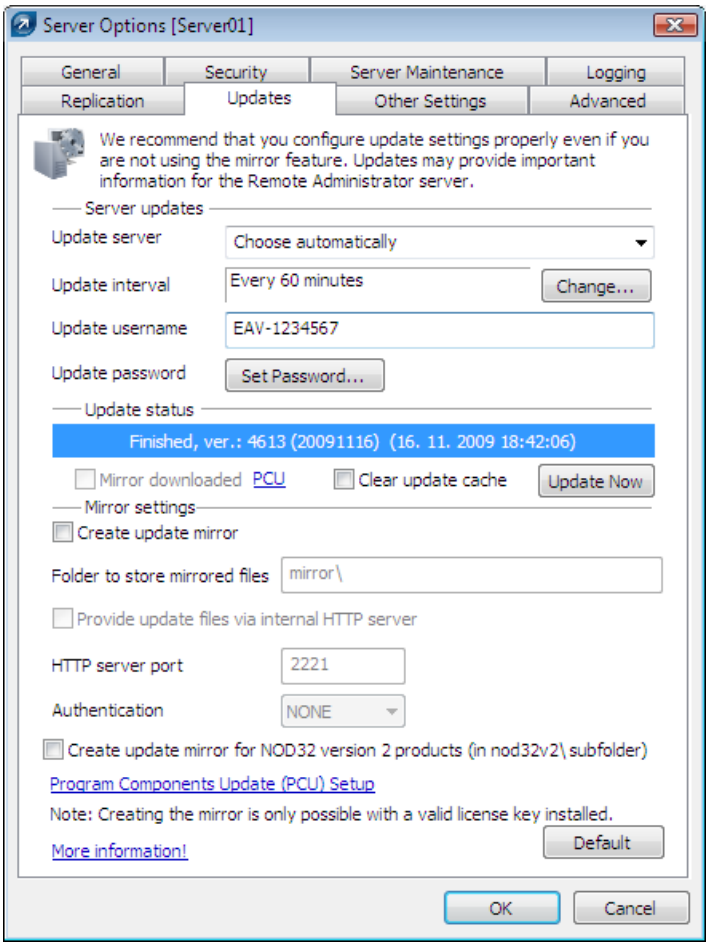
8.3.3 Включение и настройка зеркала

Если зеркало встроено непосредственно в ERA (компонент Business Edition), подключитесь к серверу ERAS с помощью консоли ERAC и выполните указанные ниже действия.

- В консоли ERAC выберите команду **«Служебные программы»** > **«Настройки сервера...»** > **«Обновления»**.
- В раскрывающемся меню **«Сервер обновлений»** выберите пункт **«Выбирать автоматически»** (обновления будут загружаться с серверов ESET) или введите URL-адрес или путь к зеркалу в формате *URL/UNC*.
- Установите интервал обновления (рекомендуется 60 минут).
- Если в предыдущем шаге было выбрано **«Выбирать автоматически»**, введите имя пользователя (имя пользователя для обновления) и пароль (пароль для обновления), полученные после приобретения продукта. При доступе к серверу верхнего уровня введите правильное имя пользователя домена и пароль для данного сервера.
- Выберите пункт **«Создать зеркало обновления»** и введите путь к папке, в которой будут храниться файлы обновления. По умолчанию это относительный путь к папке зеркального отображения, если выбран параметр **«Передавать файлы обновления с помощью внутреннего HTTP-сервера»**, а зеркало доступно по порту HTTP, заданному в поле **«Порт HTTP-сервера»** (по умолчанию 2221). Установите для параметра **«Аутентификация»** значение **«НЕТ»** (дополнительные сведения см. в разделе Работа сервера зеркала 84).

Примечание. При возникновении проблем с обновлением нажмите кнопку **«Очистить кэш обновлений»**, чтобы удалить содержимое папки с временными файлами.

- Параметр **«Зеркало загруженных обновлений программных компонентов»** позволяет активировать зеркала для программных компонентов. Чтобы настроить зеркала для обновлений программных компонентов, используйте команду **«Дополнительно» > «Изменить дополнительные настройки»** и настройте параметры в **ESET Remote Administrator** > **ERA Server** > **«Настройка» > «Зеркало»** (или **«Зеркало для NOD32 версии 2»**).
- Выберите компоненты, которые должны загружаться, в меню **«Дополнительно»** > **«Изменить дополнительные настройки...»** в разделе **ERA Server** > **«Настройка»** > **«Зеркало»** > **«Создать зеркало для выбранных компонентов программы»**. Выберите все языковые версии компонентов, которые будут использоваться в данной сети. Учтите, что загрузка языковой версии, которая не установлена в сети, будет увеличивать объем сетевого трафика.



Функция зеркала также доступна непосредственно из интерфейса программ ESET Smart Security Business Edition и ESET NOD32 Antivirus Business Edition. Администратор сам решает, с помощью какой из них будет создан сервер зеркала.

Чтобы активировать и запустить зеркало в ESET Smart Security Business Edition или ESET NOD32 Antivirus Business Edition, выполните указанные ниже действия.

1) Установите приложение ESET Smart Security Business Edition или ESET NOD32 Antivirus Business Edition.

2) В окне **«Дополнительные настройки»** (F5) выберите команду **«Разное»** > **«Лицензии»**. Нажмите кнопку **«Добавить...»**, укажите путь к файлу *.lic и нажмите кнопку **«Открыть»**. Это позволит выбрать лицензию и настроить функцию зеркала.

3) В разделе **«Обновление»** нажмите кнопку **«Настройка...»** и щелкните вкладку **«Зеркало»**.

4) Выберите параметры **«Создать зеркало обновления»** и **«Передавать файлы обновления с помощью внутреннего HTTP-сервера»**.

5) Введите полный путь к папке (**«Папка для дублируемых файлов»**), где будут храниться файлы обновления.

6) Параметры **«Имя пользователя»** и **«Пароль»** служат для аутентификации клиентских рабочих станций, пытающихся получить доступ к папке зеркального отображения. В большинстве случаев заполнять эти поля не требуется.

7) Установите для параметра «Аутентификация» значение **«НЕТ»**.

8) Выберите компоненты для загрузки (компоненты всех языковых версий, которые будут использоваться в данной сети). Компоненты отображаются только в случае, если они доступны на серверах обновления ESET.

Примечание. Для обеспечения оптимальной работы рекомендуется включать загрузку и зеркалирование программных компонентов. Если этот параметр отключен, обновляются только БД сигнатур вирусов, а программные компоненты не обновляются. Если зеркало является частью ERA, этот параметр можно настроить в консоли ERAC в меню **«Служебные программы»** > **«Настройки сервера...»** > вкладка **«Дополнительно»** > **«Изменить дополнительные настройки...»** > **ESET Remote Administrator** > **ERA Server** >

«Настройка» > **«Зеркало»**. Включите все языковые версии программы, присутствующие в сети.

8.3.4 Зеркало для клиентов NOD32 версии 2.x

В ESET Remote Administrator также можно создавать копии файлов обновления на клиентских компьютерах, на которых установлен продукт ESET NOD32 Antivirus 2.x. Для этого воспользуйтесь меню **«Служебные программы»** > **«Настройки сервера»** > **«Обновления»** > **«Создать зеркало обновления для продуктов NOD32 версии 2»**. Это относится только к ERA; в функциональности зеркала, включенной в корпоративное клиентское решение (версии 3.x), эта функция отсутствует.

Если в сети используются клиенты с версиями 2.x и 3.x в сочетании, рекомендуется использовать зеркало, встроенное в ERA. Если оба зеркала активированы на одном и том же компьютере (одно на сервере ERAS для клиентов версии 2.x, а другое в клиентской программе Business Edition версии 3.x), это может привести к конфликту между серверами HTTP, использующими один и тот же TCP-порт.

Обновления клиентов версии 2.x хранятся в подкаталоге *"nod32v2"* главного каталога зеркального отображения. Он доступен по адресу

http://имя_сервера_зеркала:порт/nod32v2

или по UNC-пути к сетевому диску

\\имя_сервера_зеркала\имя_общего_ресурса\nod32v2.

ERA также может загружать программные компоненты клиентов версии 2.x. Чтобы выбрать программные компоненты для загрузки, воспользуйтесь меню **«Служебные программы»** > **«Настройки сервера...»** > вкладка **«Дополнительно»** > команда **«Изменить дополнительные настройки...»** и разверните ветку **ESET Remote Administrator** > **ERA Server** > **«Настройка»** > **«Зеркало NOD32 версии 2»**. Чтобы уменьшить объем загружаемых данных, загружайте только те языковые версии, которые присутствуют в вашей сети.

8.4 Репликация

Репликация используется в больших сетях с несколькими серверами ERA Server, например в компании с нескольким подразделениями. Дополнительные сведения см. в разделе Установка 18.

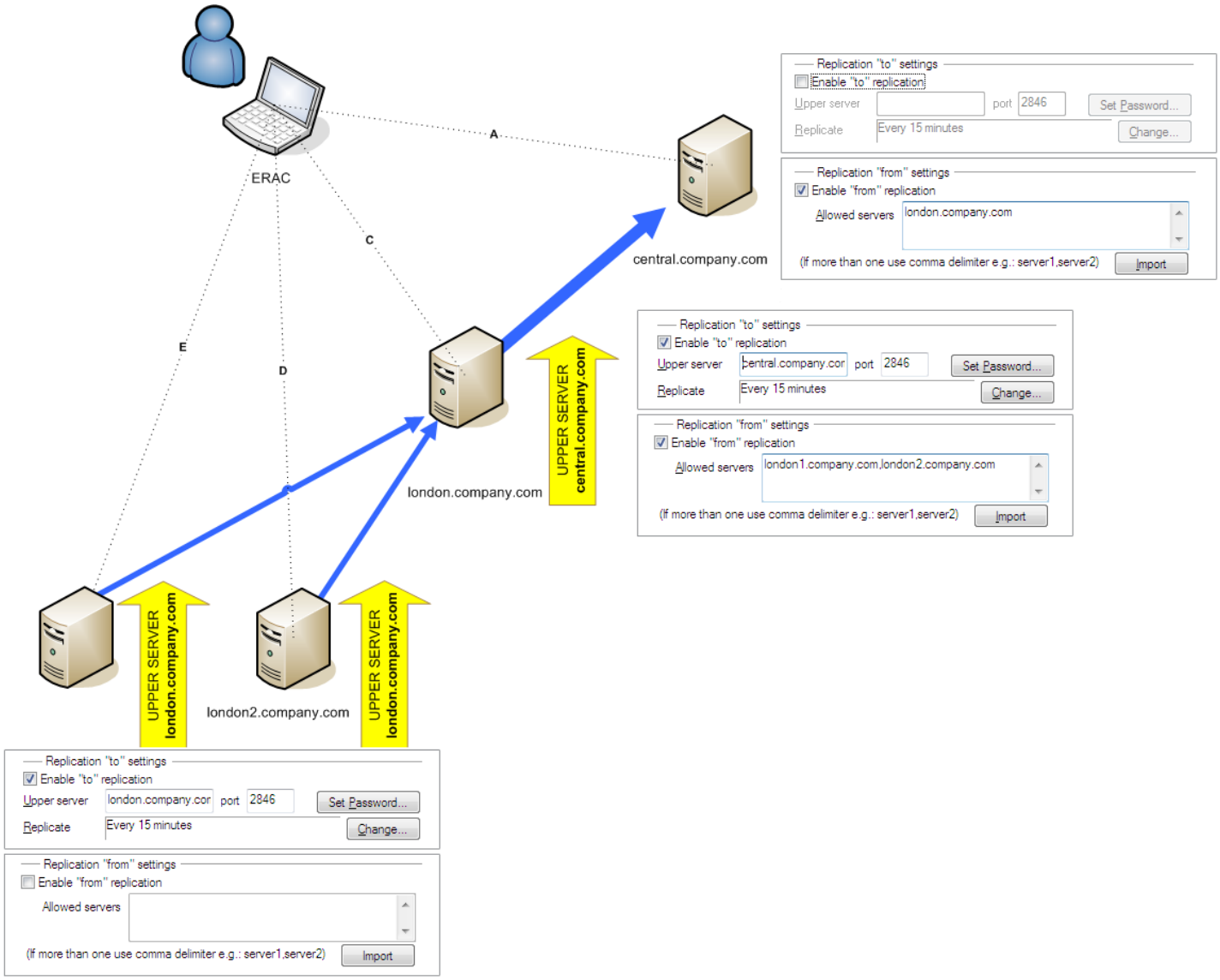
Параметры на вкладке «Репликация» (**«Служебные программы» > «Настройки сервера...»**) разделены на две части:

- «Параметры репликации „на“»
- «Параметры репликации „из“»

Раздел **«Параметры репликации "на"»** предназначен для настройки подчиненных серверов ERA Server. Необходимо активировать параметр **«Включить репликацию "на"»** и указать IP-адрес или имя главного сервера ERAS (верхнего уровня). После этого данные с подчиненного сервера реплицируются на основной сервер. **«Параметры репликации "из"»** позволяют основным серверам ERA Server (верхнего уровня) принимать данные от подчиненных серверов ERA Server или передавать их своим вышестоящим серверам. Необходимо активировать параметр **«Включить репликацию "из"»** и ввести названия подчиненных серверов, разделенные запятыми.

Для серверов ERA Server, находящихся внутри иерархии репликации (например, имеющих и подчиненный сервер, и сервер верхнего уровня), оба эти параметра должны быть включены.

Все вышеперечисленные сценарии показаны на рисунке ниже. Отдельные серверы ERA Server выделены бежевым цветом. Каждый из серверов ERAS представлен в окне репликации своим именем (которое во избежание путаницы должно совпадать со значением переменной *%Computer Name%*) и соответствующими параметрами.



Другие параметры, влияющие на репликацию серверов.

- **«Реплицировать журнал угроз»**, **«Реплицировать журнал файервола»**, **«Реплицировать журнал событий»** , **«Реплицировать журнал сканирования»**, **«Реплицировать мобильный журнал»**, **«Реплицировать журнал карантина»**
  Если выбраны эти параметры, все данные, отображаемые на вкладках **«Клиенты»**, **«Журнал угроз»**, **«Журнал файервола»**, **«Журнал событий»**, **«Журнал сканирования»**, **«Мобильный журнал»**, **«Журнал карантина»** и **«Задачи»**, реплицируются в отдельные строки и столбцы. Информация, хранящаяся не в базе данных, а в отдельных файлах (например, в текстовом (*TXT*) или *XML*-формате), может не реплицироваться. Включение этих параметров позволит реплицировать записи в таких файлах.

- **«Автоматически реплицировать данные журнала угроз»**, **«Автоматически реплицировать данные журнала сканирования»**, **«Автоматически реплицировать данные клиента»**, **«Автоматически реплицировать данные мобильного журнала»**, **«Автоматически реплицировать файлы карантина»**
  Эти параметры позволяют автоматически реплицировать подробные данные, хранящиеся в отдельных файлах. Их также можно загрузить по требованию, нажав кнопку **«Запрос»**.

Примечание. Некоторые журналы реплицируются автоматически, в то время как подробные журналы и журналы настройки клиента реплицируются только по запросу. Это связано с тем, что некоторые журналы содержат большие объемы данных, которые могут являться несущественными. Например, журнал сканирования с включенным параметром «Регистрировать все файлы» будет занимать много места на диске. Такая информация обычно не нужна и запрашивается вручную. Дочерние серверы не отправляют данные об удаленных клиентах автоматически. В связи с этим серверы верхнего уровня могут продолжать хранить сведения о клиентах, удаленных с подчиненных серверов. Чтобы удалить клиента с вкладки «Клиенты» на серверах верхнего уровня, выберите в меню **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные настройки»** > **«Настройка»** > **«Репликация»** для подчиненных серверов параметр «Включить удаление реплицированных клиентов».

Чтобы установить уровень обслуживания в ERAS, выберите меню **«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные настройки...»** > **«Настройка»** > **«Обслуживание сервера»**.

Если необходимо реплицировать только клиенты с изменением состояния, выберите команду **«Служебные программы»** > **«Настройки сервера»** > **«Репликация»** > **«Отметить все клиенты для репликации как "Начать репликацию"»**.

8.5 Ведение журнала

При работе ERAS создает журнал (параметр **«Имя файла журнала»**) с перечнем выполненных действий, детализацию которого также можно настроить (**«Степень детализации журнала»**). Если выбран параметр **«Записывать журнал в текстовый файл»**, новые файлы журнала будут создаваться (**«Ротация, если более X МБ»**) и удаляться (**«Удалять журналы старше X дней»**) ежедневно.

Параметр **«Записывать журнал в журнал приложений ОС»** разрешает копирование информации в журнал системных событий (**«Панель управления Windows»** > **«Администрирование»** > **«Просмотр событий»**).

При обычных условиях параметр **«Журнал отладки базы данных»** следует отключить.

По умолчанию выходные текстовые данные сохраняются в файл
%ALLUSERSPROFILE%\Application data\Eset\ESET Remote Administrator\Server\logs\era.log

Рекомендуется оставить уровень детализации «Уровень 2 — То же + Ошибки сеанса». Менять уровень детализации следует только при возникновении проблем или после получения соответствующей рекомендации от сотрудников службы поддержки клиентов ESET.

Для настройки степени сжатия для отдельных журналов выберите в меню команду **«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные настройки...»** > **«Настройка»** > **«Ведение журнала»** > **«Сжатие журнала отладки»**.

8.6 Управление лицензиями

Для нормальной работы ERA необходимо загрузить на сервер ключ лицензии. При покупке вместе с ключами лицензий на адрес электронной почты отправляется имя пользователя и пароль. Для управления лицензий предназначен **Диспетчер лицензий**.

В ERA версии 3.x и старше была добавлена поддержка нескольких ключей лицензий. Благодаря этой функции управлять ключами стало гораздо удобнее.

Главное окно диспетчера лицензий вызывается с помощью команды **«Служебные программы»** > **«Диспетчер лицензий»**.

Для добавления нового ключа лицензии выполните указанные ниже действия.

1) Выберите команду **«Служебные программы»** > **«Диспетчер лицензий»** или нажмите сочетание клавиши **CTRL+L**.
2) Нажмите кнопку **«Обзор»** и найдите нужны файл ключа лицензии (это файлы с расширением *LIC*).
3) Нажмите кнопку **«Открыть»**, чтобы подтвердить выбор.
4) Проверьте правильность лицензионного ключа и нажмите кнопку **«Загрузить на сервер»**.
5) Нажмите кнопку **«ОК»** для подтверждения.

Кнопка **«Загрузить на сервер»** станет активна только после выбора файла лицензии с помощью кнопки **«Обзор»**. В этой части окна отображаются сведения о ключе лицензии. Это позволяет еще раз проверить данные, прежде чем копировать ключ на сервер.

В центральной части окна отображается информация о ключе лицензии, который сейчас используется на сервере. Для просмотра подробных сведений о доступных на сервере ключах лицензии нажмите кнопку **«Детали...»**.

Сервер ERAS может выбрать из нескольких ключей лицензии самый подходящий и объединить несколько ключей в один. Если загружено несколько ключей лицензии, сервер ERAS будет всегда искать ключ с

наибольшим числом клиентов и самой поздней датой истечения срока действия.

Функция объединения нескольких ключей работает только в том случае, если эти ключи принадлежат одному пользователю. Объединение лицензий — это простой процесс, при котором создается новый ключ с количеством клиентов, равным общему числу клиентов на всех объединяемых серверах. Дата истечения срока действия нового ключа лицензии берется из ключа, срок действия которого истекает первым.

В нижней части окна диспетчера лицензий отображаются уведомления о проблемах с лицензиями. Доступны перечисленные ниже варианты.

- **«Предупредить, если срок действия лицензии сервера истекает через 20 дней»** — за X дней до истечения срока действия лицензии выводится предупреждение.
- **«Предупреждать, только если это приведет к падению числа клиентов в лицензии ниже фактического числа клиентов на сервере базы данных»** — этот вариант предписывает выводить предупреждение только в случае, если истечение срока действия лицензии или ее части приведет к падению числа клиентов ниже числа подключенных в данный момент клиентов или клиентов в базе данных сервера ERAS.
- **«Предупреждать, если в лицензии сервера осталось только 10% свободных клиентов»** — сервер выведет предупреждение в случае, если число свободных клиентов упадет ниже указанного значения (в процентах).

Сервер ERAS может объединить несколько ключей разных владельцев. Эта функция активируется с помощью специального ключа. Для получения такого ключа необходимо отметить это в заказе или связаться с местным распространителем компании ESET.

8.7 Дополнительные настройки

Дополнительные настройки ERA доступны в меню **«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные параметры»**.

Вкладка «Дополнительные настройки» содержит следующие параметры.

- **«Максимальное использование дискового пространства (процент)»**
  При превышении этого значения некоторые функции сервера могут стать недоступны. При подключении к серверу ERAS в консоли ERAC выводится уведомление при превышении указанного значения
- **«Шифрование обмена данными по протоколу»**
  Определяет тип шифрования. Рекомендуется оставлять значение по умолчанию.
- **«Включить переименование MAC-адреса (с неизвестного на действительный)»**
  После перехода с клиентского решения ESET, не поддерживающего отправку MAC-адреса (например, ESET NOD32 Antivirus 2.x), на клиентское решение, которое ее поддерживает (например, клиенты версии 3.x), запись старого клиента будет преобразована в новую. Рекомендуется оставлять значение по умолчанию («Да»).
- **«Включить переименование MAC-адреса (с действительного на неизвестный)»**
  После перехода с клиентского решения ESET, не поддерживающего отправку MAC-адреса (например, ESET NOD32 Antivirus 3.x), на клиентское решение, которое ее поддерживает (например, клиенты версии 2.x), запись старого клиента будет преобразована в новую. Рекомендуется оставлять значение по умолчанию («Нет»).
- **«Включить переименование MAC-адреса (с действительного на другой действительный)»**
  Включает переименование действительных MAC-адресов. Значение по умолчанию не позволяет выполнять переименование, что означает, что MAC-адрес участвует в уникальной идентификации клиентов. Отключите этот параметр, если для одного ПК имеется несколько записей. Рекомендуется также отключать этот параметр, если клиент идентифицируется как тот же клиент после изменения MAC-адреса.
- **«Включить переименование компьютера»**
  Позволяет переименовывать клиентские компьютеры. Если этот параметр отключен, имя компьютера будет участвовать в уникальной идентификации клиентов.
- **«Использовать вход на сервер по умолчанию во время автоматической установки»**
  Сервер ERAS позволяет задавать имя пользователя и пароль только для сценария входа и удаленной установки по электронной почте. Включение этого параметра позволяет использовать предопределенные значения и для автоматической удаленной установки.

8.8 Другие настройки

«Настройки SMTP»
Для некоторых функций ERA требуется правильная настройка сервера SMTP. В число этих функций входит удаленная установка по электронной почте и создание электронных сообщений.

«Новые клиенты»

«Вкл. новые клиенты»
Если этот параметр отключен, новые клиенты не добавляются на вкладку «Клиенты» — даже если к серверам ERA Server подключены новые клиенты, они не отображаются на этой вкладке.

«Автоматически сбрасывать флаг "Новый" для новых клиентов»
Если этот параметр включен, флаг «Новый» снимается на клиентах, подключающихся к серверу ERAS в первый раз. Дополнительные сведения см. в разделе Вкладка «Клиенты» 27.

«Порты»
Позволяет настраивать порты, на которых сервер ERAS ожидает подключений, с помощью следующих параметров: **«Консоль»** (по умолчанию 2223), **«Клиент»** (по умолчанию 2222), процесс репликации (**«Порт репликации»** по умолчанию 2846), **«Удаленный установщик ESET»** (по умолчанию 2224).

ThreatSense.Net
Если параметр включен, ERAS будет отправлять подозрительные файлы и статистические сведения клиентов на серверы ESET. Клиентские рабочие станции не всегда могут напрямую отправлять эти сведения из-за особенностей сетевой конфигурации.

9. ESET Remote Administrator Maintenance Tool

Средство ESET Remote Administrator Maintenance Tool предназначено для выполнения конкретных задач по обслуживанию сервера. Средство вызывается через меню **«Пуск»** > **«Все программы»** > **ESET Remote Administrator** > **«Сервер»**. При запуске средства ERA Maintenance появится интерактивный мастер, который поможет в выполнении необходимых задач.

Примечание. Чтобы сервер ERA Maintenance Tool нормально работал в системе Windows NT4 с пакетом обновления 6 (SP6), установите браузер Internet Explorer 5.0 или более поздней версии либо, по крайней мере, обновите библиотеку общих элементов управления (comctl32.dll). Библиотека ComCtl32 входит в состав пакета Platform SDK Comctl32 Redistributables, и ее можно загрузить на веб-сайте Майкрософт.

9.1 Сведения о ERA Server

Средство отображает сводку данных об установленном сервере ERA Server. Показанные сведения можно рассмотреть более подробно в отдельном окне, выбрав команду **«Дополнительные сведения»**, их можно скопировать в буфер обмена командой **«Копировать в буфер»** и обновить затем с помощью команды **«Обновить»**. После просмотра сведений переходите к следующему шагу с помощью кнопки далее **«Далее»**.

9.2 Тип задачи

Средство обслуживания содержит список доступных задач. В конце каждой задачи настройки можно сохранить параметры текущей задачи, нажав кнопку **«Сохранить все параметры в файл»**. Эти параметры затем можно использовать в любое время с помощью кнопки **«Загрузить все параметры из файла»**. В каждом шаге задачи настройки также есть функция **«Сохранить все параметры в файл»** или **«Загрузить все параметры из файла»**.

9.2.1 Остановка сервера ERA Server

Данная задача останавливает службу ESET Remote Administrator Server.

9.2.2 Запуск сервера ERA Server

Данная задача запускает службу ESET Remote Administrator Server.

9.2.3 Передача базы данных

Данная задача позволяет преобразовать формат базы данных. Это средство может выполнять преобразование между следующими типами баз данных:

- MS Access
- MS SQL Server
- Oracle
- MySQL

В первом шаге выбирается база данных.

Если базой данных является MS Access, укажите путь к *MDB*-файлу. По умолчанию используется путь, указанный во время установки ERA Server.
Для всех остальных форматов БД необходимо указать дополнительные параметры.

- Строка соединения: специальная строка, используемая для идентификации исходной базы данных.
- Имя пользователя: имя пользователя для доступа к базе данных.
- Пароль: пароль для доступа к базе данных.
- Название схемы: название схемы (только для Oracle и MS SQL).

Выберите пункт **«Загрузить текущую конфигурацию сервера»**, чтобы использовать текущие параметры ERA Server. Нажмите кнопку **«Проверить соединение»**, чтобы проверить соединение с сервером базы данных. Если соединение не удается установить, проверьте правильность параметров. После успешной проверки связи с БД переходите к следующему шагу, нажав кнопку **«Далее»**.

Выберите целевую базу данных. Выберите пункт **«Заменить параметры подключения к серверу»**, чтобы подключиться к серверу и использовать новую базу данных после успешного преобразования. Если не выбрать этот параметр, новая база данных будет создана без обновления сервера до новой версии базы данных.

Для всех типов баз данных (кроме MS Access) решите, нужно ли автоматически создавать таблицы базы данных (**«Автоматически создать таблицы в новой базе данных»**) или вставьте таблицы в базу данных позже (**«Просмотреть сценарий»** > **«Сохранить в файл»**) в следующем шаге. Для СУБД MS SQL параметр **«Автоматически создать новую базу данных ESETRADB»** автоматически создает новую БД MySQL с именем ESETRADB. Последним шагом является подтверждение преобразования базы данных.

9.2.4 Резервное копирование базы данных

Это средство позволяет создавать файл резервной копии базы данных. Параметры в первом окне похожи на параметры преобразования базы данных (см. раздел Передача базы данных 92). В этом окне выбрана исходная база данных. Исходная база данных будет скопирована в файл резервной копии, указанный в следующем шаге.

Необязательные параметры в нижней части окна позволяют перезаписать существующий файл (**«Перезаписать, если существует»**), а также остановить ESET Remote Administrator Server во время резервного копирования (**«Остановить сервер во время обработки»**). Чтобы подтвердить выполнение задачи, нажмите кнопку далее **«Далее»**.

9.2.5 Восстановление базы данных

Данная задача позволяет восстановить базу данных из файла резервной копии. Параметры в первом окне похожи на параметры преобразования базы данных (см. раздел Передача базы данных 92). В этом окне выбран тип база данных.

Для всех типов баз данных (кроме MS Access) решите, нужно ли автоматически создавать таблицы базы данных (**«Автоматически создать таблицы в новой базе данных»**) или вставьте таблицы в базу данных позже (**«Просмотреть сценарий»** > **«Сохранить в файл»**) в следующем шаге. Для СУБД MS SQL параметр **«Автоматически создать новую базу данных ESETRADB»** автоматически создает новую БД MySQL с именем ESETRADB. Последним шагом является подтверждение преобразования базы данных.

Выберите файл, из которого будет восстановлена БД в следующем шаге. Необязательные параметры в нижней части окна позволяют импортировать файлы из баз данных различных типов, выбранных в предыдущем шаге (**«Разрешить импорт баз данных различных типов»**), а также останавливать ESET Remote Administrator Server во время восстановления базы данных (**«Остановить сервер во время обработки»**). Нажмите кнопку далее **«Далее»** для подтверждения выполнения задачи.

9.2.6 Удаление таблиц

Данная задача удаляет текущие таблицы в базе данных. В результате база данных будет возвращена в состояние, которое было после установки ERA Server. Параметры в первом окне похожи на параметры преобразования базы данных (см. раздел Передача базы данных 92). В этом окне выбран тип база данных. В следующем шаге будет выведен запрос на подтверждение действия. выберите **«Да, принимаю»** и нажмите кнопку **«Далее»** для подтверждения действия.

Примечание. Если используется СУБД MS SQL, MySQL или Oracle, перед удалением этих таблиц рекомендуется остановить ERA Server.
Если используется СУБД MS Access, она будет заменена пустой базой данных по умолчанию.

9.2.7 Установка нового лицензионного ключа

Чтобы добавить новый лицензионный ключ для использования на сервере, укажите путь к новому лицензионному ключу.
Замените существующий ключ лицензии в случае необходимости (**«Перезаписать, если существует»**) и перезапустить сервер при необходимости (**«Принудительно запустить сервер (если он не запущен)»**).
Нажмите кнопку далее **«Далее»** для подтверждения и выполнения задачи.

9.2.8 Изменение конфигурации сервера

Эта задача запускает Configuration Editor (если он установлен). По окончании задачи открывается окно редактора конфигураций, в котором можно изменять дополнительные параметры ERA Server. Эти параметры также доступны в меню **«Служебные программы»** > **«Настройки сервера»** > **«Дополнительно»** > **«Изменить дополнительные настройки»**.

Примечание. Для работы этой функции должен быть установлен ERA Console.

10. Устранение неполадок

10.1 Часто задаваемые вопросы

В этой главе даны ответы на наиболее часто задаваемые вопросы и решения для проблем, связанных с установкой и функционированием ERA.

10.1.1 Проблемы, связанные с установкой ESET Remote Administrator на Windows Server 2000/2003

Причина
Одной из возможных причин может быть работа сервера терминалов в режиме *выполнения*.

Решение
Корпорация Microsoft рекомендует устанавливать сервер терминалов в режим *установки*, если он запущен при установке в системе программ. Это можно сделать в оснастке **«Панель управления»** > **«Установка или удаление программ»** или с помощью команды *change user /install* в командной строке. После установки введите *change user /execute* для возврата сервера терминалов в режим выполнения. Описание пошаговых инструкций этого процесса см. в следующей статье: http://support.microsoft.com/kb/320185.

10.1.2 Значения кода ошибки GLE

При установке ESET Smart Security или ESET NOD32 Antivirus в консоли ESET Remote Administrator Console может возникать ошибка GLE. Чтобы определить номер ошибки GLE, выполните следующие действия.

1) Откройте окно командной строки, выбрав в меню пункт **«Пуск»** > **«Выполнить»**. Введите *cmd* и нажмите кнопку **OK**.
2) В командной строке введите *net helpmsg номер_ошибки*.

Пример *net helpmsg 55*

Пример результата: The specified network resource or device is no longer available («Указанный сетевой ресурс или устройство больше не доступны»).

10.2 Часто встречающиеся коды ошибок

Во время работы ERA могут выводиться сообщения об ошибках, коды которых указывают на проблему с некоторой функцией или действием. В разделах ниже дано краткое описание кодов ошибок, которые возникают при автоматической установке, а также ошибок, которые содержатся в журнале сервера ERAS.

10.2.1 Сообщения об ошибках, выводимые при удаленной установке ESET Smart Security или ESET NOD32 Antivirus с использованием ESET Remote Administrator

«Код ошибки SC 6, код ошибки GLE 53. Не удалось установить подключение IPC к целевому компьютеру.»
Для установки подключения IPC должны выполняться следующие требования.
1. На компьютере с сервером ERAS и на целевом компьютере должен быть установлен стек TCP/IP.
2. Должна быть установлена служба «Общий доступ к файлам и принтерам Microsoft».
3. Должны быть открыты порты общего доступа к файлам (135–139, 445).
4. Целевой компьютер должен отвечать на PING-запросы.

«Код ошибки SC 6, код ошибки GLE 67. Не удается разместить установщик ESET на целевом компьютере.»
На системном диске клиента должен быть доступен административный общий ресурс *ADMIN$*.

«Код ошибки SC 6, код ошибки GLE 1326. Не удалось установить подключение IPC к целевому компьютеру, вероятно, из-за неправильного имени пользователя или пароля.»
Введено неправильное имя пользователя учетной записи администратора (либо оно не вводилось вообще).

«Код ошибки SC 6, код ошибки GLE 1327. Не удалось установить подключение IPC к целевому компьютеру.»
Поле пароля администратора не заполнено. Удаленная установка не запускается с пустым полем пароля.

«Код ошибки SC 11, код ошибки GLE 5. Не удается разместить установщик ESET на целевом компьютере.»
Установщику не удается получить доступ к клиентскому компьютеру из-за отсутствия достаточных прав (нет доступа).

«Код ошибки SC 11, код ошибки GLE 1726. Не удается разместить установщик NOD32 на целевом компьютере.»
Эта ошибка выводится после попытки повторной установки, если окно «Автоматическая установка» не было закрыто после первой попытки.

10.2.2 Часто встречающиеся коды ошибок в журнале era.log

0x1203 - UPD_RETVAL_BAD_URL
Ошибка модуля обновления — неправильно введенное имя сервера обновления.

0x1204 - UPD_RETVAL_CANT_DOWNLOAD
Эта ошибка может возникать в следующих случаях.

- При обновлении по протоколу HTTP:
  - сервер обновления выводит код ошибки HTTP в интервале 400— 500 кроме 401, 403, 404 и 407;
  - обновления загружаются с сервера CISCO, при этом изменился формат ответа аутентификации HTML.

- При обновлении из общей папки:
  выводимые ошибки не относятся к категориям «неправильная аутентификация» или «файл не найден» (например, *прерывание соединения*, *несуществующий сервер* и т. п.).

- При использовании обоих способов обновления:
  не удается найти ни один из серверов, указанных в файле *upd.ver* (файл находится в каталоге *%ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server\updfiles*)
  - не удалось подключиться к надежному серверу (вероятно, из-за удаления соответствующих записей ESET в реестре);

- неправильная настройка прокси-сервера на сервере ERAS
  - администратор должен указывать адрес прокси-сервера в формате.

0x2001 - UPD_RETVAL_AUTHORIZATION_FAILED
Не удалось пройти аутентификацию на сервере обновления, введены неправильное имя пользователя или пароль.

0x2102 - UPD_RETVAL_BAD_REPLY
Эта ошибка модуля обновления возникает при подключении к Интернету с использованием прокси-сервера Webwasher.

0x2104 - UPD_RETVAL_SERVER_ERROR
Ошибка модуля обновления, указывающая на то, что код ошибки HTTP превышает значение 500. При работе с HTTP-сервером ESET значение ошибки 500 означает проблему с распределением памяти.

0x2105 - UPD_RETVAL_INTERRUPTED
Эта ошибка модуля обновления возникает при подключении к Интернету с использованием прокси-сервера Webwasher.

10.3 Диагностика проблем на сервере ERAS

Если возникли подозрения, что на сервере ERAS есть проблемы или он работает неправильно, рекомендуется выполнить указанные ниже действия.

1) Проверьте журнал ERAS: в главном меню консоли ERAC выберите **«Служебные программы»** > **«Настройки сервера»**. В окне **«Настройки сервера»** щелкните вкладку **«Ведение журнала»** и нажмите кнопку **«Просмотр журнала»**.

2) Если сообщения об ошибках отсутствуют, увеличьте уровень **«Детализации журнала»** в окне **«Настройки сервера»** до уровня 5. После выявления проблемы рекомендуется вернуть значение по умолчанию.

3) Проблемы также можно обнаруживать посредством включения журнала отладки базы данных на той же самой вкладке (см. раздел **«Журнал отладки»**). **«Журнал отладки»** рекомендуется активировать только при попытке воспроизведения проблемы.

4) В случае появления кодов ошибок, не указанных в данном документе, обращайтесь в службу поддержки

клиентов ESET. Опишите работу программы, способ репликации или способ избежать возникновения проблемы. Очень важно указать версии всех используемых продуктов безопасности ESET (т. е. сервера ERAS, консоли ERAC, ESET Smart Security, ESET NOD32 Antivirus

11. Советы и подсказки

11.1 Планировщик

В ESET NOD32 Antivirus и ESET Smart Security встроен планировщик задач, который позволяет планировать регулярные проверки, обновления и т.п. В планировщике перечислены все возможные задачи.

С помощью ERA можно настроить следующие четыре типа задач:

- Запуск внешнего приложения
- Обслуживание журнала
- Сканирование компьютера
- Создать снимок состояния компьютера
- Обновление
- Автоматически проверять файлы при запуске системы

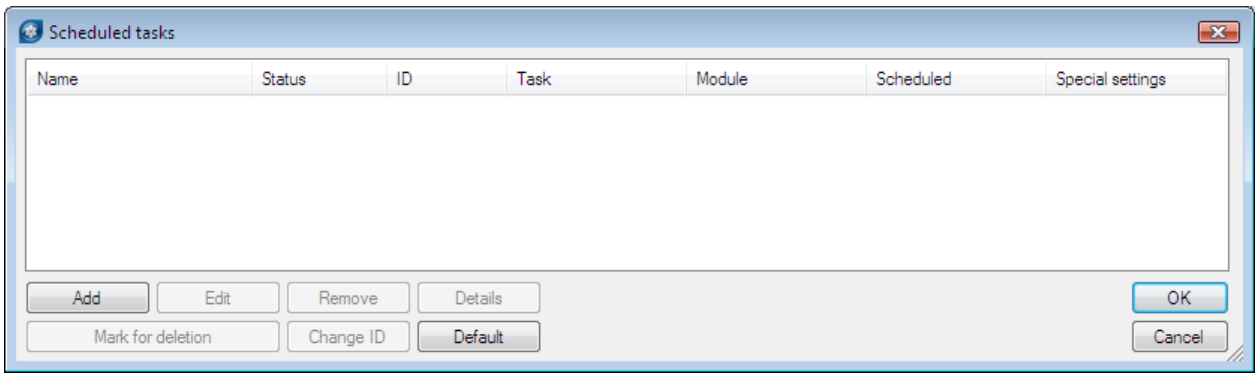
В большинстве случаев настраивать задачу **«Запуск внешнего приложения»** нет необходимости. Задача **«Автоматическая проверка файлов, исполняемых при запуске системы»** является задачей по умолчанию, поэтому не рекомендуется изменять ее параметры. Если после установки не делались никакие изменения, ESET NOD32 и ESET Smart Security содержат две предопределенные задачи этого вида. Первая задача выполняет проверку файловой системы при каждом входе в систему, а вторая задача выполняет ту же самую задачу после обновления БД сигнатур вирусов. С точки зрения администратора задачи **«Сканирование компьютера»** и **«Обновление»** возможно, представляются самыми необходимыми.

- **«Сканирование компьютера»**
  Обеспечивает регулярную проверку на наличие вирусов (обычно на локальных дисках) на клиентах.

- **«Обновление»**
  Эта задача отвечает за обновление клиентских решений ESET. Она является предопределенной и выполняется каждый час. Обычно изменять ее параметры не требуется. Единственным исключением являются ноутбуки, поскольку их владельцы часто подключаются к Интернету за пределами локальных сетей. В таком случае для этой задачи можно настроить использование двух профилей обновления. Это позволит ноутбукам обновляться с локального зеркала, а также с серверов обновления компании ESET.

Планировщик можно также настраивать в **ESET Configuration Editor** в меню ESET Smart Security / ESET NOD32 Antivirus **> «Ядро ESET»** > **«Настройка»** > **«Расписание»** > **«Расписание/Планировщик»** > **«Изменить»**.

Дополнительные сведения см. в разделе ESET Configuration Editor 34.



В диалоговом окне могут быть перечислены существующие задачи (нажмите кнопку **«Изменить»** чтобы изменить их параметры), или оно может быть пустым. Это зависит от того, открыта ли конфигурация на клиенте (например, на ранее настроенном и работающем компьютере) или новый файл с шаблоном по умолчанию, в котором отсутствуют задачи.

Каждой новой задаче присваивается идентификатор: задачам по умолчанию — десятичные (1, 2, 3...), а пользовательским — шестнадцатеричные (например, *4AE13D6C*), которые автоматически создаются для каждой новой задачи.

Если для задачи установлен флажок, это значит, что она активна и будет выполнена на указанном клиентском

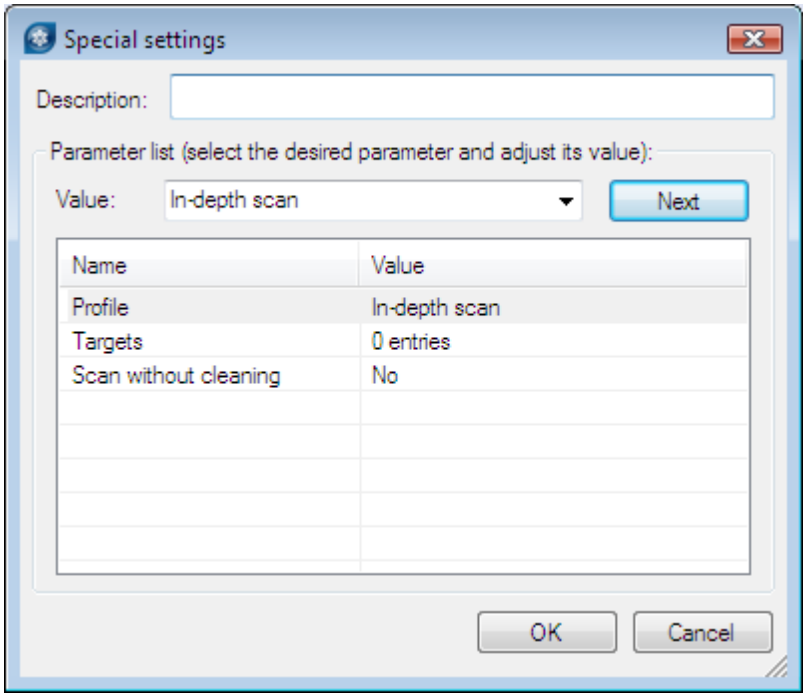
ПК.

Кнопки в окне запланированных задач выполняют следующие функции:

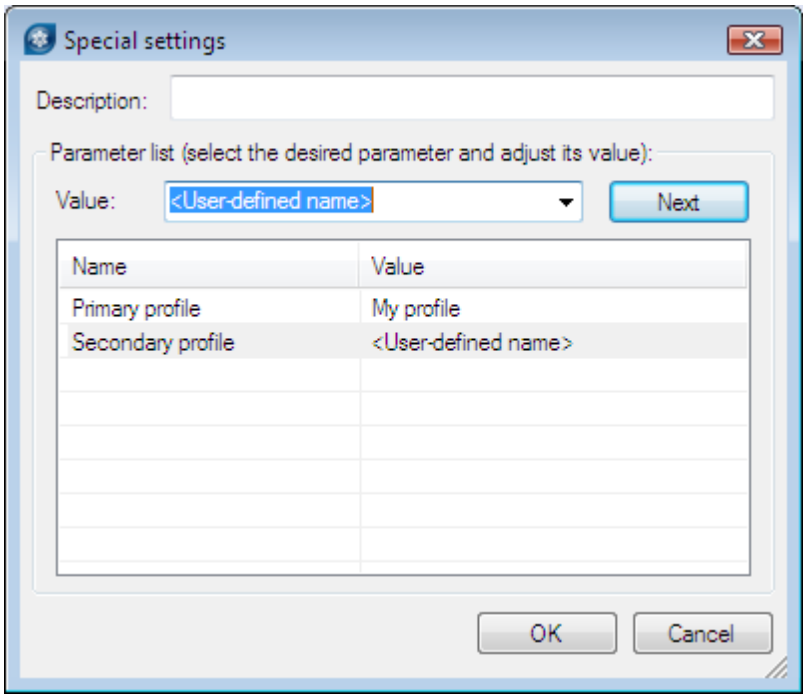
- **«Добавить»** — добавляет новую задачу;
- **«Изменить»** — изменяет выбранные задачи;
- **«Изменить идентификатор»** — изменяет идентификаторы выбранных задач;
- **Подробности** — выводит сводные данные о выбранной задаче;
- **«Выбрать для удаления»** — приложение для работы с *XML*-файлами удаляет выбранные задачи на целевых клиентах;
- **«Удалить из списка»** — удаляет выбранные задачи из списка. Обратите внимание, что задачи, удаленные из списка в XML-конфигурации, не удаляются на целевых рабочих станциях.

При создании новой задачи (кнопка **«Добавить»**) или изменении параметров существующей задачи (кнопка **«Изменить»**) необходимо указывать время ее запуска. Выполнение задачи может повторяться через определенные периоды времени (ежедневно в 12 часов, каждую пятницу и т. п.) или активироваться событием (после успешного обновления, ежедневно при первом запуске компьютера и т. п.).

На последнем этапе задачи **«Сканирование компьютера по требованию»** появляется окно специальных настроек, в котором можно задавать конфигурацию проверки,т. е. профиль и целевые объекты сканирования.



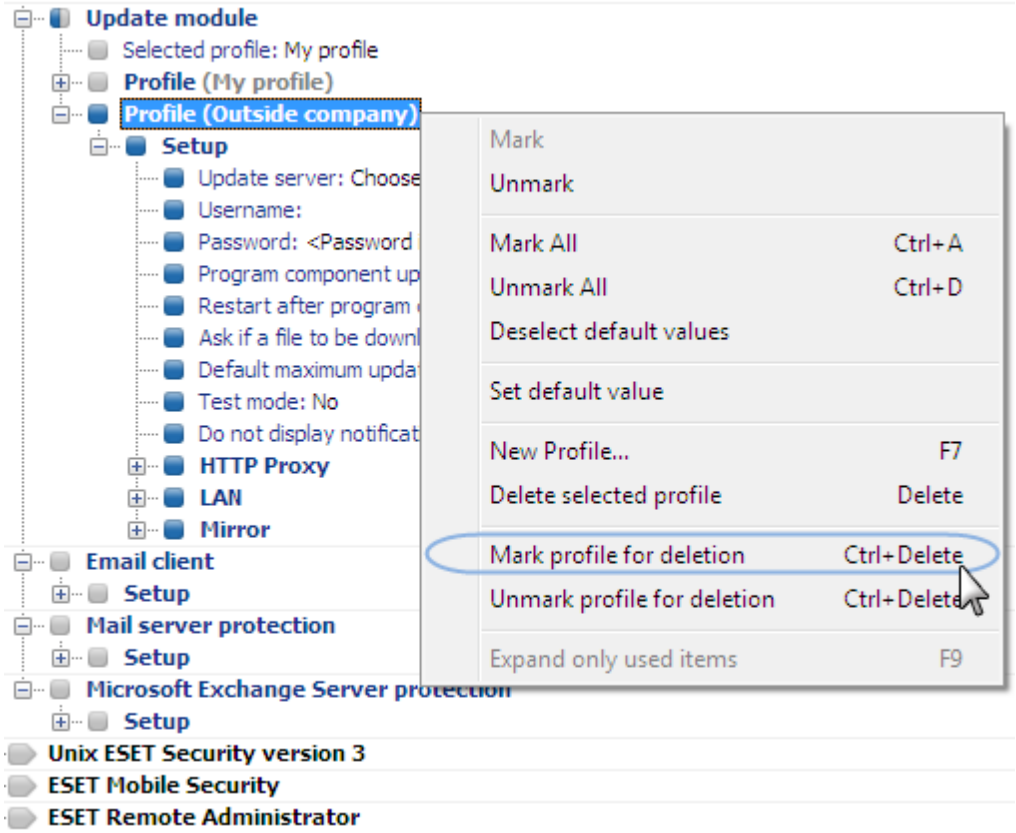
На последнем этапе задачи **«Обновление»** указываются профили обновления, которые будут запускаться в рамках данной задачи. Эта задача является предопределенной и по умолчанию выполняется каждый час. Обычно изменять ее параметры не требуется. Единственным исключением являются ноутбуки, поскольку их владельцы подключаются к Интернету и за пределами локальных сетей. В последнем диалоговом окне можно указать два разных профиля обновления для обновлений с локального сервера и с серверов обновления ESET.



11.2 Удаление существующих профилей

Иногда встречаются одинаковые профили обновления или проверки, которые были созданы по ошибке. Чтобы удаленно удалить эти профили, не затрагивая другие настройки «Планировщика», выполните указанные ниже действия.

- В консоли ERAC откройте вкладку **«Клиенты»** и щелкните дважды клиента с проблемой.
- В окне **«Свойства клиента»** откройте вкладку **«Конфигурация»**. Выберите параметры **«С последующим запуском ESET Configuration Editor для редактирования файла»** и **«Использовать загруженную конфигурацию в новой задаче»** и нажмите кнопку **«Новая задача»**.
- В мастере создания новой задачи нажмите кнопку **«Изменить»**.
- В Configuration Editor нажмите сочетание клавиш **CTRL + D** для отмены выбора (затенения) всех параметров. Это позволяет предотвратить внесение случайных изменений, поскольку новые изменения выделяются синим цветом.
- Щелкните правой кнопкой мыши профиль, который нужно удалить, и выберите в контекстном меню команду **«Отметить профиль для удаления»**. Профиль будет удален после доставки задачи на клиенты.



- Нажмите кнопку **«Консоль»** в ESET Configuration Editor и сохраните параметры.
- Убедитесь в том, что выбранный клиент находится в столбце **выбранных** справа. Нажмите кнопку **«Далее»**, а затем — **«Готово»**.

11.3 Экспорт и прочие функции XML-конфигурации клиента

В консоли ERAC выберите любой клиент на вкладке **«Клиенты»**. Щелкните по клиенту правой кнопкой мыши и выберите в контекстном меню команду **«Конфигурация...»**. Выберите команду **«Сохранить как...»**, чтобы экспортировать конфигурацию указанного клиента в *XML*-файл (*XML*-файлы конфигурации можно также извлечь непосредственно в программе ESET Smart Security). Этот *XML*-файл затем можно будет использовать в следующих операциях.

- При удаленной установке *XML*-файл можно использовать как шаблон предопределенной конфигурации. Это означает, что новый *XML*-файл не создается, а новому пакету установки назначается существующий *XML*-файл (кнопка **«Выбрать...»**). *XML*-файл конфигурации также можно получить непосредственно из интерфейса программы ESET Smart Security.

- При настройке нескольких клиентов они получают ранее загруженный *XML*-файл и используют определенные в нем настройки (новая конфигурация не создается, а просто назначается с помощью кнопки **«Выбрать...»**).

Пример
Продукт безопасности ESET устанавливается только на одной рабочей станции. Настройте параметры программы непосредственно в интерфейсе пользователя программы. Сделав это, экспортируйте настройки в *XML*-файл. *XML*-файл также впоследствии можно использовать для удаленной установки на других рабочих станциях. Данный метод очень удобен для решения таких задач как точная настройка правил файервола, если используется режим *«На основе политики»*.

11.4 Комбинированное обновление для ноутбуков

Если в локальной сети есть мобильные устройства (например, ноутбуки), рекомендуется настроить комбинированное обновление из двух источников: с серверов обновления ESET и с локального сервера обновления (зеркала). Сначала ноутбуки обращаются к зеркальному серверу, и если не удается установить соединение (они находятся вне офиса), обновления загружаются непосредственно с серверов ESET. Чтобы этот метод работал, необходимо выполнить такие действия.

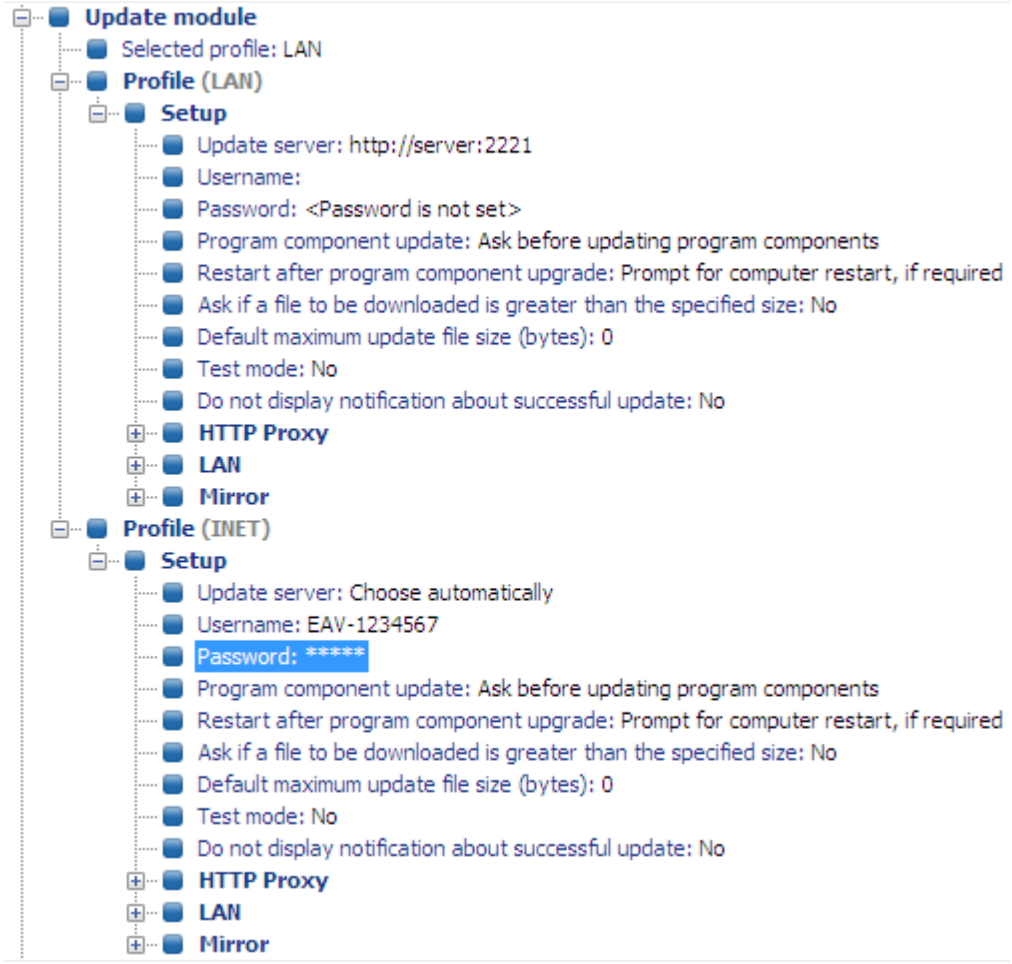
- Создайте два профиля обновления: один (Экспорт и прочие функции XML-конфигурации клиента 101) с подключением к серверу зеркала (с названием LAN в примере ниже), а второй — к серверам обновления ESET (INET)

- Создать задачу обновления или изменить существующую с помощью планировщика (меню **«Служебные программы»** > **«Расписание»** в главном окне программы ESET Smart Security или ESET NOD32 Antivirus).

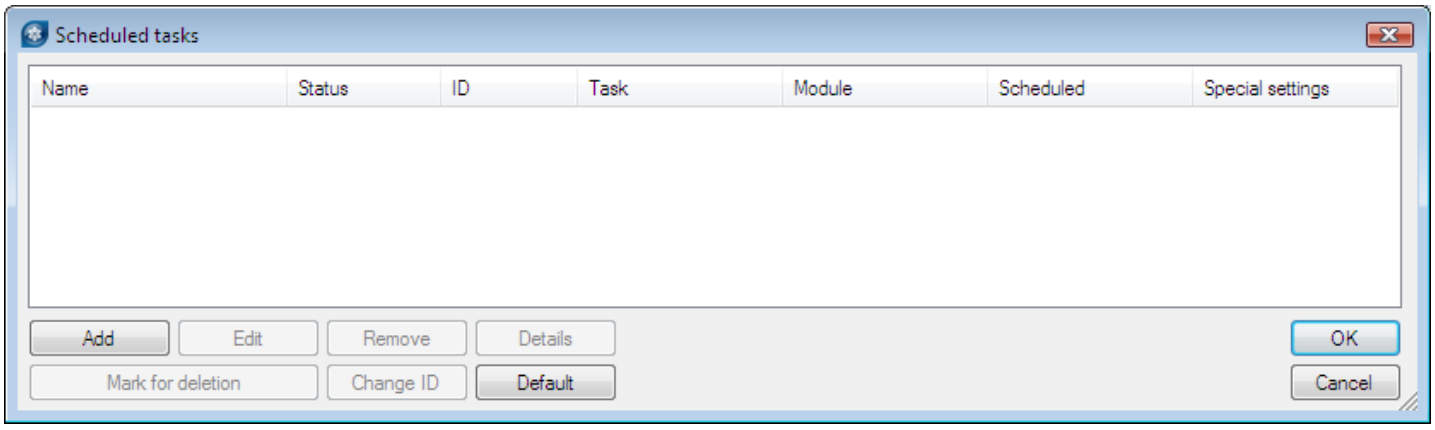
Настройку можно выполнять непосредственно на ноутбуках или удаленно с помощью ESET Configuration Editor. Созданную конфигурацию можно применять во время установки или позже в виде задачи конфигурации.

Чтобы создать новый профиль в ESET Configuration Editor, щелкните правой кнопкой мыши по ветке **«Обновление»** и выберите в контекстном меню пункт **«Новый профиль»**.

Результат изменений будет примерно соответствовать приведенному ниже примеру.



Профиль LAN загружает обновления с локального зеркала компании (*http://server:2221*), а профиль INET подключается к серверам ESET (**«Выбирать автоматически»**). Затем нужно указать задачу обновления, которая последовательно запускает каждый из профилей обновления. Для этого в выберите пункт **ESET Smart Security**, **ESET NOD32 Antivirus** > **«Ядро»** > **«Настройка»** > **«Расписание/Планировщик»** в ESET Configuration Editor. Нажмите кнопку **«Изменить»**, чтобы открыть окно **«Запланированные задачи»**.



Для создания новой задачи нажмите кнопку **«Добавить»**. В раскрывающемся меню **«Запланированная задача»** выберите пункт **«Обновить»** и нажмите кнопку **«Далее»**. Введите **название задачи** (например, *«Комбинированное обновление»*), установите флажок **«Многократно каждые 60 минут»** и перейдите к выбору основного и дополнительного профилей.

Если рабочие станции на ноутбуках должны сначала обращаться к серверу зеркала, главным должен быть профиль LAN, а дополнительным — профиль INET. Профиль INET должен использоваться только при сбое обновления по профилю LAN.

Рекомендация. Экспортируйте текущую *XML*-конфигурацию с клиента (дополнительные сведения см. в разделе Диагностика проблем на сервере ERAS? 96) и внесите указанные изменения в экспортированный *XML*-файл. Это позволит избежать дублирования в расписании и неиспользуемых профилях.

11.5 Установка продуктов сторонних производителей с помощью программы ERA

Помимо удаленной установки продуктов ESET, программа ESET Remote Administrator может устанавливать и другие программы. Единственным требованием является то, чтобы пользовательский пакет был в формате *MSI*. Удаленную установку пользовательских пакетов можно выполнить с использованием процесса, аналогичного тому, что описан в разделе Удаленная установка 38.

Основное отличие заключается в процессе создания пакета, который описан ниже.

1) В консоли ERA откройте вкладку ERAC **«Удаленная установка»**.
2) Нажмите кнопку **«Пакеты...»**.
3) В раскрывающемся меню «Тип пакета» выберите пункт **«Пользовательский пакет»**.
4) Нажмите кнопку **«Добавить**, выберите команду **«Добавить файл»** и выберите нужный *MSI*-пакет.
5) Выберите файл в раскрывающемся меню **«Входной файл пакета»** и нажмите кнопку **«Создать»**.
6) Вернувшись в исходное окно, задайте для *MSI*-файла параметры командной строки, если это необходимо. Эти параметры будут такими же, как и при локальной установке этого пакета.
7) Нажмите кнопку **«Сохранить как...»**, чтобы сохранить пакет.
8) Нажмите кнопку **«Закрыть»**, чтобы закрыть редактор пакета установки.

Созданный пользовательский пакет можно разослать по клиентским рабочим станциям так же, как и при удаленной установке, описанной в предыдущих главах. При удаленной автоматической установке, установке через сценарий входа или отправке по электронной почте пакет отправляется на целевые рабочие станции. После запуска пакета управление установкой переходит к службе установки Microsoft Windows.

12. ESET SysInspector

12.1 Введение в ESET SysInspector

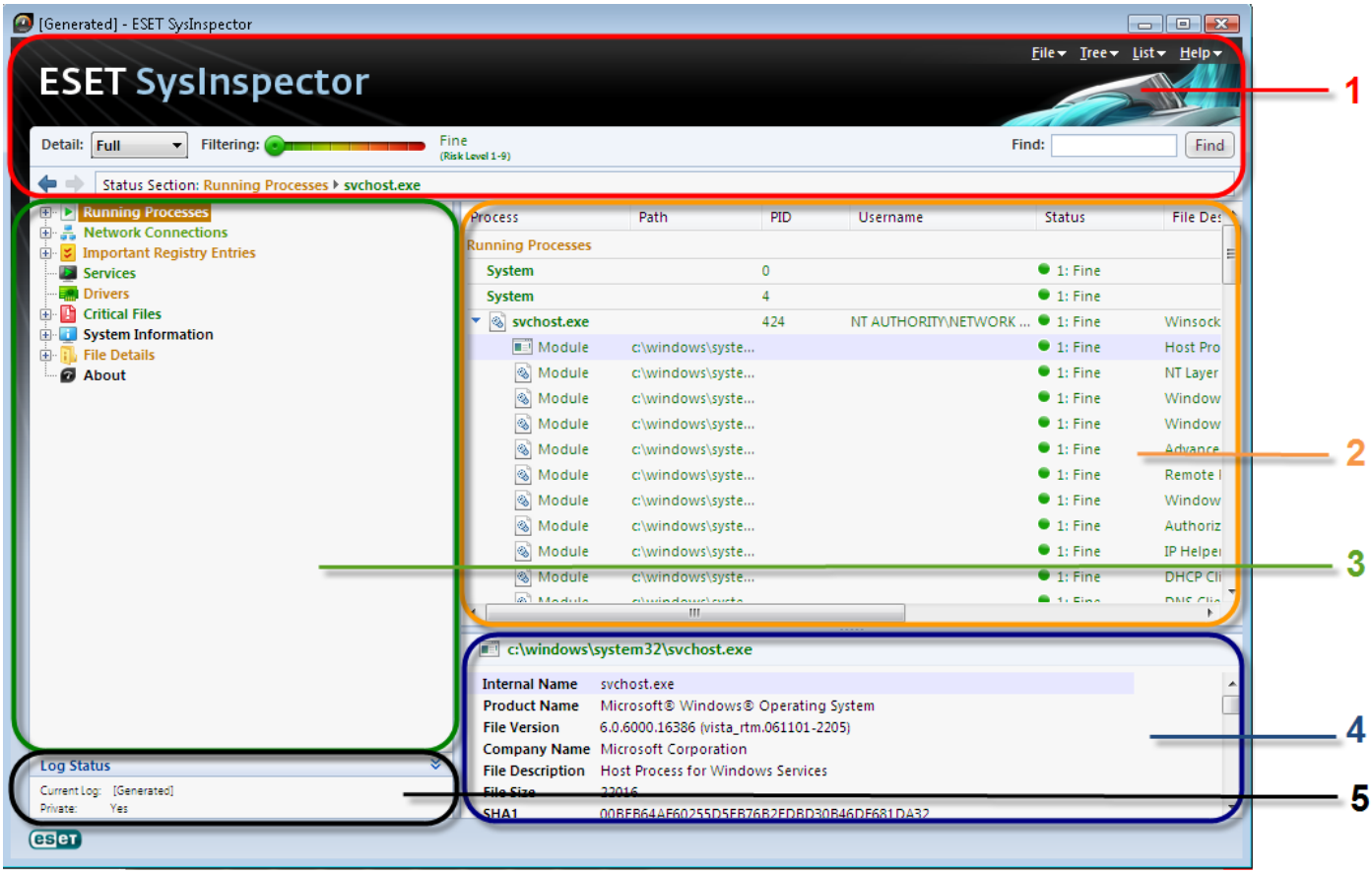
ESET SysInspector — это приложение, которое тщательно проверяет компьютер и отображает собранные данные в обобщенном виде. Такая информация, как данные об установленных драйверах и приложениях, сетевых соединениях и важных записях в реестре, позволяет определить причину подозрительного поведения системы, которое могло иметь место, например, вследствие несовместимости программного или аппаратного обеспечения или заражения вредоносными программами.

12.1.1 Запуск ESET SysInspector

Чтобы запустить ESET SysInspector, достаточно выполнить файл *SysInspector.exe*, загруженный с веб-сайта ESET. Если у вас уже установлен один из продуктов ESET для обеспечения безопасности, ESET SysInspector можно запустить непосредственно из меню «Пуск» («Программы» > ESET > …). Подождите, пока программа проверяет систему: это может занять несколько минут в зависимости от оборудования и собираемых данных.

12.2 Интерфейс пользователя и работа в приложении

Для удобства главное окно разделено на четыре раздела: вверху находятся элементы управления программой (1), слева — окно навигации (3), справа по центру — окно описания (2), а справа внизу — окно подробных сведений (4). В разделе «Состояние журнала» (5) перечислены основные параметры журнала (используемый фильтр, тип фильтра, является ли журнал результатом сравнения и т. д.).



12.2.1 Элементы управления программой

В этом разделе описаны все элементы управления приложением ESET SysInspector.

Файл
Позволяет сохранить данные о текущем состоянии системы для их последующего изучения или открыть ранее сохраненный журнал. Если планируется опубликовать журнал, при его создании рекомендуется использовать параметр **«Подходит для отправки»**. В этом случае из него исключается конфиденциальная информация (например, имя текущего пользователя, имена компьютера и домена, права текущего пользователя, переменные окружения и т. п.).

Примечание. Чтобы просмотреть сохраненные ранее отчеты ESET SysInspector, достаточно просто перетащить их в главное окно программы.

Дерево
Позволяет развернуть или свернуть все узлы, а также экспортировать выбранные разделы в сценарий обслуживания.

Список
Содержит функции, облегчающие навигацию в пределах программы, а также прочие функции (например, средства поиска информации в Интернете).

Справка
Содержит сведения о приложении и его функциях.

Подробнее
Дополняет сведения, отображаемые в других разделах главного окна, упрощая тем самым работу с программой. В основном режиме пользователю доступна информация, необходимая для поиска решений стандартных проблем, возникающих в системе. В среднем режиме программа ESET SysInspector отображает расширенные данные, а в полном — всю информацию, необходимую для решения самых нестандартных проблем.

Фильтрация элементов
Используется для поиска подозрительных файлов или записей в реестре системы. С помощью ползунка можно фильтровать элементы по их уровню риска. Если ползунок установлен в крайнее левое положение (уровень риска 1), отображаются все элементы. При перемещении ползунка вправо программа отфильтровывает все элементы с уровнем риска, меньшим текущего уровня, и выводит только те элементы, уровень подозрительности которых выше выбранного уровня. Если ползунок находится в крайнем правом положении, программа отображает только явно вредоносные элементы.

Все элементы с уровнем риска от 6 до 9 могут быть опасными для системы. Если вы не используете решения компании ESET для обеспечения безопасности, после нахождения программой такого элемента рекомендуется проверить систему с помощью ESET Online Scanner. Пользование продуктом ESET Online Scanner предоставляется бесплатно.

Примечание. Уровень риска элемента легко определяется путем сравнения цвета элемента с цветом на ползунке уровней рисков.

Поиск
Служит для быстрого нахождения определенного элемента по его названию или части названия. Результаты поиска отображаются в окне описания.

Возврат
С помощью стрелок назад и вперед можно переходить в окне описания к ранее отображенной информации. Вместо кнопок перехода назад и вперед можно использовать соответственно клавишу Backspace и пробел.

Раздел состояния
Отображает текущий узел в окне навигации.

Внимание! Элементы, выделенные красным цветом, являются неизвестными, поэтому программа помечает их как потенциально опасные. Если элемент выделен красным, это не означает, что его можно удалить. Перед удалением убедитесь в том, что эти файлы действительно опасны и не являются необходимыми.

12.2.2 Навигация в ESET SysInspector

ESET SysInspector распределяет информацию разного типа по нескольким базовым разделам, называемым узлами. Для того чтобы получить дополнительные сведения о каком-либо из разделов, разверните вложенные узлы соответствующего узла. Для того чтобы открыть (развернуть) узел, дважды щелкните по названию узла или по значку ⊞ либо ⊟ справа от названия узла. При перемещении по древовидной структуре узлов в окне навигации о каждом из них доступны различные сведения, отображаемые в окне описания. При переходе к конкретному элементу в окне подробной информации появляются дополнительные сведения о нем.

Ниже описаны главные узлы в окне навигации и относящиеся к ним сведения в окнах описания и подробной информации.

Запущенные процессы
Этот узел содержит сведения о приложениях и процессах, выполняемых в момент создания журнала. В окне описания могут находиться дополнительные сведения о каждом из процессов, например названия динамических библиотек, используемых процессом, и их местонахождение в системе, название поставщика приложения, уровень риска файла и т. п.

Окно подробной информации содержит дополнительные сведения об элементах, выбранных в окне описания, например размер файла или его хэш.

Примечание. Любая операционная система состоит из нескольких важных компонентов, которые постоянно запущены и обеспечивают работу базовых и жизненно важных функций для других пользовательских приложений. В определенных случаях путь к файлам таких процессов начинается в программе ESET SysInspector с символов «\??\». Эти символы обеспечивают таким процессам оптимизацию до запуска и с точки зрения системы являются безопасными и правильными.

Сетевые подключения
В окне описания перечислены процессы и приложения, которые обмениваются данными через сеть по протоколу, выбранному в окне навигации (TCP или UDP), а также удаленные адреса, с которыми эти приложения устанавливают соединения. Также в нем можно найти IP-адреса DNS-серверов.

Окно подробной информации содержит дополнительные сведения об элементах, выбранных в окне описания, например размер файла или его хэш.

Важные записи реестра
Содержит список определенных записей реестра, которые часто бывают связаны с различными проблемами в системе: например, автоматически загружаемые программы, объекты модуля поддержки обозревателя и т. п.

В окне описания также могут быть перечислены файлы, связанные с некоторыми из этих записей. Окно подробных сведений может содержать дополнительную информацию.

Службы
В окне описания перечислены файлы, зарегистрированные в качестве служб Windows. В окне подробных сведений можно увидеть способ запуска службы, а также просмотреть некоторую дополнительную информацию.

Драйверы
Список драйверов, установленных в системе.

Критические файлы
В окне описания отображается содержимое критически важных файлов операционной системы Microsoft Windows.

Информация о системе
Содержит подробные сведения об оборудовании и программном обеспечении, а также сведения о переменных окружения и правах пользователя.

Сведения о файле
Список важных системных файлов и файлов из папки Program Files. В окнах описания и подробных сведений может отображаться дополнительная информация о них.

О программе
Информация о программе ESET SysInspector.

12.2.3 Сравнение

С помощью функции сравнения пользователь может сравнить два существующих журнала. Результатом работы этой команды является набор элементов, не совпадающих в этих журналах. Это позволяет отслеживать изменения в системе — таким образом можно, например, обнаружить деятельность вредоносных программ.

После запуска приложение создает новый журнал, который открывается в новом окне. Чтобы сохранить журнал в файл, в меню **«Файл»** выберите пункт **«Сохранить журнал»**. Сохраненные файлы журналов можно впоследствии открывать и просматривать. Чтобы открыть существующий журнал, в меню **«Файл»** выберите пункт **«Открыть журнал»**. В главном окне программы ESET SysInspector всегда отображается только один журнал.

Принцип сравнения двух журналов заключается в сравнении активного журнала с журналом из файла. Чтобы сравнить журналы, в меню **«Файл»** выберите пункт **«Сравнить журналы»** и выполните команду **«Выбрать файл»**. Выбранный журнал сравнивается с активным журналом в главном окне программы. В результате создается так называемый сравнительный журнал, содержащий различия между двумя сравниваемыми журналами.

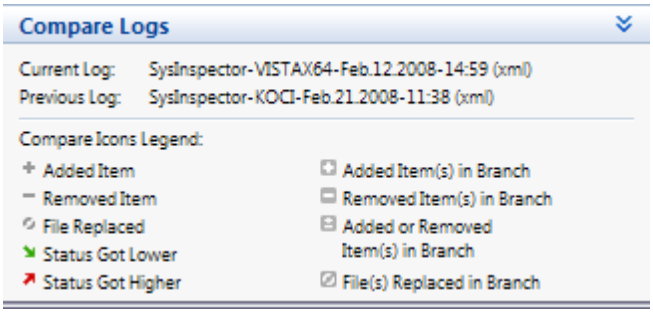
Примечание. При сравнении двух файлов журналов в меню **«Файл»** выберите пункт **«Сохранить журнал»** и сохраните журнал как ZIP-файл. В результате будут сохранены оба файла. Если такой файл впоследствии открыть, содержащиеся в нем журналы сравниваются автоматически.

Напротив отображенных элементов SysInspector выводит символы, обозначающие различия между журналами.
Элементы, отмеченные знаком –, есть только в активном журнале и отсутствуют в открытом сравниваемом журнале. Элементы, отмеченные знаком +, есть только в открытом журнале и отсутствуют в активном.

Ниже описаны все символы, которые могут отображаться напротив элементов.

+ новое значение, отсутствует в предыдущем журнале
раздел древовидной структуры содержит новые значения
– удаленное значение, присутствует только в предыдущей версии журнала
раздел древовидной структуры содержит удаленные значения
значение или файл были изменены
раздел древовидной структуры содержит измененные значения или файлы
уровень риска снизился или был выше в предыдущей версии журнала
уровень риска повысился или был ниже в предыдущей версии журнала

В разделе пояснений в левом нижнем углу отображается описание всех символов, а также названия сравниваемых журналов.



Любой сравниваемый журнал можно сохранить в файл и открыть его позже.

Пример

Создайте и сохраните журнал, содержащий исходную информацию о системе, в файл с названием «предыдущий.xml». Внеся в систему изменения, откройте SysInspector и создайте новый журнал. Сохраните его в файл с названием *«текущий.xml»*.
Чтобы отследить различия между этими двумя журналами, в меню **«Файл»** выберите пункт **«Сравнить журналы»**. Программа создаст сравнительный журнал с перечнем различий между исходными журналами.

Тот же результат можно получить с помощью следующей команды, вызываемой из командной строки:

SysIsnpector.exe текущий.xml предыдущий.xml

12.3 Параметры командной строки

В ESET SysInspector можно формировать отчеты из командной строки. Для этого используются перечисленные ниже параметры.

/gen	создание журнала непосредственно из командной строки без запуска графического интерфейса пользователя
/privacy	создание журнала без включения в него конфиденциальной информации
/zip	сохранение журнала непосредственно на диск в сжатом файле
/silent	скрытие индикатора выполнения при создании журнала
/help, **/?**	отображение сведений о параметрах командной строки

Примеры

Чтобы открыть определенный журнал непосредственно в браузере, воспользуйтесь следующей командой: *SysInspector.exe "c:\клиентский_журнал.xml"*
Чтобы создать журнал в текущей папке, воспользуйтесь следующей командой: *SysInspector.exe /gen*
Чтобы создать журнал в определенной папке, воспользуйтесь следующей командой: *SysInspector.exe /gen="c:\папка\"*
Чтобы создать журнал в определенной папке и в определенном файле, воспользуйтесь следующей командой: *SysInspector.exe /gen="c:\папка\новый_журнал.xml"*
Чтобы создать журнал, из которого исключена конфиденциальная информация, в сжатом файле, воспользуйтесь следующей командой: *SysInspector.exe /gen="c:\новый_журнал.zip" /privacy /zip*
Чтобы сравнить два журнала, воспользуйтесь следующей командой: *SysInspector.exe "текущий.xml" "исходный.xml"*

Примечание. Если название файла или папки содержит пробел, это название необходимо заключить в кавычки.

12.4 Сценарий обслуживания

Сценарий обслуживания является вспомогательным средством для пользователей программы ESET SysInspector. Он предназначен для удаления из системы нежелательных объектов.

Сценарий обслуживания позволяет целиком или частично экспортировать журнал SysInspector. После экспорта можно выбрать и отметить объекты для удаления. Затем сценарий запускается с отредактированным журналом для удаления отмеченных объектов.

Сценарий обслуживания предназначен для пользователей, имеющих определенный опыт в диагностике компьютерных систем. Неквалифицированное использование данного средства может привести к тому, что операционная система окажется неработоспособна.

Пример

При наличии подозрений на заражение компьютера вирусом, который не определяется антивирусной программой, можно воспользоваться описанной ниже пошаговой процедурой.

- Запустите ESET SysInspector и создайте новый снимок состояния компьютера.
- Щелкните первый элемент в разделе слева (в древовидной структуре), нажмите клавишу CTRL, а затем выберите последний объект, чтобы отметить все элементы в списке. Отпустите клавишу CTRL.
- Щелкните выделенные объекты правой кнопкой и выберите в контекстном меню команду **«Экспортировать выбранные разделы в сценарий обслуживания»**.
- Выбранные объекты будут экспортированы в новый журнал.
- Далее следует наиболее важный шаг всей процедуры: откройте созданный журнал и измените атрибут «–» на «+» для всех объектов, подлежащих удалению. Ни в коем случае не отмечайте объекты, жизненно важные для работы операционной системы.

- Запустите решение ESET SysInspector, в меню **«Файл»** выберите пункт **«Загрузить сценарий обслуживания»** и укажите путь к своему сценарию.
- Нажмите кнопку **«OK»**, чтобы запустить сценарий.

12.4.1 Создание сценариев обслуживания

Для того чтобы создать сценарий, щелкните правой кнопкой любой объект в древовидном меню в левой панели основного окна SysInspector. В контекстном меню выберите команду **«Экспортировать все разделы в сценарий обслуживания»** или **«Экспортировать выбранные разделы в сценарий обслуживания»**.

Примечание. Сценарий обслуживания нельзя экспортировать в ходе сравнения двух журналов.

12.4.2 Структура сценария обслуживания

Первая строка заголовка сценария содержит данные о версии ядра (ev), версии интерфейса (gv) и версии журнала (lv). Эти данные позволяют отслеживать изменения в XML-файле, используемом для создания сценария. Они гарантируют согласованность версий на этапе выполнения. Эту часть сценария изменять не следует.

Остальное содержимое файла разбито на разделы, объекты в которых можно редактировать. Те из них, которые должны быть обработаны сценарием, следует пометить. Для этого символ «-» перед объектом надо заменить символом «+». Разделы отделены один от другого пустой строкой. Каждый раздел имеет собственный номер и название.

01) Running processes (Выполняемые процессы)

Этот раздел содержит список процессов, запущенных в системе. Каждый процесс идентифицируется по UNC-пути, а также по коду CRC16, заключенному в символы звездочки (*).

Пример

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

В данном примере выбран (помечен символом «+») процесс module32.exe. При выполнении сценария этот процесс будет завершен.

02) Loaded modules (Загруженные модули)

В этом разделе перечислены используемые в данный момент системные модули.

Пример

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

В данном примере модуль khbekhb.dll помечен символом «+». При выполнении сценария процессы, использующие данный модуль, распознаются и прерываются.

03) TCP connections (TCP-соединения)

Этот раздел содержит данные о существующих TCP-соединениях.

Пример

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

При запуске этого сценария обнаруживается владелец сокета помеченного TCP-соединения, после чего сокет останавливается, высвобождая системные ресурсы.

04) UDP endpoints (Конечные точки UDP)

Этот раздел содержит информацию о существующих конечных точках UDP.

Пример

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

При выполнении сценария определяется владелец сокета помеченных конечных точек UDP, после чего сокет останавливается.

05) DNS server entries (Записи DNS-сервера)

Этот раздел содержит информацию о текущей конфигурации DNS-сервера.

Пример

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

При выполнении сценария помеченные записи DNS-сервера удаляются.

06) Important registry entries (Важные записи в реестре)

Этот раздел содержит информацию о важных записях в реестре.

Пример

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

При выполнении сценария помеченные записи будут удалены, сведены к 0-разрядным значениям или сброшены к значениям по умолчанию. Действия, применяемые к конкретным записям, зависят от категории и значения раздела в определенной записи реестра.

07) Services (Службы)

Этот раздел содержит список служб, зарегистрированных в системе.

Пример

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

При выполнении сценария помеченные службы, а также все зависящие от них службы будут остановлены и удалены.

08) Drivers (Драйверы)

В этом разделе перечислены установленные драйверы.

Пример

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

При выполнении сценария регистрация указанных драйверов отменяется, а драйверы удаляются.

09) Critical files (Важные файлы)

Этот раздел содержит информацию о файлах, играющих важную роль с точки зрения правильной работы операционной системы.

Пример

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[…]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[…]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[…]
```

Выбранные объекты будут удалены или возвращены к исходным значениям.

12.4.3 Выполнение сценариев обслуживания

Пометьте нужные объекты, сохраните и закройте сценарий. Запустите измененный сценарий непосредственно из основного окна SysInspector с помощью команды «Запуск сценария обслуживания» в меню «Файл». При открытии сценария появится следующее сообщение: **«Выполнить сценарий обслуживания "%Scriptname%"?»** После подтверждения может появиться еще одно предупреждение, сообщающее о попытке запуска неподписанного сценария. Для того чтобы запустить сценарий, нажмите кнопку **«Запуск»**.

В диалоговом окне появится подтверждение о выполнение сценария.

Если сценарий может быть обработан только частично, отобразится следующее сообщение: **«Сценарий обслуживания выполнен частично. Показать отчет об ошибке?»** Для того чтобы просмотреть полный отчет об ошибках, в котором перечислены невыполненные действия, нажмите кнопку **«Да»**.

Если сценарий не был признан действительным, отобразится следующее сообщение: **«Выбранный сценарий обслуживания не подписан. Выполнение неподписанных и неизвестных сценариев может привести к повреждению данных на компьютере. Выполнить сценарий и все действия?»** Этот эффект может быть вызван несоответствиями в сценарии (поврежден заголовок, изменено название раздела, пропущена пустая разделительная строка и т. д.). В этом случае откройте файл сценария и исправьте ошибки либо создайте новый сценарий обслуживания.

12.5 Сочетания клавиш

Ниже представлен список клавиш быстрого доступа, которые можно использовать при работе с программой ESET SysInspector.

Файл

Ctrl+O	открывает существующий журнал
Ctrl+S	сохраняет созданные журналы

Создание

Ctrl+G	стандартная проверка состояния системы
Ctrl+H	проверка состояния системы, при которой регистрируется конфиденциальная информация

Фильтрация элементов

1, O	подробные сведения, отображаются элементы с уровнем риска 1—9
2	подробные сведения, отображаются элементы с уровнем риска 2—9
3	подробные сведения, отображаются элементы с уровнем риска 3—9
4, U	неизвестные элементы, отображаются элементы с уровнем риска 4—9
5	неизвестные элементы, отображаются элементы с уровнем риска 5—9
6	неизвестные элементы, отображаются элементы с уровнем риска 6—9
7, B	опасные элементы, отображаются элементы с уровнем риска 7—9
8	опасные элементы, отображаются элементы с уровнем риска 8—9
9	опасные элементы, отображаются элементы с уровнем риска 9
-	понижает уровень риска
+	повышает уровень риска
Ctrl+9	выбор режима фильтрации, равный или более высокий уровень
Ctrl+0	выбор режима фильтрации, только равный уровень

Просмотр

Ctrl+5	просмотр по производителям, все производители
Ctrl+6	просмотр по производителям, только Майкрософт
Ctrl+7	просмотр по производителям, все другие производители
Ctrl+3	отображает полные сведения
Ctrl+2	отображает сведения средней степени подробности
Ctrl+1	основной вид
BackSpace	переход на один шаг назад
Пробел	переход на один шаг вперед
Ctrl+W	разворачивает дерево
Ctrl+Q	сворачивает дерево

Прочие элементы управления

Ctrl+T	переход к исходному местоположению элемента после его выделения в результатах поиска
Ctrl+P	отображает базовые сведения об объекте
Ctrl+A	отображает полные сведения об объекте
Ctrl+C	копирует дерево текущего элемента
Ctrl+X	копирует элементы
Ctrl+B	ищет сведения о выбранных файлах в Интернете
Ctrl+L	открывает папку, в которой находится выбранный файл
Ctrl+R	открывает соответствующую запись в редакторе реестра
Ctrl+Z	копирует путь к файлу (если элемент связан с файлом)
Ctrl+F	переход в поле поиска
Ctrl+D	закрывает результаты поиска
Ctrl+E	запускает сценарий обслуживания

Сравнение

Ctrl+Alt+O	открывает исходный или сравнительный журнал
Ctrl+Alt+R	отменяет сравнение
Ctrl+Alt+1	отображает все элементы
Ctrl+Alt+2	отображает только добавленные элементы (отображаются только элементы из текущего журнала)
Ctrl+Alt+3	отображает только удаленные элементы (отображаются только элементы из предыдущей версии журнала)
Ctrl+Alt+4	отображает только замененные элементы (включая файлы)
Ctrl+Alt+5	отображает только различия между журналами
Ctrl+Alt+C	отображает результаты сравнения
Ctrl+Alt+N	отображает текущий журнал
Ctrl+Alt+P	отображает предыдущую версию журнала

Разное

F1	вызывает справку
Alt+F4	закрывает программу
Alt+Shift+F4	закрывает программу без вывода запроса
Ctrl+I	статистика журнала

12.6 Требования к системе

Для правильной работы ESET SysInspector система должна отвечать перечисленным ниже аппаратным и программным требованиям:

Операционная система Windows 2000, XP, 2003
Процессор 400 МГц, 32-разрядный (x86) или 64-разрядный (x64)
128 МБ оперативной памяти
10 МБ свободного места на диске
Монитор Super VGA (800 × 600)

Операционная система Windows 7, Vista, 2008
Процессор 1 ГГц, 32-разрядный (x86) или 64-разрядный (x64)
512 МБ оперативной памяти
10 МБ свободного места на диске
Монитор Super VGA (800 × 600)

12.7 Часто задаваемые вопросы

Требуются ли для запуска ESET SysInspector права администратора?

Хотя для запуска ESET SysInspector права администратора не требуются, некоторые из собираемых этим приложением данных доступны только для учетной записи администратора. Запуск с правами обычного пользователя или с ограниченными правами приведет к сбору меньшего объема данных о системе.

Создает ли ESET SysInspector файлы журнала?

ESET SysInspector может создать файл журнала с конфигурацией системы. Чтобы сохранить такой журнал, выберите в главном меню команду «Файл» > «Сохранить журнал». Журналы сохраняются в формате XML. По умолчанию файл журнала сохраняется в папке «%USERPROFILE%\Мои документы\» и получает название «SysInpsector-%COMPUTERNAME%-ГГММДД-ЧЧмм.XML». Перед сохранением файла журнала можно изменить его местоположение и название.

Как просмотреть файл журнала ESET SysInspector?

Чтобы просмотреть журнал, созданный в ESET SysInspector, запустите программу и выберите в главном меню команду «Файл» > «Открыть журнал». Кроме того, файлы журнала можно перетаскивать в окно приложения ESET SysInspector. Если вы часто просматриваете файлы журнала ESET SysInspector, создайте на рабочем столе ярлык для файла SYSINSPECTOR.EXE. После этого просматриваемые файлы можно просто перетаскивать на этот ярлык. По соображениям безопасности в ОС Windows Vista может быть запрещено перетаскивать элементы между окнами с разными настройками безопасности.

Доступна ли спецификация для формата файлов журнала? Существует ли пакет SDK?

В настоящее время ни спецификация файла журнала, ни пакет SDK недоступны, поскольку программа все еще находится на стадии разработки. После выхода окончательной версии программы мы можем предоставить эти данные по просьбам клиентов.

Как ESET SysInspector оценивает риск определенного объекта?

В большинстве случаев ESET SysInspector присваивает объектам (файлам, процессам, разделам в реестре и т. п.) уровни риска, используя наборы эвристических правил, которые изучают характеристики каждого объекта и затем оценивают угрозу их вредоносного действия. По результатам этого эвристического анализа объектам присваивается уровень риска от «1 — хорошо (зеленый)» до «9 -— опасно (красный)». В окне навигации слева разделы окрашиваются в разные цвета в зависимости от уровня риска объекта внутри них.

Означает ли уровень риска «6 — неизвестно (красный)», что объект является опасным?

Анализ ESET SysInspector не гарантирует, что данный объект является вредоносным — эта оценка должна выполняться специалистом по безопасности. Приложение ESET SysInspector разработано для того, чтобы специалист по безопасности имел возможность быстро оценить, какие объекты системы следует изучить и проверить их необычное поведение.

Зачем ESET SysInspector в ходе работы подключается к Интернету?

Как и многие приложения, программа ESET SysInspector подписана цифровым сертификатом, гарантирующим, что издателем программы является компания ESET и что программа не была изменена. Для проверки сертификата и подлинности издателя программы операционная система связывается с центром сертификации. Это нормальное поведение программ с цифровыми подписями в Microsoft Windows.

Что такое технология Anti-Stealth?

Технология Anti-Stealth обеспечивает эффективное обнаружение руткитов.
Если система атакована вредоносной программой, которая ведет себя как руткит, пользователь подвергается риску повреждения, потери или кражи данных. Без специального инструмента для борьбы с руткитами такие программы практически невозможно обнаружить.

Почему иногда в файлах, помеченных как «Подписано MS», в записи «Название компании» стоит название другой компании?

В ходе идентификации цифровой подписи исполняемого файла программа SysInspector сначала проверяет наличие в файле встроенной цифровой подписи. В этом случае при проверке используются идентификационные данные из файла. Если в файле отсутствует цифровая подпись, программа ESI начинает поиск соответствующего CAT-файла (в каталоге безопасности %systemroot%\system32\catroot), содержащего сведения об обрабатываемом исполняемом файле. Если соответствующий CAT-файл найден, при проверке исполняемого файла применяется его цифровая подпись.

Поэтому иногда в некоторых файлах с пометкой «Подписано MS» имеется запись с названием другой компании.

Пример

В системе Windows 2000 есть приложение HyperTerminal, которое находится в папке C:*Program Files\Windows NT*. Исполняемый файл приложения не имеет цифровой подписи, однако программа SysInspector помечает его в качестве подписанного корпорацией Microsoft. Причиной этому служит ссылка в файле C:*WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat*, которая указывает на файл C:*Program Files\Windows NT\hypertrm.exe* (основной исполняемый файл приложения HyperTerminal), а файл *sp4.cat* имеет цифровую подпись Microsoft.

13. ESET SysRescue

Средство ESET SysRescue предназначено для создания загрузочного диска с продуктом ESET NOD32 Antivirus (EAV) или ESET Smart Security (ESS). Главным преимуществом ESET SysRescue является то, что приложения ESS и EAV запускаются независимо от операционной системы компьютера, имея при этом доступ к жесткому диску и всей файловой системе. Это позволяет удалять такие заражения, которые в обычной ситуации (например, при запущенной операционной системе и т. п.) удалить невозможно.

13.1 Минимальные требования

Средство ESET SysRescue работает в среде предустановки Microsoft Windows (Windows PE) версии 2.x, созданной на базе системы Windows Vista. Windows PE является частью свободно распространяемого пакета автоматической установки Windows (Windows AIK), поэтому перед созданием ESET SysRescue необходимо установить Windows AIK (http://www.microsoft.com/Downloads/details.aspx?familyid=94BB6E34-D890-4932-81A5-5B50C657DE08&displaylang=en). Поскольку поддержка среды Windows PE ограничивается ее 32-разрядной версией, при создании пакета ESET SysRescue в 64-разрядных системах необходимо использовать установочный пакет 32-разрядной версии ESS/EAV. Средство ESET SysRescue поддерживает пакет Windows AIK версии 1.1 и выше. Средство ESET SysRescue доступно в составе пакетов ESS/EAV версии 4.0 и выше.

Поддерживаемые операционные системы

- Windows 7
- Windows Vista
- Windows Vista с пакетом обновления 1 (SP1)
- Windows Server 2008
- Windows Server 2003 с пакетом обновления 1 (SP1) с KB926044
- Windows Server 2003 с пакетом обновления 2 (SP2)
- Windows XP с пакетом обновления 2 (SP2) с KB926044

13.2 Создание компакт-диска аварийного восстановления

При условии соответствия минимальным требованиям к созданию компакт-диска ESET SysRescue процедура его создания достаточно проста. Чтобы запустить мастер ESET SysRescue, выберите в меню **«Пуск»** > **«Программы»** > **ESET** > **ESET NOD32 Antivirus** > **ESET SysRescue**.

На первом этапе мастер определяет наличие в системе установленного пакета Windows AIK и подключенного к компьютеру устройства, подходящего для создания загрузочного носителя.

На следующем этапе предлагается выбрать носитель для размещения на нем файлов ESET SysRescue. Помимо компакт-диска, DVD-диска и USB-устройства, образ диска ESET SysRescue можно сохранить в файл ISO. Впоследствии этот файл с ISO-образом можно записать на компакт- или DVD-диск или использовать его другим способом (например, в виртуальной среде VmWare или Virtualbox).

На последнем этапе после указания всех параметров пользователю дается возможность просмотреть отчет о работе мастера ESET SysRescue, проверить правильность параметров и приступить к созданию диска. Доступны перечисленные ниже параметры.

Папки 117
Антивирус ESET 117
Дополнительно 117
Загрузочное USB-устройство 117
Запись 117

13.2.1 Папки

«Временная папка» — это рабочий каталог для файлов, необходимый при создании диска ESET SysRescue.

«Папка с ISO» — это папка, в которую сохраняется полученный ISO-файл.

В списке на этой вкладке перечислены все локальные и сетевые диски с указанием свободного места на них. Если какие-то из папок располагаются на диске с недостатком свободного места, рекомендуется выбрать другой диск, на котором места достаточно. В противном случае недостаток свободного места не позволит создать образ диска.

13.2.2 Антивирус ESET

При создании компакт-диска ESET SysRescue можно выбрать один из двух источников файлов ESET для компилятора:

«Папка ESS» — файлы, уже содержащиеся в папке, в которую установлен программный продукт ESET;
«MSI-файл» — файлы, которые содержатся в установщике MSI.
«Профиль» — источником имени пользователя и пароля может послужить один из двух следующих вариантов:
«Установленный ESS» — имя пользователя и пароль копируются из установленных продуктов (ESET Smart Security или ESET NOD32 Antivirus);
«От пользователя» — имя пользователя и пароль вводятся в соответствующие текстовые поля, расположенные ниже.

Примечание. Продукты ESET Smart Security и ESET NOD32 Antivirus на компакт-диске ESET SysRescue обновляются из Интернета или из решения ESET для обеспечения безопасности, установленного на компьютере, на котором запускается компакт-диск ESET SysRescue.

13.2.3 Дополнительные настройки

На вкладке **«Дополнительно»** можно настроить параметры компакт-диска ESET SysRescue в соответствии с объемом оперативной памяти компьютера. Чтобы записать содержимое компакт-диска в оперативную память (ОЗУ), выберите вариант **«512 МБ и больше»**. Если выбрать вариант **«Меньше 512 МБ»**, при работе WinPE будет постоянно происходить обращение к компакт-диску восстановления.

«Внешние драйверы»: в этом разделе можно добавить драйверы для конкретных аппаратных устройств (обычно для сетевой карты). Хотя система WinPE создана на основе ОС Windows Vista с пакетом обновления 1 (SP1), поддерживающей самое разное аппаратное обеспечение, иногда оборудование не распознается и драйвер для него приходится добавлять вручную. Добавить драйвер на диск ESET SysRescue можно двумя способами: вручную (кнопка **«Добавить»**) и автоматически (кнопка **«Автопоиск»**).При добавлении драйвера вручную необходимо указать путь к соответствующему INF-файлу (в той же папке должен находиться и SYS-файл). В режиме автоматического добавления драйвер находится в операционной системе данного компьютера автоматически. Режим автоматического добавления рекомендуется использовать только в том случае, если средство ESET SysRescue установлено на компьютере с такой же сетевой картой, как и на компьютере, на котором был создан диск ESET SysRescue. При создании компакт-диска ESET SysRescue драйвер добавляется в сборку, поэтому пользователю впоследствии не приходится его искать.

13.2.4 Загрузочное USB-устройство

Если в качестве целевого носителя было выбрано USB-устройство, на вкладке **«Загрузочное USB-устройство»** можно указать один из доступных USB-носителей (если доступно несколько USB-устройств).

13.2.5 Запись

Если в качестве целевого носителя выбран компакт-диск или DVD-диск, на вкладке «Запись» можно задать дополнительные параметры записи.

«Удалить ISO-файл»: установите этот флажок, чтобы удалить ISO-файлы после создания компакт-диска аварийного восстановления ESET SysRescue.
«Включить удаление»: этот параметр позволяет сделать выбор между быстрой и полной очисткой диска.
«Устройство записи»: выберите диск, который будет использоваться для записи.

Предупреждение. Этот параметр установлен по умолчанию. При использовании перезаписываемого компакт- или DVD-диска все данные на нем будут стерты.

В разделе «Носитель» указаны сведения о диске в дисководе.

«Скорость записи»: выберите нужную скорость из раскрывающегося списка. При выборе скорости необходимо учитывать возможности записывающего устройства и тип компакт- или DVD-диска.

13.3 Работа с ESET SysRescue

Для эффективного использования функции аварийного восстановления с носителей CD, DVD и USB необходимо загрузить компьютер с загрузочного носителя, на котором установлено средство ESET SysRescue. Порядок загрузки настраивается в параметрах BIOS. Кроме того, на этапе запуска компьютера можно вызвать меню загрузки; обычно оно вызывается с помощью клавиш F9—F12 (в зависимости от версии системной платы и BIOS).

После загрузки запускается ESS или EAV. Поскольку средство ESET SysRescue используется лишь в особых случаях, некоторые модули защиты и функции ESS и EAV не требуются. В результате список доступных модулей сужен до функций **«Сканирование компьютера»**, **«Обновление»** и ряда модулей в разделе **«Настройка»**. Наиболее важной функцией ESET SysRescue является возможность обновления базы данных сигнатур вирусов. Перед началом сканирования компьютера рекомендуется обновить программу.

13.3.1 Использование ESET SysRescue

Представим себе ситуацию, когда компьютеры в сети заражены вирусами, изменяющими исполняемые файлы (EXE). Система ESS/EAV способна излечить все инфицированные файлы, кроме файла проводника explorer.exe, который не может быть излечен даже в безопасном режиме.
Файл Explorer.exe, как один из основных компонентов системы Windows, загружается и используется даже в безопасном режиме. Система ESS/EAV не может выполнить с этим файлом никаких действий, поэтому он остается зараженным.
В такой ситуации проблему может решить средство ESET SysRescue. Для работы средства ESET SysRescue не требуется ни один компонент операционной системы компьютера, поэтому оно способно обрабатывать (очищать, удалять) любые файлы на диске.