# Лабораторная работа № 1
# Взлом пароля в системе Windows 7

## 1. Цель работы

В рамках выполнения лабораторной работы необходимо ознакомиться с процедурой «Взлома/Обнуления» пароля пользователя в операционной системеWindows 7.

Продолжительность работы — 2 часа.

## 2. Теоретическая часть

### 2.1. Введение

**Под взломом пароля** в рамках теории компьютерной безопасности и крипто анализа понимается процесс восстановления паролей из данных, которые были сохранены или переданы с помощью компьютерной системы. Суть метода заключается в применении метода подбора для нахождения пароля. Не менее эффективным способом является процедура восстановления пароля в случае, если он был «забыт».

Существует множество причин, из-за которых приходится прибегать к методам взлома:

1. в случае если пользователь забыл пароль (в этом случае смена пароля возможна, если у пользователя есть права администратора);
2. несанкционированный доступ к системе;
3. проведение проверочных работ администраторами сети, когда они тестируют возможность взлома.

При взломе файловой системы пароль необходим для получения доступа к цифровой информации, доступ к которой как правило и ограничен паролем.

### 2.2. Основные характеристики программы SAMInside

Программа SAMInside предназначена для восстановления паролей пользователей Windows NT, Windows 2000,

Windows XP, Windows 2003, Windows Vista, Windows 7 и имеет ряд особенностей, выгодно отличающих ее от аналогичных программ:

— Данный программный продукт облает небольшим размером, в инсталляции нет необходимости и может запускаться с внешнего носителя (например: USB-накопитель, SD-карта, CD/DVD-диск).

— Для взлома паролей программа позволяет использовать 6 видов атак для восстановления паролей.

Атаки для восстановления пароля подразделяют на следующие виды:

— атака полным перебором;

— атака распределенным перебором;

— атака по маске;

— атака по словарям;

— гибридная атака;

— атака по предварительно рассчитанным Rainbow-таблицам.

Программа позволяет в короткие сроки осуществить побор пароля, что обусловлено ее написанием на машинном языке Ассемблер.

Программа корректно извлекает имена и пароли пользователей Windows в национальных кодировках символов.

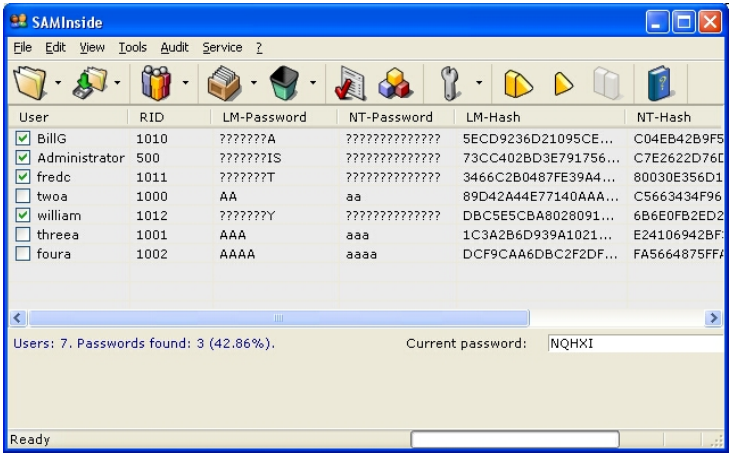


*Рис. 1.1.* Диалоговое окно

## 2.3. Импорт данных

Программа имеет следующие возможности для импорта данных:

«Import SAM and SYSTEM Registry Files» — импорт пользователей из файла SAM реестра Windows. Если в загружаемом файле SAM используется дополнительное шифрование ключом SYSKEY (а в Windows 2000/XP/2003/Vista такое шифрование включено принудительно), то программе дополнительно потребуется файл SYSTEM реестра Windows, располагающийся в той же директории Windows, что и файл реестра SAM, а именно — в каталоге %SystemRoot%\System32\Config. Также копии этих файлов могут находиться в каталогах %SystemRoot%\Repair и %SystemRoot%\Repair\RegBack.

«Import from *.HDT File» — импорт пользователей из файлов, создаваемых программами Proactive Windows Security Explorer и Proactive Password Auditor.

«Import from *.LST File» — импорт пользователей из файла LMNT.LST, создаваемого программой Cain&Abel.

«Import LM-Hashes from *.TXT File» — импорт списка LM-хэшей из текстового файла.

«Import NT-Hashes from *.TXT File» — импорт списка NT-хэшей из текстового файла.

«Import Local Users ...» — импорт пользователей с локального компьютера (для этого программу нужно запустить под пользователем с правами Администратора). В программе используются следующие методы получения хэшей локальных пользователей:

«...via LSASS» — импорт локальных пользователей, используя подключение к процессу LSASS.

«...via Scheduler» — импорт локальных пользователей с использованием системной утилиты Scheduler.

## 2.4. Экспорт данных

Для экспорта данных в программе предусмотрены следующие инструменты:

— «Export Users to PWDUMP File» — экспорт всех пользователей в текстовый файл в формате программы PWDUMP.

После чего полученный файл можно загружать в любую программу для восстановления паролей.

— «Export Selected Users to PWDUMP File» — экспорт выделенных пользователей в текстовый файл в формате программы PWDUMP.

— «Export Found Passwords» — экспорт найденных паролей в формате «User name: Password».

— «Export Statistics» — экспорт текущей статистики программы в текстовый файл.

— «Export Users to HTML» — экспорт информации о пользователях в HTML-файл.

## 2.5. Способы и методы хранения паролей в Windows

ОС Windows хранит все пароли в зашифрованном виде. При этом применяемый алгоритм шифрования является необратимым, т. е. он не подлежит расшифровке, но возможность подобрать такой пароль, который после шифрования будет таким же, как и искомый, сохраняется.

Искомый и подобранный пароль могут не совпасть, но в зашифрованном виде они являются абсолютно одинаковыми. Данное явление носит название ***коллизия***. Поэтому чем сложнее алгоритм шифрования, тем он дает меньше коллизий.

**Хэш-функция** позволяет реализовать необратимое (однонаправленное) шифрование, процесс шифрования получил название **хэширование**, а результат соответственно **хэшем**.

Учетные записи ОС как правило для доступа запрашивают пароль, который, не хранится в открытом виде, а хэшируется с помощью OWF функции. Таким образом пароль сохраняется в ОС в виде хэша.

При следующей попытке входа ОС запрашивает пароль, который также хэшируется и сравнивается с ранее сохраненным. В случае совпадения — пользователь получает доступ к системе, в противном случае ему необходимо еще раз ввести пароль.

Таким образом, оригинальный текстовый пароль не хранится в системе.

## 2.6. Способы подбора паролей

*Атака полным перебором*

В данном случае подбор паролей выполняется перебором всех возможных вариантов паролей.

Помимо полного перебора, данный метод позволяет реализовать и распределенный перебор, который для восстановления пароля использует несколько компьютеров, распределив между ними обрабатываемые пароли. В случае если пользователь задает количество компьютеров, задействованных в атаке более одного, то автоматически запускается распределенный подбор паролей. Затем на текущем компьютере появляется возможности настройки диапазона паролей для атаки.

Для реализации атаки методом распределённого перебора необходимо выполнить следующую последовательность действий:

1. Активировать программу на нескольких компьютерах.
2. Задать во всех активированных программах требуемое количество ПК.
3. Установить одинаковые настройки для перебора на всех компьютерах.
4. Для каждого ПК задать свой диапазон перебора паролей.
5. Запустить на каждом компьютере атаку полным перебором.

*Атака по маске*

При наличии какой-либо первоначальной информации о пароле позволяет применять данный вид атак. Например:

— пароль начинается с комбинации символов «12345»;

— первые 4 символа пароля — цифры, остальные — латинские буквы;

— пароль имеет длину 10 символов и в середине пароля есть сочетание букв «admin»;

Настройки перебора по маске позволяют сформировать маску для перебираемых паролей, а также установить максимальную длину перебираемых паролей.

В программе используются следующие символы маски:

? — Любой печатаемый символ (ASCII-коды символов 32...255).

A — Любая заглавная латинская буква (A...Z).

a — Любая строчная латинская буква (a...z).

S — Любой специальный символ (!@#...).

N — Любая цифра (0...9).

1...8 — Любой символ из соответствующего пользовательского набора символов.

*Атака по словарям*

Словарь — это текстовый файл, состоящий из часто употребляемых паролей типа:

— 1.123;

— admin;

— master.

При активации атаки по словарям можно выбрать также и гибридную атаку, которая имеет возможность добавлять к проверяемым паролям до 2 символов справа и слева, что позволяет восстанавливать такие пароли как «master12» или «#admin».

*Атака по предварительно рассчитанным таблицам*

Алгоритм работы атаки основывается на применении Rainbow-технологию в процессе создания предварительно рассчитанных таблиц.

Дополнительные возможности программы:

1. Программа имеет возможность осуществлять проверку паролей всех пользователей системы. Для активации данной функции в текстовом поле «Current password:» необходимо ввести нужный пароль и нажать F2, после чего программа проверит данный пароль на всех пользователях, пароль к которым еще не найден.

2. «Скрытый режим» работы программы (Ctrl+Alt+H).

Работа в этом режиме позволяет программисту полностью исчезнуть с экрана и с панели задач. Нажатие той же комбинации клавиш возвращает пользователя в обычный режим.

3. Архив программы содержит консольные утилиты для работы с файлами реестра SAM и SYSTEM:

— GetSyskey — программа извлекает из файла реестра SYSTEM системный ключ SYSKEY и сохраняет его в отдельный 16-байтовый файл.

— GetHashes — программа извлекает хэши пользователей из файла реестра SAM, используя файл с ключом SYSKEY.

— LoginRecoveryToPWDUMP — программа преобразует хэши из формата программы «Login Recovery» в формат PWDUMP.

— PasswordToSyskey — программа генерирует ключ SYSKEY на основе вводимого пароля.

### 2.7. Методика составления «защищенного» от подбора пароля

Проблема обеспечения надежности паролей к учетным записям важных пользователей является довольно сложной.

Не смотря применения максимально сложной многоуровневой системы безопасности данных, если у учетных записей пользователей сети недостаточно сложные пароли, безопасность всей сети будет находиться под угрозой.

С применением групповой политике необходимо внедрять ограничения по созданию сложных паролей. Но, не смотря на то, что данная политика позволит существенно усложнить пароли, от атаки хакеров никто не застрахован.

Необходимо объяснить сотрудникам важность создания для разных учетных записей разных паролей и хранить все пароли только в голове. Поскольку ни один пароль не является совершенным, через определенные промежутки времени возникает необходимость их менять.

Пароли необходимо периодически менять, т. к. ни один пароль не может быть совершенным.

## 3. Порядок выполнения работы

1. На первом этапе необходимо запустить виртуальную машину с ОС Windows 7 с помощью программы VMware Workstation.

2. Затем создать учетную запись «Студент» с паролем, включающим в себя только цифры (минимальная длина 7 символов, максимальная — 9).

3. Запустив CD/DVD-приводы, подключаем предложенный нам ISO образ диска, выполняем перезагрузку ОС. Перед

началом загрузки Windows 7 будет предложен на выбор ряд опций, установленных на этом диске. Необходимо указать опцию Alklivedvd.

4. Как только ОС запустилась необходимо запустить программу SAMInside.

После запуска операционной системы запускаем программу SAMInside (Пуск — Все программы — Взломщики — SAMInside). В папке Windows\System32\config в файле реестра SAM и System лежат пароли пользователей ОС Windows.

Затем для подбора паролей добавляем файл в программу. В появившемся списке выбираем необходимого пользователя, методику хэширования, параметры для перебора. Через пункт меню Сервис — Настройки задаются параметры перебора, тип (в рамках выполнения работы рассматриваем от A-Z, a-z и от 0 до 9) и запускаем выполнение атаки. В случае если пароль оказался довольно простым, программа почти сразу выдаст результат, в противном случае запускается режим прямого перебора. Как только программа завершила работу выполняем перезагрузку ОС.

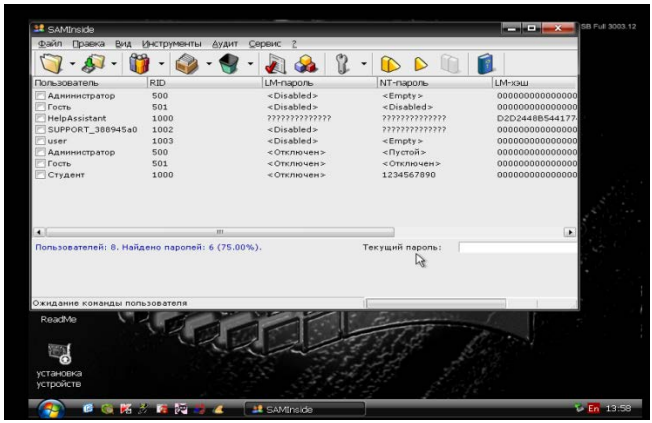


*Рис. 1.2.* Процесс работы программы SAMInside

5. После перезагрузки, выбираем опцию с диска Active@ Password Changer. Данная программа предоставляет список пользователей ОС в режиме DOS (*рис. 1.3*). Далее выбрав нужного пользователя, «студент», обнуляем его пароль, в ходе чего, при загрузке ОС Windows больше не требовала ввода пароля.

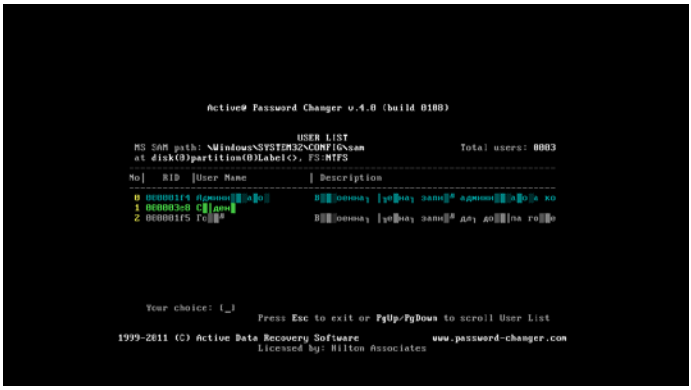


*Рис. 1.3.* Процесс работы программы Active@ Password Changer v.4.0 (build 0108)

## 4. Форма и содержание отчета

Отчет должен содержать:

1. Титульный лист.
2. Описание хода работы со скриншотами.
3. Список литературы.

Отчет выполняется на листах формата А4 печатным способом. Должен содержать цели и задачи работы, ход выполнения, сопровождающийся соответствующими иллюстрациями, заключение.

## 5. Контрольные вопросы

1. Опишите процесс взлома пароля пользователя.
2. Назовите основное назначение программы SAMInside.
3. Опишите алгоритм работы с применением программы SAMInside в рамках лабораторной работы.
4. Перечислите основные способы хранения пароля.
5. Дайте определения терминам хэш и коллизия.
6. Назовите известные вам виды атак для восстановления пароля учетной записи.
7. Опишите алгоритм «Атака полным перебором».
8. Опишите принципы и алгоритм работы «Атака по словарям».

**9.** Какой метод является наиболее эффективным для восстановления сложного пароля?

# Лабораторная работа № 2
# Разграничение прав доступа пользователей

## 1. Цель работы

В рамках выполнения работы необходимо ознакомиться и реализовать на практике методы разграничения доступа учетных записей пользователей в ОС Windows.

Продолжительность работы — 4 часа.

## 2. Теоретическая часть

Рассмотрим основные понятия и определения.

**Политика информационной безопасности** — набор законов, мероприятий, правил, требований, ограничений, инструкций, нормативных документов, рекомендаций и т. д., регламентирующих порядок обработки информации и направленных на защиту информации от определенных видов угроз.

**Объект доступа (Access object) —** единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

**Субъект доступа (Access subject)** — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Идентификация (Identification)** — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Идентификатор доступа (Access identifier)** — уникальный признак субъекта или объекта доступа.

**Аутентификация (Authentication)** — проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

**Авторизация (Authorization)** — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

**Права доступа** — совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы (*информации*, её носителям, процессам и другим ресурсам) установленных правовыми документами или собственником, владельцем информации.

Под правами доступа понимается разрешенный набор операций над объектами данных пользователю той или иной учетной записи. Такое разграничение прав возможно с применением специализированного ПО.

## 2.1. Политики управления доступом

Согласно ГОСТу Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии РФ определены три вида (принципа) разграничения доступа:

— дискретное управление доступом;
— мандатное управление доступом;
— управление доступом по ролям.

### *2.1.1. Дискретное управление доступом*

**Дискретное управление доступом** представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Данный метод основан на том, что некий субъект сети, обладающий максимальными правами (как правило владелец объекта) определяет права доступа к объекту остальным пользователям.

Текущее состояние прав доступа в случае дискретного управления доступом описывается матрицей, в строках которой перечислены субъекты, а в столбцах — объекты (*табл. 2.1*).

*Таблица 2.1*

**Матрица доступа**

| | $Q_1$ | $Q_2$ | … | $Q_n$ |
|---|---|---|---|---|
| $S_1$ | *r* | *r, w* | … | *r* |
| $S_2$ | *r,a* | *0* | … | *e* |
| … | … | … | … | … |
| $S_n$ | *r,w* | *0* | … | *e* |

В клетках, расположенных на пересечении строк и столбцов, записываются способы доступа для субъекта по отношению к объекту, например: чтение, запись, выполнение, возможность передачи прав другим субъектам и т. д.

В данном случае каждый элемент $\mathbf{M_{ij}}$ матрицы доступа **M** определяет права доступа Si**-го** субъекта к $\mathbf{Q_j}$**–му** объекту (чтение, запись, выполнение и т. п.).

Элементы в матрице доступа имеют следующие значения: r — чтение, w — запись, e — выполнение, a — дописать в файл, 0 — нельзя использовать.

### *2.1.2. Мандатное управление доступом*

**Мандатное управление доступом** основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности. *Метка субъекта* определяет уровень его полномочий. *Метка объекта* — степень его конфиденциальности.

Метки безопасности состоят из двух частей: уровня секретности и списка категорий. Уровни секретности, поддерживаемые системой, образуют упорядоченное множество, которое может выглядеть, например, так:

— особой важности;

— совершенно секретно;

— секретно;

— несекретно.

Категории образуют неурегулированный набор. Их назначение состоит в описании наглядной области, к которой относятся данные. Механизм категорий позволяет разделить информацию «по отсекам», что способствует лучшей защищенности. Субъект не может получить доступ к «чужим категориям», даже если его уровень полномочий — «совершенно секретно».

Данный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированные метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

### *2.1.3. Разграничение доступа по ролям*

**Ролевая модель** разграничения доступа основана на конструировании ролей и назначении их пользователям на основании выполняемых ими конкретных должностных обязанностей. При назначении и использовании ролей возможно наложение динамических и статических ограничений на совмещение разных ролей одним субъектом, одновременное использование одной роли разными субъектами и т. п. Подобный подход к разграничению доступа к объектам позволяет разделить обязанности между конструктором ролей и диспетчером ролей, а также более точно связать права доступа пользователей к объектам компьютерной системы с их обязанностями, исключить избыточность полномочий.

## 3. Порядок выполнения работы

1. На первом этапе выполнения работы необходимо задать трех пользователей с различным типом прав. Пользователю под номером 1 наделяем обычным типом прав и паролем на вход в систему. Второму пользователю также присваиваем обычные права, но не даем пароля для входа в систему. Права администратора и пароль на вход систему отдаем пользователю под номером 3.

2. В каждой из созданных учетных записей создаем по одной папке в корневой директории на диске С.

3. Теперь необходимо создать вложенную папку и текстовый документ в имеющихся под каждым пользователем директориях.

4. Затем выполняем разграничение прав доступа:

— Необходимо войти в свойства каждой из созданных папок.

— В появившемся меню выбираем пункт «Безопасность» — «Дополнительно» — «Изменить» — нажимаем последовательно клавиш «Добавить» — «Дополнительно» — «Поиск». После чего необходимо выбрать кнопку «Ок».

5. Выбираем учетную запись Пользователь 1 и заходим, устанавливаем права для текстового документа «Только на чтение» для «Всех пользователей». На вложенную папку Пользователя 2 установить запрет на запись.

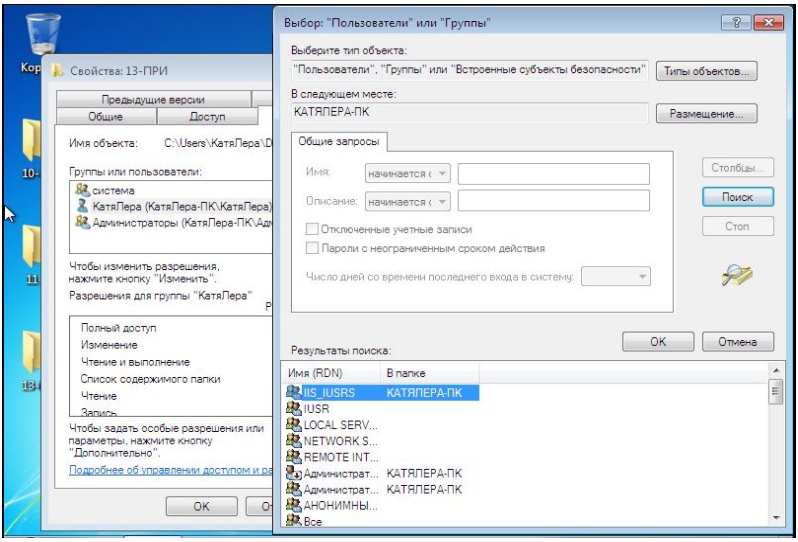


*Рис. 2.1.* Меню присваивания прав на доступ к папке пользователям и группам пользователей

6. Выбираем учетную запись Пользователь 2 и заходим, устанавливаем для текстового документа «Запрет доступа к документу» для всех пользователей, кроме Пользователя 2. Пользователю 3 устанавливаем запрет на доступ к вложенной папке.

7. Выбираем учетную запись Пользователь 3 и заходим, разрешаем пользователю 3 доступ к текстовому документу и вложенной папке, а остальным пользователям запрещаем.

8. Выбираем учетную запись Пользователь 1 и выполняем проверку в директории Пользователя 2. Получаем отказ в доступе к текстовому документу. А в директории Пользователя 3 запрещен доступ к текстовому документу и вложенной папке.

9. Выбираем учетную запись Пользователь 2. При попытке доступа в директорию Пользователя 1 к текстовому документу мы его открываем, но наталкиваемся на запрет во внесении изменений, а для вложенной папки существует запрет на запись. После этого переходим в директорию Пользователя 3, и видим что, установлен запрет для текстового документа и вложенной папки.

10. Выбираем учетную запись Пользователь 3. Видим, что в директории Пользователя 1 для текстового документа установлены только права на чтение, а в директории Пользователя 2 установлен запрет доступа к документу и вложенной папке.

11. Затем входим в журнал событий с помощью команды eventvwr.msc.

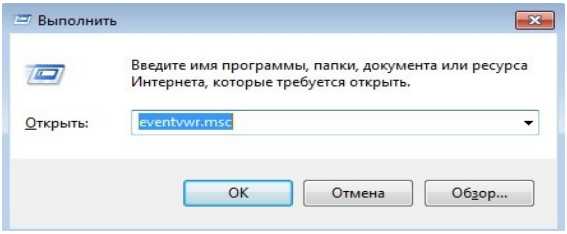


*Рис. 2.2.* Вызов журнала событий

12. В открывшемся диалоговом окне выбираем «Просмотр событий» — «Журнал Windows» — «Безопасность» — выбираем заданное событие и создаем для него задачу. Для этого необходимо в меню справа выбрать «Действие» — «Привязать задачу к событию». После этого на экране появится новое диалоговое окно.

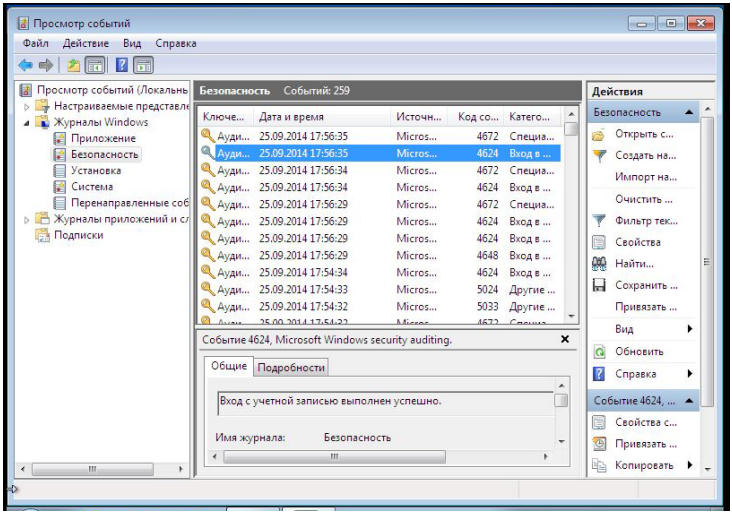


*Рис. 2.3.* Диалоговое окно «Журнал событий»

13. Для заполнения строк открывшегося окна необходимо учесть:

— В качестве «Имени» необходимо указать «Лабораторная работа №»;

— В «Описании» — записываем список выполнивших работу студентов и номер группы.

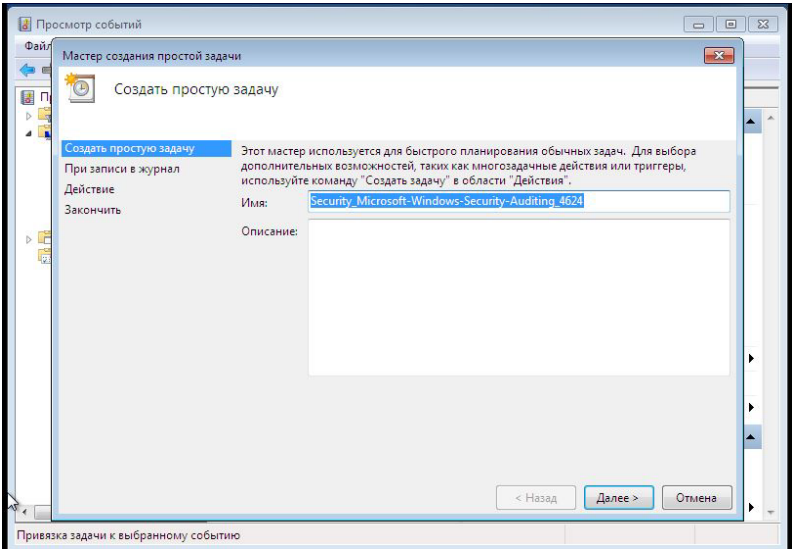


*Рис. 2.4.* Диалоговое окно «Создание задачи для события»

## 4. Форма и содержание отчета

Отчет должен содержать:

1. Титульный лист.
2. Описание хода работы со скриншотами.
3. Список литературы.

Отчет выполняется на листах формата А4 печатным способом. Должен содержать цели и задачи работы, ход выполнения, сопровождающийся соответствующими иллюстрациями, заключение.

## 5. Контрольные вопросы

1. Дайте определение политике информационной безопасности.

2. Дайте определение и назовите основные отличия понятий: идентификация, аутентификация и авторизация.

3. Права доступа и что они определяют.

4. Виды (принципы) разграничения доступа.

5. В каких целях применяется матрица разграничения доступа?

6. Назовите основные принципы мандатного управления доступом.

7. Разграничение доступа по ролям.