

Сергей Потопенко, potapenko@hi-tech.ua

Панда на страже:

тонкая настройка Panda Internet Security 2009



Полную версию программы ищите на hi-Tech DVD

Что интересно

Ключевыми особенностями Panda Internet Security 2009 (www.pandasecurity.com/ukraine) можно назвать движок Anti-Malware для выявления различного вредоносного ПО, а также усовершенствованную технологию TruPrevent для анализа поведения программ, позволяющую обнаружить неклассифицированные угрозы. Кроме того, в программе достаточно грамотно реализована система родительского контроля — даже самый догадливый ребенок не сможет отключить приложение или удалить его, не зная пароля администратора.

Сегодня большинство антивирусных приложений после установки неплохо справляются с «заразой» и с настройками по умолчанию. Однако «неплохо» — это не «отлично», поэтому настроить программу вручную не повредит

В своих публикациях мы уже не раз поднимали тему антивирусной защиты, тестируя различные программы и рассказывая о тонкостях их работы (см. hi-Tech PRO 4/2008, с. 90, 11/2008, с. 62). Альтернатив достаточно, однако практика показывает, что выбор инструмента — это только полдела. Ведь даже самое мощное и многофункциональное приложение не сможет стать надежной защитой, если не настроить его работу правильно.

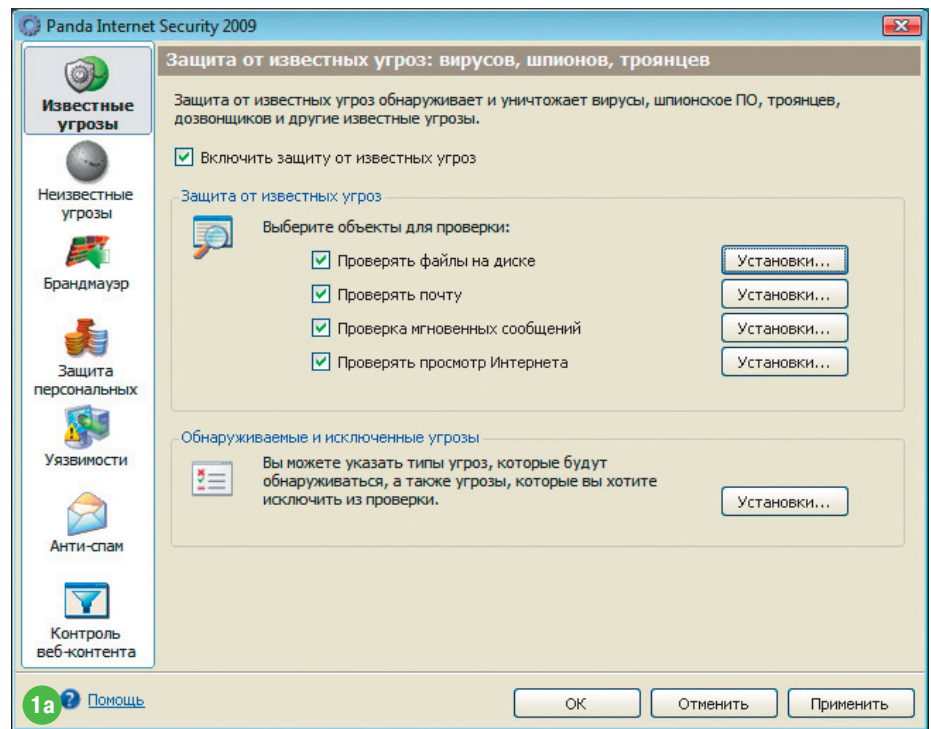
На hi-Tech DVD в феврале вы найдете еще один популярный продукт для защиты ПК от виртуальной инфекции и угроз из Интернета — пакет утилит Panda Internet Security 2009. Далее вы узнаете, как настроить антивирусный модуль, брандмауэр, антиспам-фильтр и другие компоненты приложения таким образом, чтобы оно, с одной стороны, не допустило на ПК программ-вредителей, а с другой — не превратилось в надоедливый параноика ☺.

Настройка Panda Internet Security 2009

Защита

- 1 Антивирус
- 2 Брандмауэр
- 3 Защита персональных данных
- 4 Уязвимости
- 5 Антиспамовый фильтр
- 6 Контроль веб-содержимого

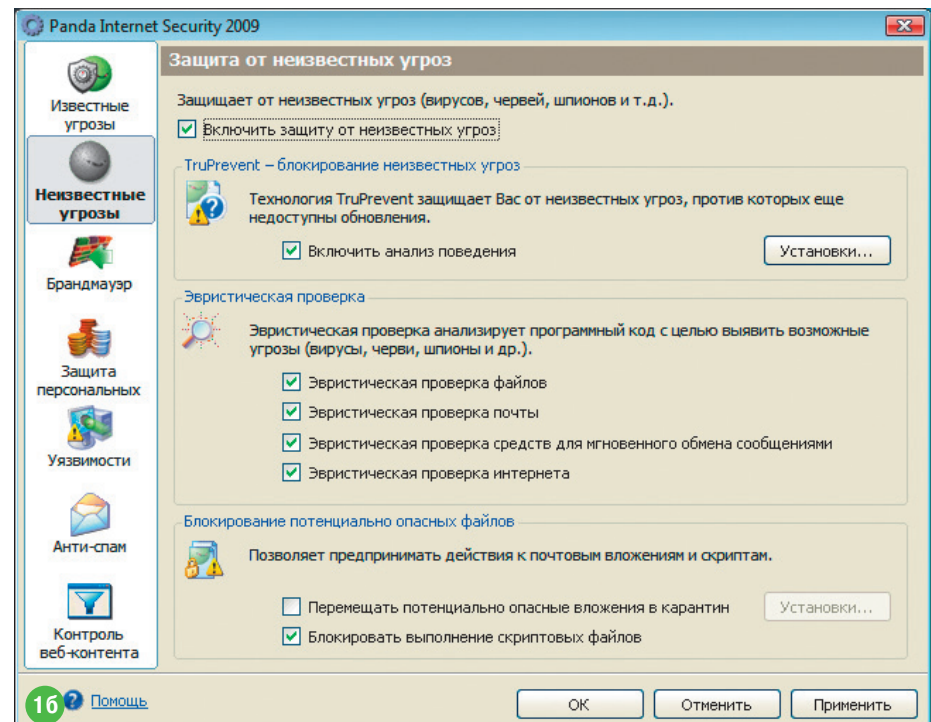
В настройках антивирусного модуля можно исключить из общей проверки некоторые типы угроз



Анализируя поведение процессов, Panda Internet Security 2009 позволит выявить и те зловерные программы, сигнатуры которых отсутствуют в базе приложения (например, новые вирусы)

1 Вирусный КПП

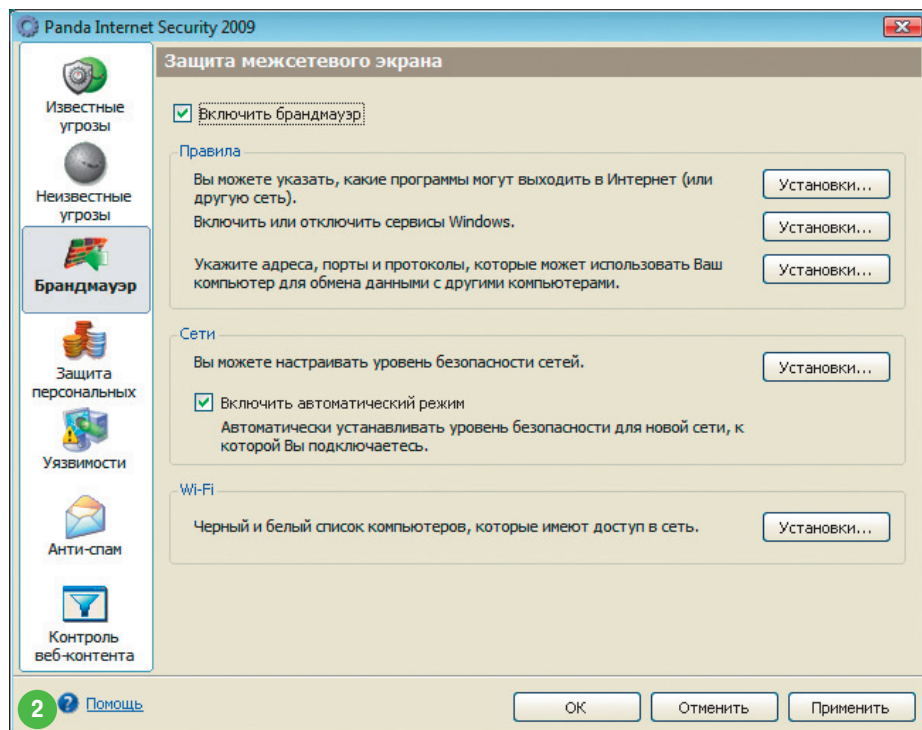
Настройка антивирусного модуля проводится на закладке *Известные угрозы*. Здесь необходимо отметить объекты, которые будут проверяться: файлы на жестком диске, электронная корреспонденция, мгновенные сообщения интернет-пейджеров и веб-сайты. Для каждой из этих категорий можно установить параметры сканирования (кнопка *Установки...* напротив соответствующей записи) — типы проверяемых данных и действия в случае обнаружения инфекции. В настройках проверки почтовых сообщений несложно включить/отключить проверку сообщений, а также прикрепленных к письмам файлов. В разделе *Обнаруживаемые и исключаемые угрозы* можно исключить проверку на некоторые типы угроз. Например, если вы используете утилиты — сканеры локальной сети, антивирус часто рассматривает их как зловерное ПО. В этом случае лучше исключить категорию *Нежелательное ПО* из области проверки.



2 Диагностика на лету

На закладке *Неизвестные угрозы* можно настроить эвристическую проверку данных,

а также включить технологию TruPrevent, анализирующую поведение процессов в системе и на основе результатов анализа де-



Приложение позволит защитить конфиденциальные данные от кражи — просто необходимо внести их в базу программы, чтобы она знала, что не позволить «утащить»

Личный резерв

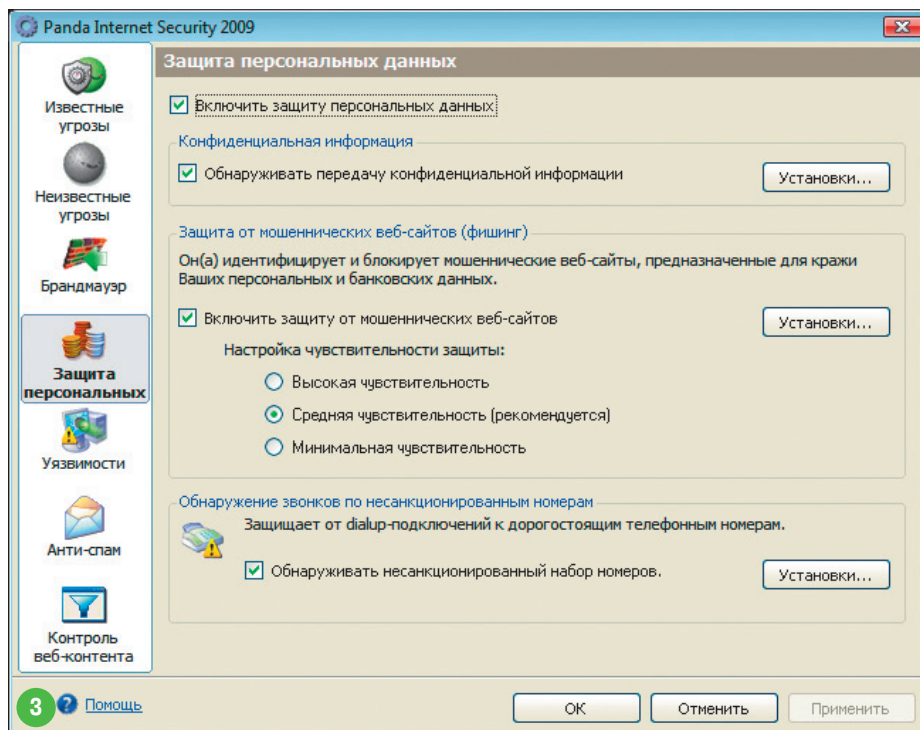
Panda Internet Security 2009 позволяет создать резервную копию важных данных на случай критических сбоев Windows. Причем это можно сделать как вручную, так и запланировать автоматическое обновление бэкапа по расписанию. Для этого на закладке *Статус* в разделе *Обслуживание* нажмите на кнопку *Настроить* и, запустив мастер создания резервных копий (кнопка *Новая копия...*), выберите данные для сохранения и метод создания архива — запланированная или внеочередная копия. Кроме того, приложение позволяет воспользоваться сервисом хранения резервной копии в Интернете. Переход по ссылке *Онлайновая резервная копия* приведет вас на специальный сервер разработчиков программы, на котором вы получите 1 ГБ для хранения своих архивов.

лающую выводы о степени подозрительности объектов. Кроме того, здесь устанавливаются правила блокировки подозрительных вложений в почтовых сообщениях.

5 Крепка ли броня?

Panda Internet Security 2009 может анализировать степень защиты ПК, чтобы выявить возможные уязвимости для проведения атак на ваш компьютер. Чтобы включить эту функцию, на закладке *Уязвимости* отметьте пункт *Включить защиту от уязвимостей*. Чтобы просканировать систему на наличие брешей в защите вручную, перейдите на закладку *Проверка* главного окна приложения и нажмите на *Поиск уязвимостей*.

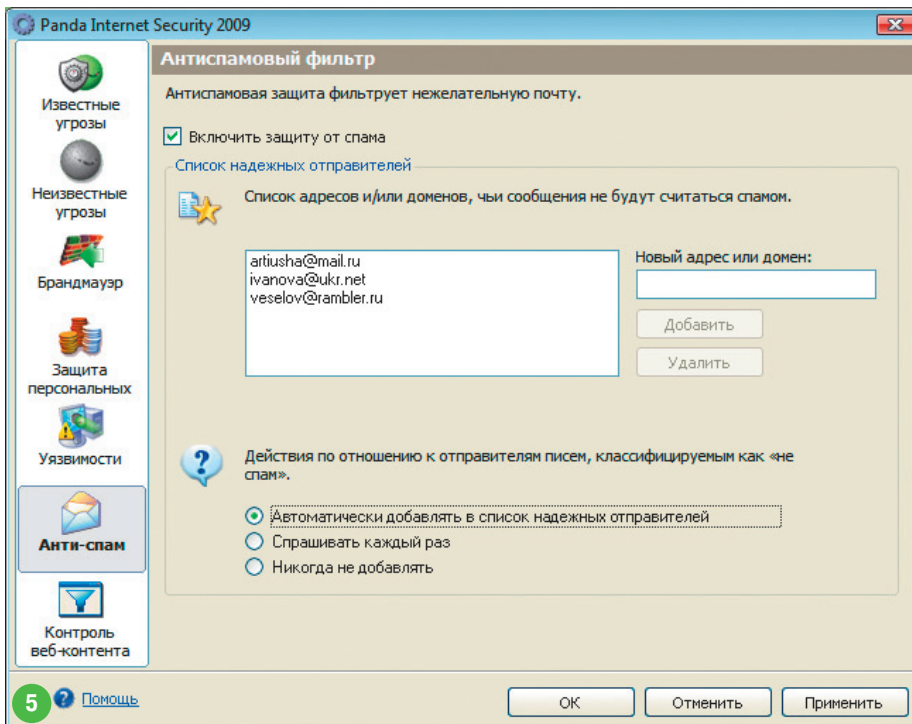
Если вы планируете использовать брандмауэр, не забудьте отключить стандартное средство защиты Windows



3 Непробиваемый барьер

Чтобы настроить работу брандмауэра, необходимо, во избежание возможных конфликтов, отключить стандартный защитник Windows. В разделе *Правила* можно обозначить список приложений, которым разрешено выходить в Интернет, или же, на-

оборот, запретить определенным программам подключение ко Всемирной сети, включить или отключить сервисы синхронизации времени и удаленного *Рабочего стола*, а также указать адреса, порты и протоколы, по которым дозволено производить обмен данными с вашим ПК. При новом подключе-



Чтобы важные сообщения не попали в спам, добавьте проверенные контакты в список надежных отправителей


уровень чувствительности приложения и сформировав белый и черный списки ресурсов. Кроме того, раздел *Конфиденциальная информация* позволяет включить обнаружение передачи личной информации, внося в базу данных Panda Internet Security 2009 пароли, номера счетов, адреса электронной почты и другие данные. Программа способна также «отлавливать» несанкционированные звонки, чтобы предотвратить подключение к дорогостоящим телефонным номерам.

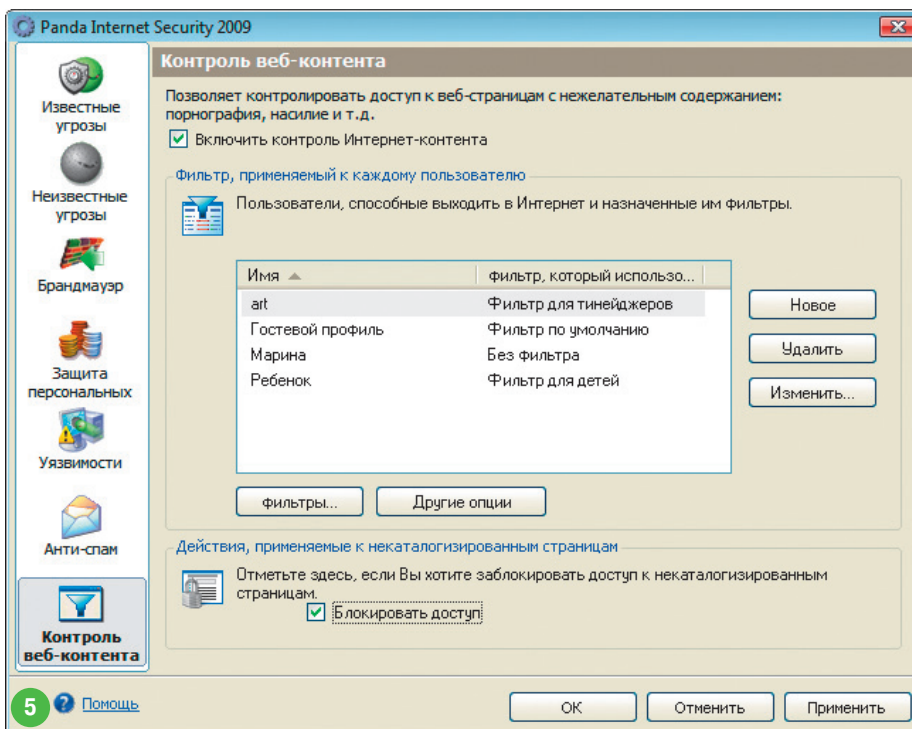
6 Клуб для избранных

Чтобы предотвратить попадание важной почты в список нежелательных сообщений, необходимо составить перечень тех адресов и доменов, корреспонденции от которых вы доверяете на все сто. Тогда полученные от них письма не будут считаться спамом.

7 В Сеть — по пропускам!

На закладке *Контроль веб-контента* вы сможете установить правила фильтрации посещаемых интернет-ресурсов. Сперва необходимо ввести пароль администратора (супервайзера), который впоследствии позволит получить доступ в этот раздел. После этого отметьте пункт *Включить контроль Интернет-контента* и создайте учетные записи для всех, кто пользуется этим компьютером. Нажав на кнопку *Новое*, вы сможете ввести имя пользователя и пароль на его аккаунт. В выпадающем списке *Используется фильтр*: устанавливаются правила доступа к веб-ресурсам. Чтобы узнать, какие ресурсы блокирует определенный фильтр, необходимо щелкнуть на *фильтры...*, выбрать нужный и нажать на *Изменить...* — перед вами список категорий сайтов, доступ к которым будет закрыт. Можно также вручную составить черный и белый списки ресурсов для каждого пользователя. Для этого выберите нужный профиль и нажмите на кнопки *Изменить...* и *Дополнительные установки...*

Естественно, не все ресурсы Всемирной сети попадают под присутствующие в программе категории. Судьбу доступа к ним можно решить с помощью опции *Блокировать доступ* в разделе *Действия, применяемые к некаталогизированным страницам*. 



Чтобы не позволить детям посещать порносайты, включите модуль для контроля веб-содержимого

нии к сети вы сможете установить уровень доверия к соединению, обозначив его как *Надежная директория* (делает компьютер видимым для других пользователей сети) либо *Общественная директория* (ограничивает видимость ПК для других пользователей сети, а также доступ программ в Интер-

нет). Можно также доверить выбор этого режима самой программе, отметив пункт *Включить автоматический режим*.

4 На закладке *Защита персональных данных* вы сможете настроить блокировку мошеннических веб-сайтов, установив