

Аудит в операционных системах

Аудит

- Аудит безопасности включает в себя распознавание, запись, хранение и анализ информации, связанной с действиями, относящимися к безопасности.
- Записи, получаемые в результате аудита, могут быть проанализированы, чтобы определить, какие действия, относящиеся к безопасности, происходили, и кто из пользователей их сгенерировал.
- Фиксирование записей происходит в журнале аудита (журнале безопасности).

Задачи, решаемые за счёт осуществления аудита

- Обеспечение подотчётности пользователей и администраторов.
- Обнаружение попыток нарушения информационной безопасности.
- Обеспечение возможности восстановления хода событий при расследовании инцидентов, связанных с информационной безопасностью.

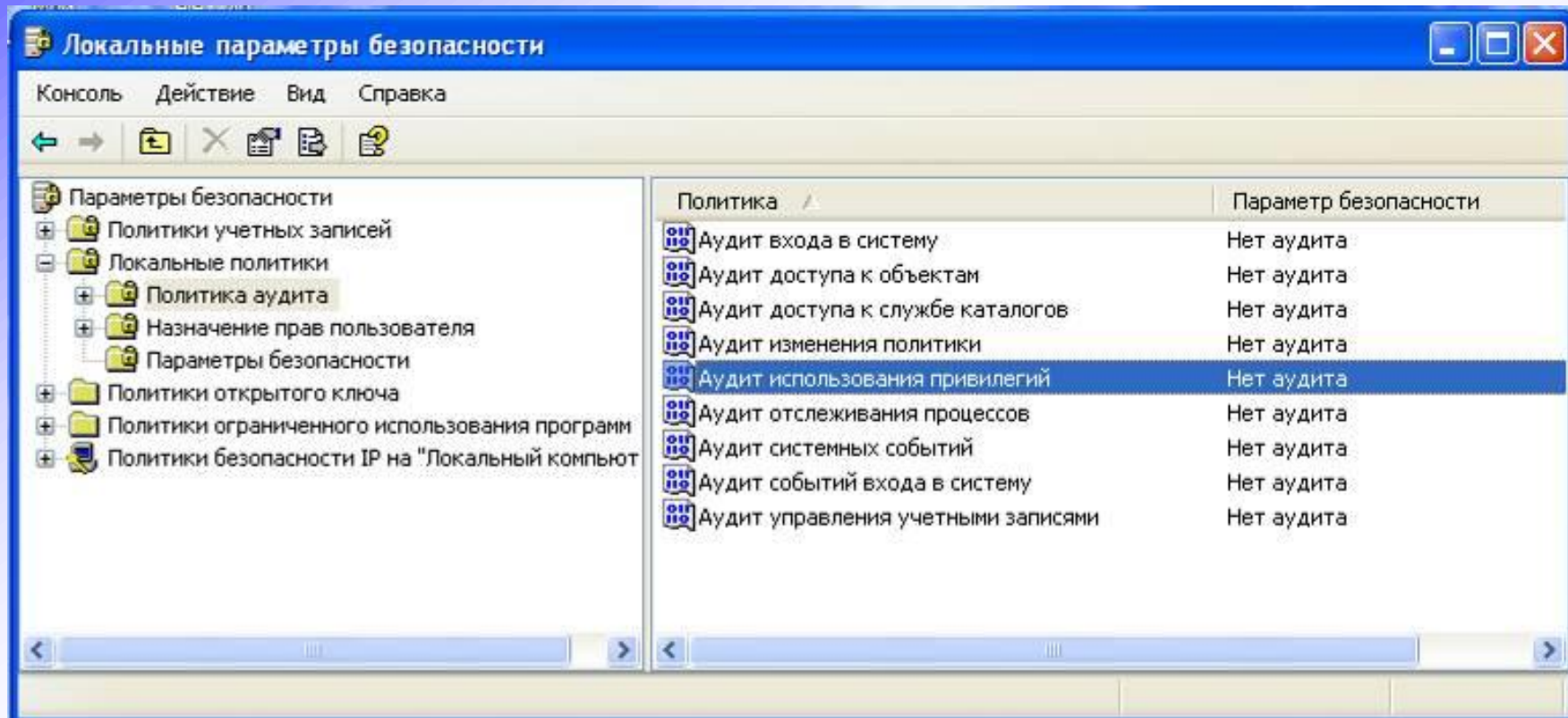
Требования к аудиту в операционных системах

Требования к системе защиты по РД ГТК «СВТ. Защита от НСД»

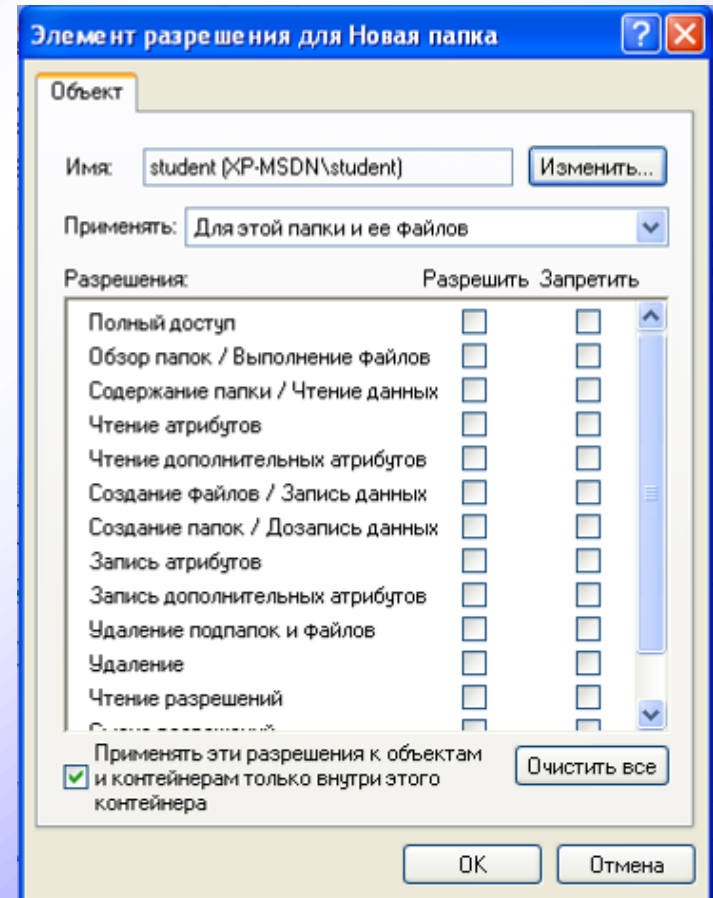
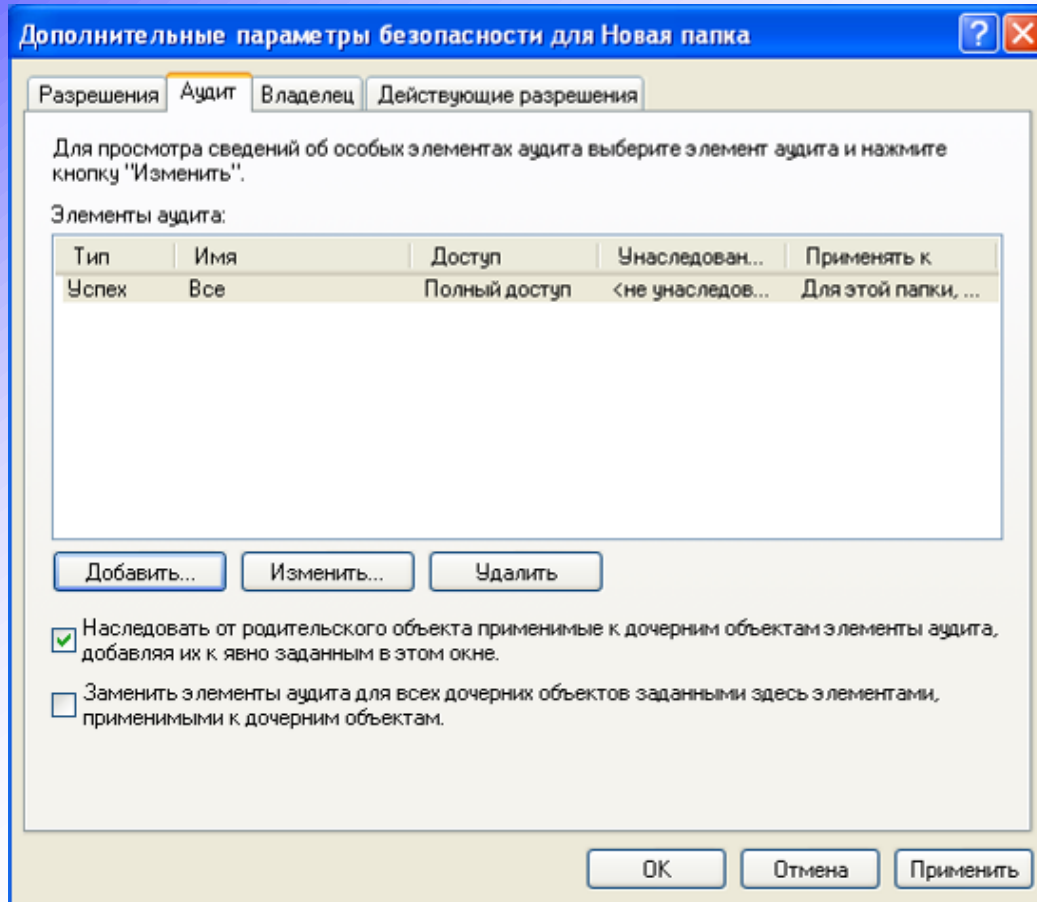
Для 5-го класса защищённости КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
- создание и уничтожение объекта;
- действия по изменению правил разграничения доступа.

Политика аудита в Windows XP



Аудит доступа к файловым объектам в Windows XP

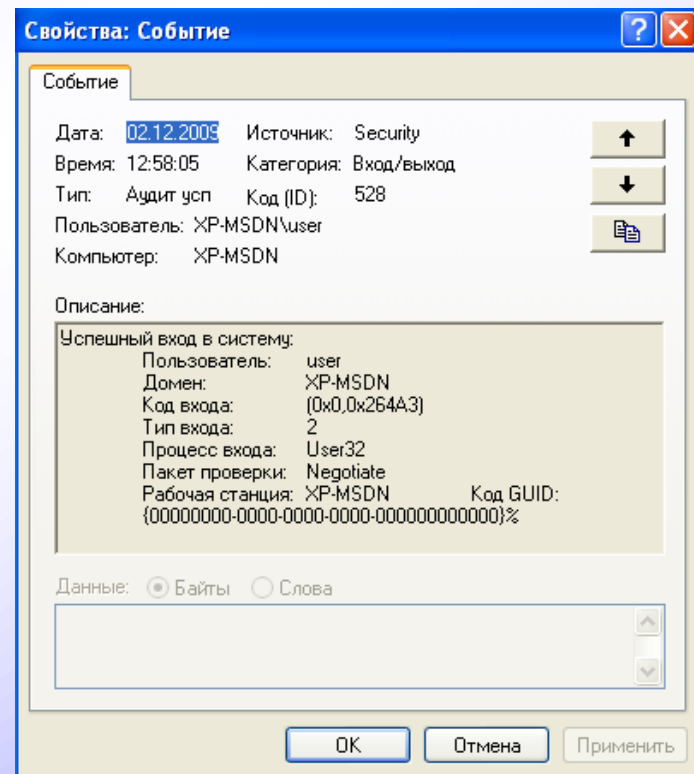
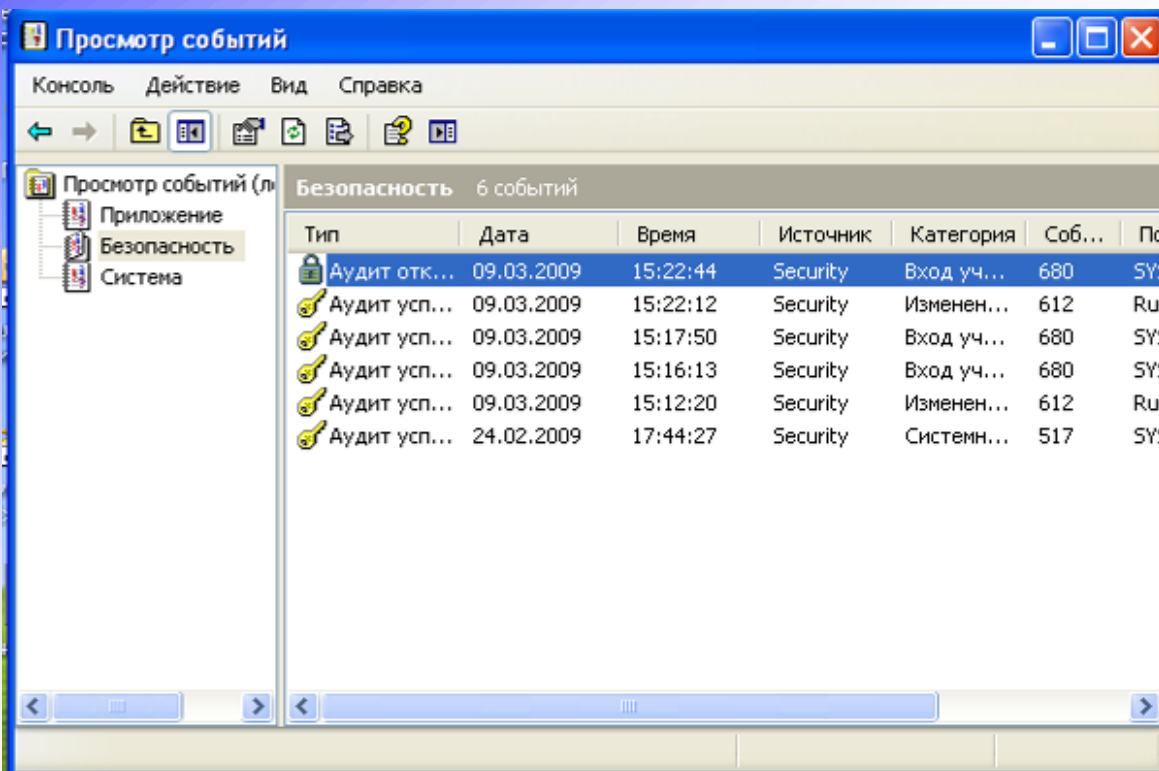


Требования к системе защиты по РД ГТК «СВТ. Защита от НСД»

Для каждого из этих событий должна регистрироваться следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).
- КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией.

Журнал аудита в Windows XP



Требования к системе защиты по РД ГТК «СВТ. Защита от НСД»

Для 4-го и выше класса защищённости дополнительно к требованиям 5-го класса должна быть предусмотрена регистрация всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.).

Требования к системе защиты по РД ГТК «АС. Защита от НСД»

Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и её программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы (все классы);
- результат попытки входа: успешная или неуспешная (при НСД) (все классы, кроме ЗБ);
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа (вся 1-я группа+2А);
- код или пароль, предъявленный при неуспешной попытке (1-я группа, кроме 1Д).

Требования к системе защиты по РД ГТК «АС. Защита от НСД»

Должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов (для классов 2А, 1Г, 1В). Для классов 1Б и 1А – всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный – несанкционированный);
- полная спецификация соответствующего файла "образа" программы (процесса, задания) - устройство (том, каталог), имя файла (расширение) (только для класса 1А).

Требования к системе защиты по РД ГТК «АС. Защита от НСД»

Для классов 2А, 1Г, 1В, 1Б, 1А должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием её результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;
- имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту (для классов 1В, 1Б, 1А);
- вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.) (для классов 1В, 1Б, 1А).

Требования к системе защиты по РД ГТК «АС. Защита от НСД»

Для классов 2А, 1Г, 1В, 1Б, 1А должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием её результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)];
- имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту (для классов 1В, 1Б, 1А);
- вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.) (для классов 1В, 1Б, 1А).

Требования к системе защиты по РД ГТК «АС. Защита от НСД»

Для классов 1В, 1Б, 1А должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

- дата и время изменения полномочий;
- идентификатор субъекта доступа (администратора), осуществившего изменения;
- идентификатор субъекта, у которого проведено изменение полномочий и вид изменения (пароль, код, профиль и т.п.) (для классов 1Б, 1А);
- спецификация объекта, у которого проведено изменение статуса защиты и вид изменения (код защиты, уровень конфиденциальности) (для классов 1Б, 1А).

Требования к системе защиты по РД ГТК «АС. Защита от НСД»

Для классов 1Б, 1А должна осуществляться сигнализация (для класса 1А – надёжная) попыток нарушения защиты на терминал администратора и нарушителя.

Требования к системе защиты по РД ГТК «Безопасность ИТ»

Семейства класса «Аудит безопасности»:

- автоматическая реакция аудита безопасности;
- генерация данных аудита безопасности;
- анализ аудита безопасности;
- просмотр аудита безопасности;
- выбор событий аудита безопасности;
- хранение данных аудита безопасности.

Автоматическая реакция аудита безопасности

- Семейство определяет реакцию на обнаружение событий, указывающих на возможное нарушение безопасности.
- ФБО должны генерировать заданные действия (предупреждение для уполномоченного администратора) при обнаружении возможного нарушения безопасности.

Генерация данных аудита безопасности

Семейство определяет требования по регистрации возникновения событий, относящихся к безопасности, которые подконтрольны ФБО. Это семейство идентифицирует уровень аудита, перечисляет типы событий, которые потенциально должны подвергаться аудиту с использованием ФБО, и определяет минимальный объём связанной с аудитом информации, которую следует представлять в записях аудита различного типа.

Генерация данных аудита безопасности

ФБО должны быть способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту:

- запуск и завершение выполнения функций аудита;
- все события, потенциально подвергаемые аудиту;
- запуск и завершение функционирования операционной системы;
- использование специальных разрешений (например, от уполномоченных администраторов), которые позволяют обходить политики управления доступом.

Генерация данных аудита безопасности

ФБО должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию:

- дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный);
- для каждого типа событий, потенциально подвергаемых аудиту, из числа определённых в функциональных компонентах, которые включены в ПЗ/ЗБ:

идентификатор объекта;

для изменений в данных ФБО – новое значение (кроме данных аутентификации и открытых значений критических данных);

для попыток аутентификации – начало попытки (например, окончание идентификации);

для использования роли – тип роли и начало запроса на роль.

Генерация данных аудита безопасности

ФБО должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события (при неуспешных попытках входа в систему не требуется ассоциация пользователя, потому что пользователь не находится под управлением ФБО до окончания успешной идентификации/аутентификации, тем не менее, начало попытки фиксируется.).

Анализ аудита безопасности

Семейство определяет требования для автоматизированных средств, которые анализируют показатели функционирования системы и данные аудита в целях поиска возможных или реальных нарушений безопасности. Этот анализ может использоваться для поддержки как обнаружения проникновения, так и автоматической реакции на ожидаемое нарушение безопасности. Может работать в реальном времени и в пакетном режиме.

- ФБО должны быть способны применить набор правил мониторинга событий, подвергающихся аудиту, и указать на возможное нарушение ПБО, основываясь на этих правилах.
- ФБО должны реализовать накопление или объединение заданных событий, потенциально подвергаемых аудиту, указывающих на возможное нарушение безопасности.

Анализ аудита безопасности

Выявление аномалии, основанное на профиле:

- ФБО должны быть способны сопровождать профили использования системы, где каждый отдельный профиль представляет известные шаблоны предыстории использования, выполнявшиеся участниками целевой группы;
- ФБО должны быть способны сопровождать рейтинг подозрительной активности для каждого пользователя, чьи действия отражены в профиле, где рейтинг подозрительной активности показывает степень несогласованности действий, выполняемых пользователем, с установленными шаблонами использования, представленными в профиле;
- ФБО должны быть способны указать на ожидаемое нарушение ПБО, когда рейтинг подозрительной активности пользователя превышает заданные пороговые условия.

Анализ аудита безопасности

Простая эвристика атаки:

- ФБО должны быть способны сопровождать внутреннее представление заданных характерных событий системы, которые могут указывать на нарушение ПБО;
- ФБО должны быть способны сравнить характерные события с записью показателей функционирования системы, полученных при обработке заданной информации, используемой для определения показателей функционирования системы;
- ФБО должны быть способны указать на ожидаемое нарушение ПБО, когда событие системы соответствует характерному событию, указывающему на возможное нарушение ПБО.

Анализ аудита безопасности

Сложная эвристика атаки:

- ФБО должны быть способны сопровождать внутреннее представление заданных последовательностей событий известных сценариев проникновения и заданных характерных событий системы, которые могут указывать на возможное нарушение ПБО;
- ФБО должны быть способны сравнить характерные события и последовательности событий с записью показателей функционирования системы, полученных при обработке информации, используемой для определения показателей функционирования системы;
- ФБО должны быть способны указать на ожидаемое нарушение ПБО, когда показатели функционирования системы соответствуют характерному событию или последовательности событий, указывающим на возможное нарушение ПБО.

Просмотр аудита безопасности

Компонент предоставит уполномоченным пользователям возможность получать и интерпретировать информацию. Для человека-пользователя эту информацию требуется представлять в понятном для него виде. Для внешнего объекта ИТ информацию требуется представлять только в электронном виде.

- ФБО должны предоставлять уполномоченным администраторам возможность читать всю информацию аудита из записей аудита.
- ФБО должны предоставлять записи аудита в виде, позволяющем уполномоченному администратору воспринимать содержащуюся в них информацию, используя средство доступа к журналу аудита.

Просмотр аудита безопасности

- ФБО должны запретить всем пользователям доступ к чтению записей аудита, за исключением пользователей, которым явно предоставлен доступ для чтения.
- ФБО должны предоставить возможность выполнить поиск и сортировку данных аудита, основанные на следующих атрибутах:
 - идентификатор пользователя;
 - дата события;
 - время события;
 - тип события.

Выбор событий аудита безопасности

ФБО должны быть способны к включению событий, потенциально подвергаемых аудиту, в совокупность событий, подвергающихся аудиту, или к их исключению из этой совокупности по следующим атрибутам:

- идентификатор объекта;
- идентификатор пользователя;
- идентификатор узла сети;
- тип события.

Хранение данных аудита безопасности

Семейство определяет требования, при выполнении которых ФБО способны создавать и сопровождать журнал аудита безопасности.

- ФБО должны защищать хранимые записи аудита от несанкционированного удаления.
- ФБО должны быть способны предотвратить модификацию записей аудита.
- Когда журнал аудита становится полным, ФБО должны генерировать предупреждение об опасности уполномоченному администратору и предоставлять администратору возможность предотвращать подвергающиеся аудиту события (кроме сгенерированных уполномоченным администратором при обслуживании ОО).

Просмотр и хранение данных аудита безопасности

Свойства: Безопасность

Общие **Фильтр**

Типы событий

Уведомления Аудит успехов
 Предупреждения Аудит отказов
 Ошибки

Источник события: Security

Категория: Вход/выход

Код события:

Пользователь:

Компьютер:

С: первого 02.12.2009 12:57:48

До: последнего 02.12.2009 12:59:05

Восстановить умолчания

OK Отмена Применить

Свойства: Безопасность

Общие **Фильтр**

Выводимое имя: Безопасность

Имя журнала: C:\WINDOWS\System32\config\SecEvent.Evt

Размер: 64,0 КБ (65 536 байт)

Создан: 25 августа 2008 г. 20:17:25

Изменен: 25 августа 2008 г. 20:17:25

Открыт: 25 августа 2008 г. 20:17:25

Размер журнала

Максимальный размер журнала: 512 КБ

По достижении максимального размера журнала:

Затирать старые события по необходимости

Затирать события старше 7 дней

Не затирать события (очистка журнала вручную)

Восстановить умолчания

Подключение по медленной линии

Очистить журнал

OK Отмена Применить

События аудита в Windows XP

- События системы – события, связанные с безопасностью, такие как отключение системы и её перезапуск; события, влияющие на журнал безопасности.
- Отслеживание процесса – детализированное отслеживание вызова процесса, дубликатов процессов, непрямого доступа к объектам и уничтожения процесса.
- Изменение политики – изменение политики безопасности, включая присвоение привилегий, модификацию политики аудита и параметров доверия.

События аудита в Windows XP

- Использование привилегий – использование привилегий, присвоение специальных привилегий.
- Управление учётной записью – создание, изменение, удаление пользователей и групп; изменение паролей.
- Доступ к службе каталогов – отслеживание доступа к Active Directory. Включается для разрешения аудита определенных объектов каталога, работает только на контроллерах домена.

События аудита в Windows XP

- События входа в учетную запись – аутентификация на локальном компьютере или через сеть.
- События входа – интерактивный вход или сетевые подключения к локальному компьютеру; генерируются в том месте, где происходит вход.
- Доступ к объектам – попытки доступа к определённым объектам: файлам, каталогам, учётным записям пользователей и параметрам реестра.

Типы событий, потенциально подвергаемых аудиту

- Вход (выход) пользователей в операционную систему.
- Доступ к защищаемым ресурсам (создание, чтение, изменение, удаление и др.).
- Управление учётными записями (создание, удаление, смена пароля и др.).

Типы событий, потенциально подвергаемых аудиту

- Изменение правил и прав разграничения доступа.
- Использование привилегий (чтение журнала аудита, резервное копирование и др.).
- Работа процессов (запуск программ, обращение процесса к файлу и др.).

Данные, фиксируемые при ведении аудита

- Дата и время события.
- Имя учётной записи пользователя, запросившего действие.
- Имя рабочей станции, где произошло событие.
- Тип события.
- Было ли дано разрешение на выполнение запрошенного действия (Успех) или в выполнении действия было отказано (Отказ).

Дополнительные данные, фиксируемые при ведении аудита

- При отслеживании работы процессов указывается имя программы с указанием полного пути к ней.
- При доступе к ресурсам указываются имя ресурса и использовавшийся тип доступа.
- При изменении правил разграничения доступа к ресурсу указывается не только пользователь, изменявший права, но пользователь, которому они были изменены, а также имя ресурса.

Примеры анализа данных аудита

- Установка аудита отказов на доступ к конфиденциальному файлу – можно определить, какие пользователи, не имевшие права доступа, пытались его прочесть.
- Установка аудита успехов на работу с принтером – можно определить, кто распечатывал конфиденциальный документ.

Методы активного аудита

Пассивный и активный аудит

- Пассивный аудит подразумевает сохранение информации о событиях в соответствующем журнале и дальнейший анализ (с установленной периодичностью) этой информации уполномоченным лицом.
- Активный аудит подразумевает наличие возможности обнаружения попыток нарушений информационной безопасности и автоматического выполнения определённых действий в качестве реакции на это нарушение.

Методы, используемые в системах активного аудита

- Сигнатурный метод – основан на сравнении текущих событий с набором сигнатур атаки. Сигнатура атаки – совокупность условий, при выполнении которых атака считается имевшей место.
- Статистический метод – выявление нетипичного («подозрительного») поведения пользователей путём сравнения текущего значения выбранных характеристик с пороговыми значениями.

Примеры работы методов активного аудита

- Сигнатура атаки – три неудачных попытки входа пользователя в систему. Реакция системы активного аудита – блокирование учётной записи пользователя.
- Статистическая характеристика – резкое превышение среднестатистического размера сетевого трафика.

Особенности сигнатурного метода

Достоинства:

- высокая производительность;
- малое количество ошибок первого рода;
- обоснованность решений.

Недостаток:

- неумение обнаруживать неизвестные атаки и вариации известных атак.

Особенности статистического метода

Достоинства:

- универсальность;
- возможность обнаружения неизвестных атак – уменьшение количества ошибок второго рода.

Недостатки:

- увеличение количества ошибок первого рода;
- некачественная работа при типичности неправомерного поведения, при плавном переходе от легального поведения к неправомерному, а также при отсутствии типичного поведения пользователя.

Возможная реакция системы активного аудита

- Оповещение сотрудника службы безопасности.
- Блокирование выхода в Интернет.
- Блокирование учётной записи пользователя.
- Блокирование действий приложения.
- Блокирование доступа к определённым данным.

Контроль целостности

Контролируемые характеристики

- Активность средства защиты информации.
- Целостность средства защиты информации.
- Целостность аппаратной конфигурации.
- Целостность исполняемых файлов (файлов с данными).
- Целостность настроек средства защиты информации.
- Целостность ключей реестра.

Этапы контроля целостности

- Создание эталона объекта.
- Проверка целостности объекта.
- Реакция на обнаружение нарушения целостности объекта.

Требования к средству защиты при контроле целостности

- Средство защиты информации должно иметь возможность обнаруживать нарушение целостности объекта.
- При обнаружении нарушения целостности объекта средство защиты информации должно предоставлять возможность восстановления корректного экземпляра объекта из сохранённого эталона.

Требования к средству защиты при контроле целостности

- Средство защиты информации должно предоставлять уполномоченному администратору возможность санкционированного изменения эталона (подтверждения внесённых в эталон изменений).

Анализ и настройка безопасности в Windows

Шаблон безопасности

- Шаблон безопасности – набор настроек ОС Windows, связанных с информационной безопасностью.
- Шаблон безопасности используется в качестве эталона для контроля целостности входящих в него настроек.

Состав шаблона безопасности

- Настройки политики учётных записей (политики паролей, блокировки).
- Настройки локальной политики безопасности.
- Настройки аудита.
- Настройки учётных записей пользователей.
- Настройки системных служб.
- Настройки доступа и аудита доступа к ключам реестра.
- Настройки доступа и аудита доступа к файловым объектам.

Предустановленные шаблоны безопасности

- Setup security – шаблон, применяемый при установке ОС.
- Compatws – содержит разрешения по умолчанию для рабочих станций и серверов (не контроллеров домена).
- Securews – шаблон для настройки рабочих станций; определяются параметры надежных паролей, блокировки и аудита.
- Securedc – шаблон для настройки рабочих станций; определяются параметры надежных паролей, блокировки и аудита.

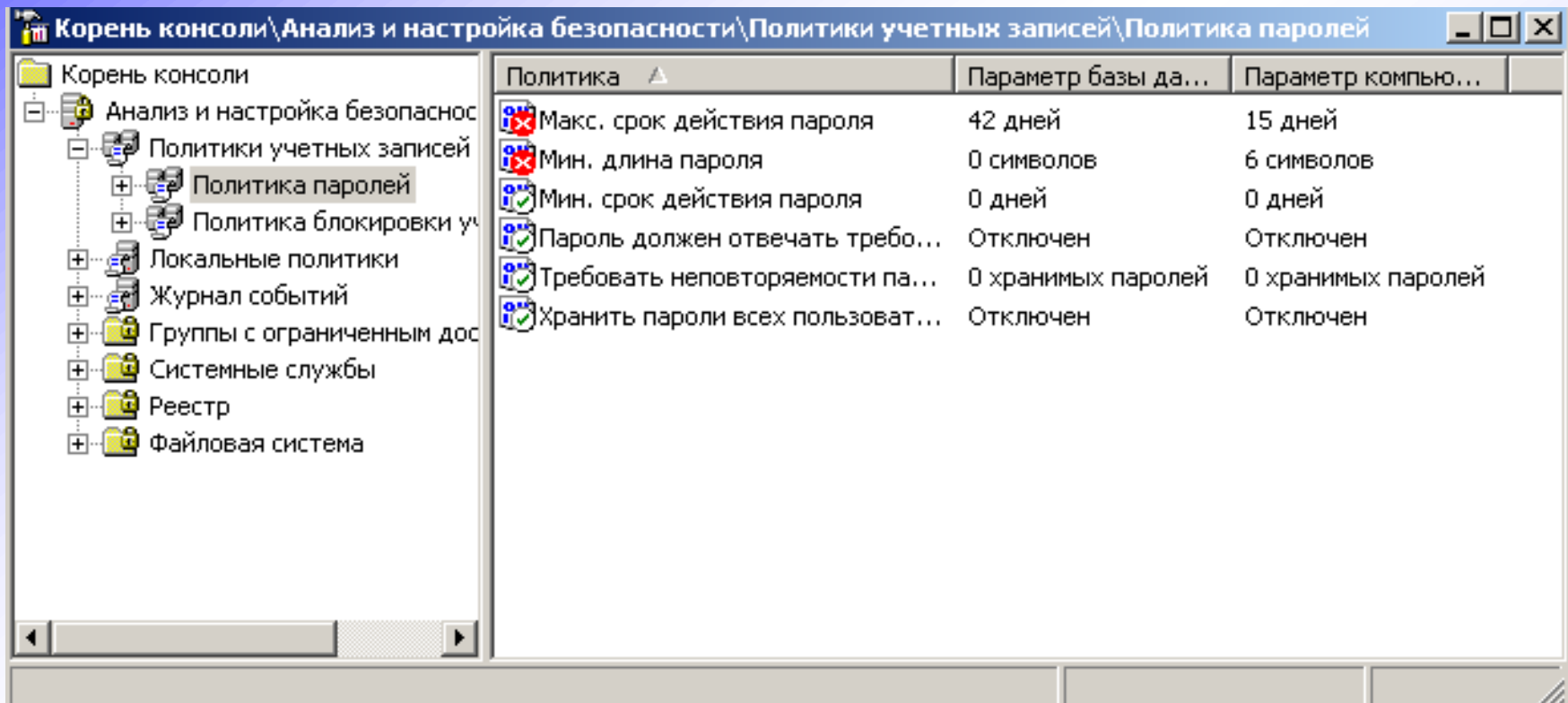
Предустановленные шаблоны безопасности

- Hisecws – шаблон с повышенными требованиями защиты для рабочих станций.
- Hisecdc – шаблон с повышенными требованиями защиты для контроллеров домена.
- Rootsec – шаблон включает разрешения для корневого каталога Windows.

Анализ безопасности

- Анализ безопасности включает сравнение текущих настроек ОС, связанных с безопасностью, с шаблоном.
- Результатом сравнения является перечень настроек, значения которых отличаются от эталонных (т.е. настроек, целостность которых была нарушена).

Результаты анализа безопасности



The screenshot shows the Windows Security console window titled "Корень консоли\Анализ и настройка безопасности\Политики учетных записей\Политика паролей". The left pane shows a tree view with "Политика паролей" selected. The right pane displays a table of policy parameters.

Политика	Параметр базы да...	Параметр компью...
Макс. срок действия пароля	42 дней	15 дней
Мин. длина пароля	0 символов	6 символов
Мин. срок действия пароля	0 дней	0 дней
Пароль должен отвечать требо...	Отключен	Отключен
Требовать неповторяемости па...	0 хранимых паролей	0 хранимых паролей
Хранить пароли всех пользоват...	Отключен	Отключен

Варианты результатов анализа безопасности

- Элемент определен в базе данных анализа и в системе; значения параметров безопасности совпадают.
- Элемент определен в базе данных анализа и в системе, однако, значения параметров безопасности не совпадают.
- Элемент определен в базе данных анализа, однако, не существует в текущей конфигурации системы.

Настройка безопасности

- Настройка безопасности подразумевает восстановление из эталона (шаблона безопасности) настроек безопасности.
- Может использоваться для автоматизации настройки ОС за счёт применения параметров из шаблона к реальной ОС.

Рассмотренные вопросы

- Требования к организации аудита, входящие в руководящие документы.
- События, подвергаемые аудиту.
- Особенности пассивного и активного аудита.
- Контроль целостности настроек безопасности операционной системы Windows.

**Всем спасибо –
все свободны,
если нет вопросов**