Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности. Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей.

Аудит - это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Практическими средствами регистрации и аудита являются:

· различные системные утилиты и прикладные программы;

· регистрационный (системный или контрольный) журнал.

Значение параметров аудита системы

Параметр	Значение
Аудит событий входа в систему	Определяет, подлежит ли аудиту каждая попытка пользователя войти в систему или выйти из нее на другом компьютере при условии, что данный компьютер используется для проверки подлинности учетной записи. Если этот параметр политики определен, можно задать аудит успехов или отказов, либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.
Аудит управле-ния учетными записями	Определяет, подлежат ли аудиту все события, связанные с управлением учетными записями на компьютере. К таким событиям относятся следующие события: · создание, изменение или удаление учетной записи пользователя или группы; · переименование, отключение или включение учетной записи пользователя; · задание или изменение пароля.
Аудит доступа к службе каталогов	Определяет, подлежит ли аудиту событие доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом.
Аудит входа в систему	Определяет, подлежит ли аудиту каждая попытка пользователя войти в систему или выйти из нее на данном компьютере, или подключиться к нему через сеть.

Аудит доступа к объектам	Определяет, подлежит ли аудиту событие доступа пользователя к объекту - например, к файлу, папке, разделу реестра, принтеру и т. п. - для которого задана собственная системная таблица управления доступом.
Аудит изменения политики	Определяет, подлежит ли аудиту каждый факт изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.
Аудит использования привилегий	Определяет, подлежит ли аудиту каждая попытка пользователя воспользоваться предоставленным ему правом.
Аудит отслеживания процессов	Определяет, подлежат ли аудиту такие события, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.
Аудит системных событий	Определяет, подлежат ли аудиту события перезагрузки или отключения компьютера, а также события, влияющие на системную безопасность или на журнал безопасности.

Механизм регистрации и аудита

активизируется с помощью оснастки *Локальные политики безопасности* (рис. 3.1). Алгоритм активизации состоит из следующих шагов.

- 1. Выбрать кнопку *Пуск* панели задач.
- 2. Открыть меню *Панель управления.*
- 3. В открывшемся окне выбрать ярлык *Администрирование Локальная политика безопасности.*
- 4. Выбрать пункт *Политика аудита* (рис. 3.1).
- 5. В правой части окна отобразится список опций *Политика* и соответствующих им состояний *Параметров безопасности.* Подробное описание каждой политики приведено в табл. 3.1.

Примечание. Значения опции Политика аудита описываются значениями параметров аудита (рис. 3.1). По умолчанию все параметры безопасности Политика аудита выключены.

6. Включить значения аудита для всех видов политики аудита. Такими вариантами значений являются параметры Аудит успеха или аудит отказа:

• для включения или отключения параметров безопасности политики выбрать требуемый вид политик и дважды щелкнуть левой клавишей мыши;

• для каждого вида политики можно задать либо аудит успеха, либо аудит отказа, либо отключить аудит событий данного типа (рис. 3.2);

• нажать кнопку ОК.

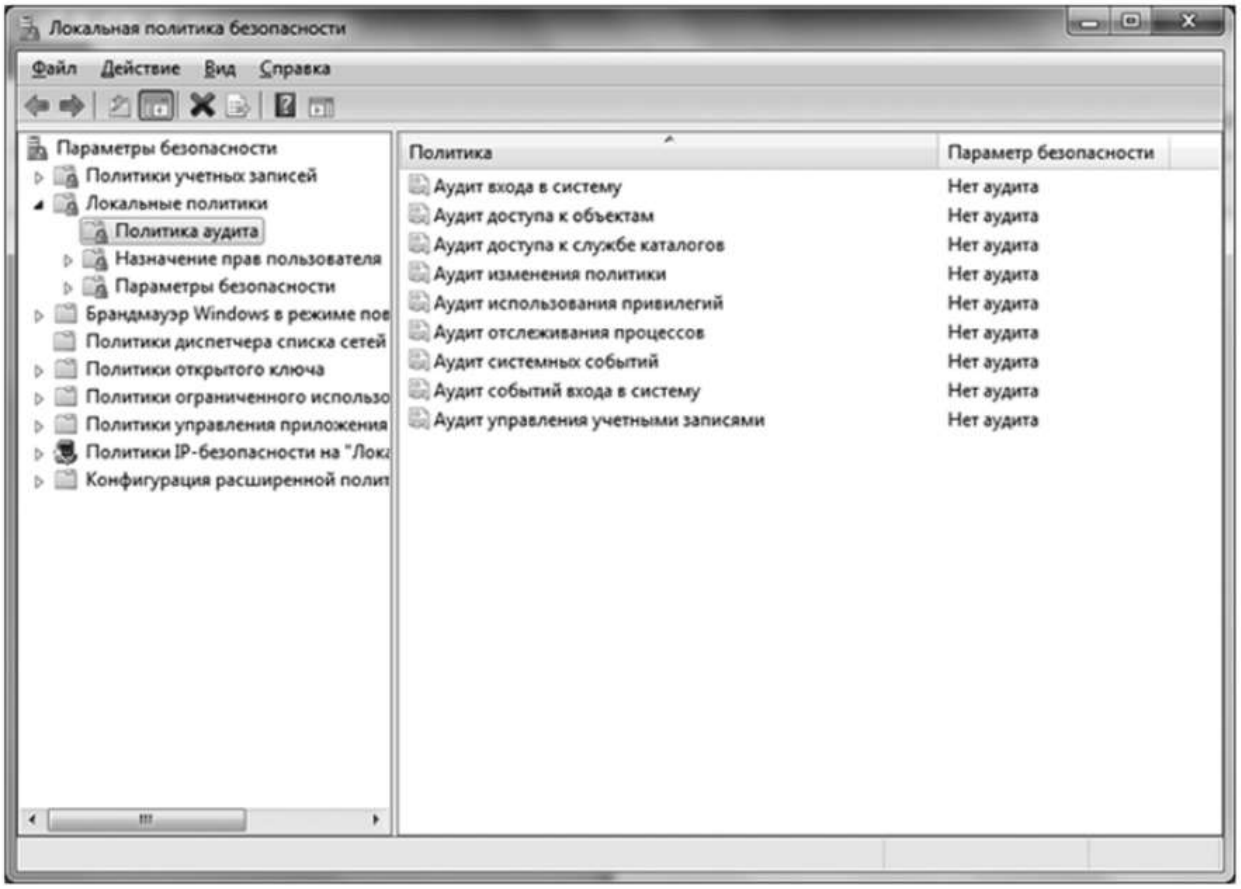

Рис. 3.1. Окно *Локальная политика безопасности. Политика аудита*

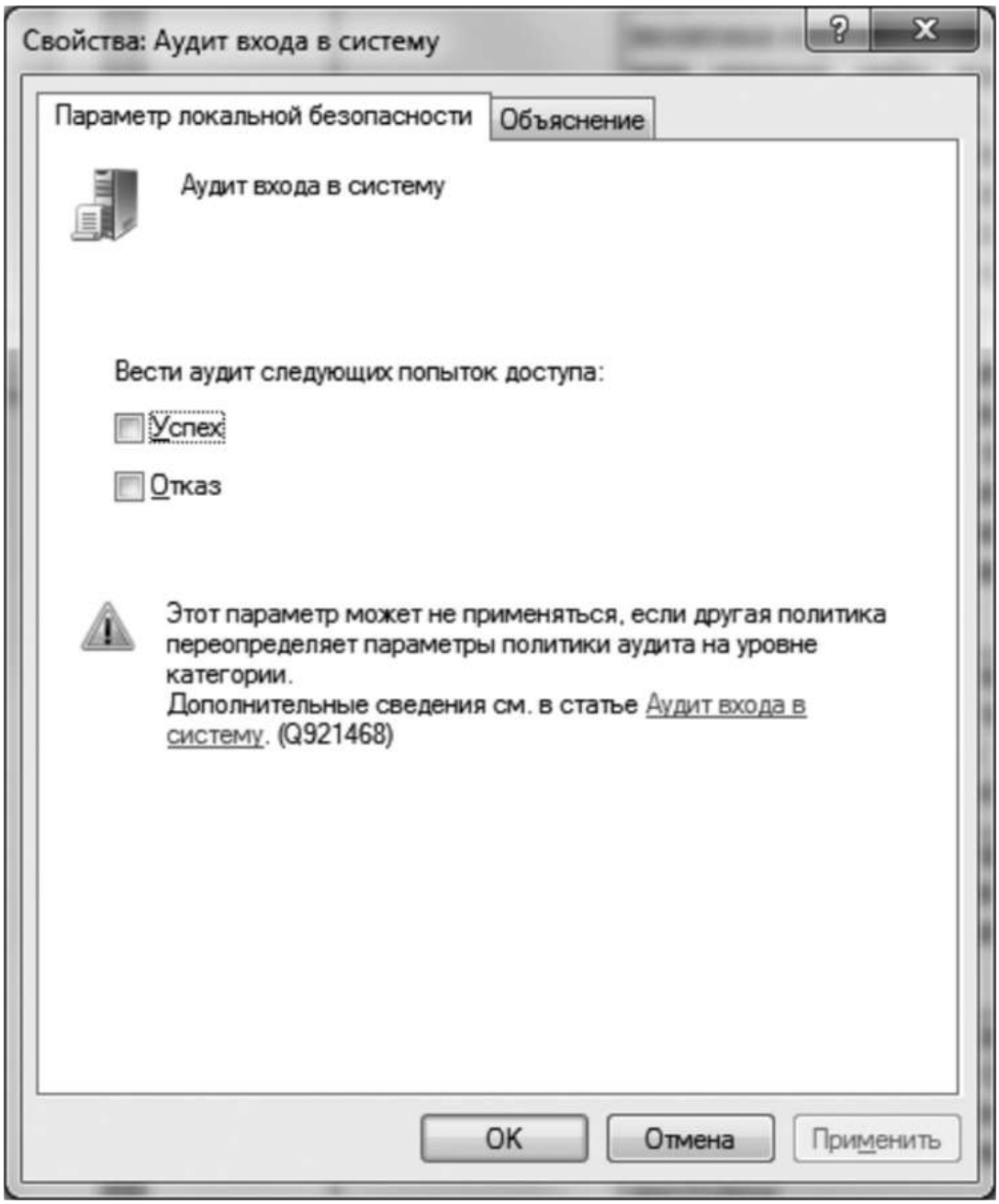

Рис. 3.2. Окно *Свойства: Аудит входа в систему*

Шаблоны безопасности Windows — это файлы, содержащие в специальном формате описания значений системных настроек операционной системы, необходимых для достижения определенного уровня безопасности. Система шаблонов позволяет экспортировать и импортировать настройки политики безопасности, которые записываются в специального вида текстовые файлы с расширением *«.inf»*. Преимущество такого механизма заключается в упрощении переноса данных безопасности на другие компьютеры по сравнению с использованием баз данных безопасности.

При помощи шаблонов безопасности возможно настраивать параметры политики, которые отвечают за следующие компоненты безопасности:

- • *политики учетных записей.* Предназначен для настройки политики паролей, политики блокировки учетной записи;
- • *локальные политики.* Доступны при настройке политики аудита, назначении прав пользователей, а также параметры безопасности, аналогичные параметрам политики оснастки *Редактор объектов групповых политик*;
- • *журналы событий.* Обеспечивает возможность изменения настройки журналов *Приложения, Система* и *Безопасность*, таких как политики создания файлов журналов, максимальный размер ипр.;
- • *группы с ограниченным доступом.* Настройки ограничений доступа пользователей, которые являются членами различных групп;
- • *настройки системных служб.* Предназначены для управления типом запуска и разрешением доступа всех системных служб, которые можно найти в оснастке *Службы*;
- • *настройки системного реестра.* Можно добавлять разрешения на доступ к разделам реестра;
- • *настройки безопасности файловой системы.* Предоставляют возможность задавать разрешения на доступ к файлам и папкам.
- • Установлен ряд предопределенных шаблонов безопасности, перечень которых приведен ниже:
- • *шаблон SETUP SECURITY* содержит используемые по умолчанию параметры безопасности. Его не следует импортировать через групповые политики;
- • *шаблон COMPATWS* ослабляет используемые по умолчанию разрешения доступа группы *Пользователи* к файлам и реестру таким образом, чтобы это соответствовало требованиям большинства несертифицированных приложений, также используется для обеспечения совместимости с более старыми программами и содержит строгие ограничения доступа к системным файлам. Рекомендуется использовать группу *Опытные пользователи* для работы с ^сертифицированными приложениями;
- • *шаблон SECUREWS* предоставляет расширенные политики для управления локальными учетными записями, ограничивает использование проверки подлинности *LanManager,* включает подписывание сообщений протокола *SMB* — сетевого протокола прикладного уровня для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного

взаимодействия, со стороны сервера, накладывает дальнейшие ограничения для анонимных пользователей;

- • *шаблон HISECWS* содержит охватывающий набор для *SECUREWC*. Накладывает дальнейшие ограничения на проверку подлинности *LanManager* и новые требования для шифрования и подписывания данных, передаваемых по безопасным каналам, и данных SMB. Чтобы применить шаблон *HISECWS* к входящим в домен компьютерам, все контроллеры домена, хранящие учетные записи всех пользователей, которые могут выполнить вход на этот клиентский компьютер, должны работать под управлением Windows NT4 SP4 или более поздних систем;
- • *шаблон ROOTSEC* обеспечивает применение стандартных корневых разрешений для раздела операционной системы и распространение их на дочерние объекты, наследующие разрешения от корня. Время распространения зависит от количества незащищенных дочерних объектов;
- • *шаблон SECURE DC* предоставляет расширенные политики для управления учетными записями в домене, ограничивает использование проверки подлинности *LanManager*, накладывает дальнейшие ограничения для анонимных пользователей. Если контроллер домена использует *шаблон SECUREDC,* то пользователь с учетной записью в этом домене не сможет подключаться к рядовым серверам только с помощью клиента *LanManager,*
- • *шаблон HISECDC* содержит охватывающий набор для *шаблона SECUREDC*. Накладывает дальнейшие ограничения на проверку подлинности *LanManager* и новые требования для шифрования и подписывания данных, передаваемых по безопасным каналам, и данных *SMB*. Чтобы применить *шаблон SECUREDC* к контроллеру домена, все другие контроллеры в доверенных и доверяющих доменах должны работать под управлением Windows 2000 или более поздних систем.