МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Анализ файловой структуры по идентификаторам пользователей в NTFS

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Митиной Елены Дмитриевны

Научный руководитель
к. ю. н., доцент _____ А. В. Гортинский
19.01.2026 г.

Заведующий кафедрой
д. ф.-м. н., профессор _____ М. Б. Абросимов
19.01.2026 г.

Саратов 2026

ВВЕДЕНИЕ

Актуальность темы состоит в том, что анализ файловой структуры по идентификаторам пользователей в NTFS, имеет широкий спектр применения. Его можно применять для выявления возможных нарушений безопасности, таких как несанкционированный доступ или использование привилегий другими пользователями. Также с помощью него можно решить проблемы с доступом или другими нарушениями прав доступа, в управлении ресурсами, например, определении того, какие файлы и папки находятся под контролем определенного пользователя и какие права доступа к ним у него есть.

Целью данной преддипломной практики является программная реализация анализа файловой структуры по идентификаторам пользователей в NTFS.

Исходя из поставленной цели, необходимо решить следующие задачи:

1) осветить в работе теоретические аспекты, необходимые для реализации;

2) написать программу на высокоуровневом языке программирования, которая должна решать следующие задачи:

2.1) формировать список SID, файлы владельцев которых присутствуют в указанном разделе;

2.2) формировать список SID, тех владельцев, чьих файлов нет в указанном разделе;

2.3) формировать список файлов с указанным (из сформированного ранее списка) SID владельца;

2.4) формировать список файлов, на которые у пользователя с данным SID (из сформированного ранее списка) есть право на запись;

2.5) формировать список файлов, на которые у пользователя с данным SID (из сформированного ранее списка) есть право на чтение;

2.6) формировать список файлов с пустым ACL и по требованию удалить его;

2.7) формировать статистику типовых путей для каждого пользователя;

2.8) сканировать систему на предмет возможных аномалий размещения файлов и нарушений прав доступа.

Дипломная работа состоит из введения, 6 разделов, заключения, списка использованных источников и 3 приложений. Общий объем работы – 147 страниц, из них 61 страница – основное содержание, включая 57 рисунков и 2 таблицы, список использованных источников из 13 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В разделе 1 «Дескриптор безопасности» рассмотрены основы модели безопасности Windows и роль дескриптора безопасности как ключевой структуры контроля доступа. Описаны составляющие дескриптора безопасности, разница между списками DACL и SACL, а также влияние наличия или отсутствия списка DACL на фактический доступ к объекту.

В разделе 2 «Архитектура файловой системы NTFS» изложены ключевые элементы архитектуры NTFS, необходимые для понимания, как в системе хранится и применяется информация о владельцах и правах доступа.

В подразделе 2.1 «Master File Table» показано, что одной из ключевых концепций NTFS является хранение служебных данных в виде файлов, вследствие чего центральным элементом файловой системы выступает главная файловая таблица MFT (Master File Table), содержащая сведения обо всех файлах и каталогах. Каждый объект представлен как минимум одной записью MFT, при необходимости формируется несколько записей, где первая считается базовой.

В подразделе 2.2 «Атрибуты записей MFT» описано, что основная часть информации о файле хранится в виде набора атрибутов, каждый из которых имеет тип и собственную структуру. Помимо этого, объясняется различие резидентных и нерезидентных атрибутов, которое заключается в том, что резидентные размещаются непосредственно внутри записи MFT, тогда как нерезидентные хранятся во внешних кластерах, и в MFT сохраняются лишь ссылки на их расположение. Также приводится назначение файла метаданных $AttrDef, описывающего атрибуты и их характеристики.

В подразделе 2.3 «Атрибут $STANDARD_INFORMATION» описана структура обязательного для всех файлов и каталогов атрибута $STANDARD_INFORMATION. Он содержит ключевые метаданные объекта, включая сведения, относящиеся к идентификации владельца и безопасности. Среди полей особое внимание уделяется Owner ID (идентификатор владельца)

и Security ID (идентификатор безопасности), так как рассмотрение этих понятий задает основу для выполнения практической части работы. Здесь показано, что Owner ID обычно автоматически заполняется при создании объекта и позволяет определить владельца, а Security ID (SID) используется вместо имени, для идентификации всего, что производит в системе действия.

В подразделе 2.4 «Файлы метаданных файловой системы» показано, что NTFS использует специализированные файлы метаданных, имена которых начинаются с «$», для хранения административных данных файловой системы. Здесь приводится перечень основных файлов метаданных, среди которых выделяется $Secure как критически важный для хранения сведений о безопасности.

В подразделе 2.5 «Файл метаданных $Secure» описано, что в NTFS дескрипторы безопасности хранятся в файле $Secure. Непосредственно данные дескрипторов размещаются в атрибуте $SDS, а для эффективного поиска и сопоставления используются индексы $SDH и $SII. Индекс $SDH предназначен для обращения к дескрипторам по хэш-значению и содержит ссылки на записи в $SDS, тогда как $SII обеспечивает связь SID с указателем на дескриптор в $SDS. Также подчеркивается связь атрибута $STANDARD_INFORMATION и файла метаданных $Secure, так как данный атрибут содержит идентификатор безопасности (SID) и именно по этому значению сортируется индекс $SII. При проверке доступа система находит нужный дескриптор безопасности файла с помощью индекса $SII. NTFS читает SID безопасности файла из атрибута $STANDARD_INFORMATION, а затем NTFS использует запись $SII, чтобы найти указатель на дескриптор безопасности объекта в $SDS, который соответствует SID, найденному в атрибуте $STANDARD_INFORMATION. По смещению в атрибуте $SDS система NTFS считывает дескриптор безопасности и завершает проверку безопасности.

В разделе 3 «Техники атак, связанные с аномальным размещением файлов и нарушениями прав доступа в Windows» рассматриваются распространенные техники атак, реализуемые за счет аномального размещения

исполняемых файлов и манипуляций с правами доступа к объектам файловой системы Windows.

В подразделе 3.1 «Слабые права доступа на каталоги приложений и служб» акцент делается на том, что корректная настройка прав на каталоги размещения приложений и служб является одним из важных условий безопасности. Поясняется, что уязвимые конфигурации часто возникают из-за наследования избыточных разрешений от родительских каталогов (например, когда прикладное ПО размещено в корне системного тома либо в созданной подпапке с широкими правами). В таких условиях непривилегированный пользователь может получить техническую возможность модифицировать исполняемые файлы, а их последующий запуск приведет к выполнению подмененного кода, в том числе в контексте привилегированного процесса.

В подразделе 3.2 «Подмена библиотеки динамической компоновки» показано, что одной из характерных форм эксплуатации слабых прав является подмена DLL при загрузке библиотек уязвимым приложением. Отмечается, что риск возникает, когда приложение не указывает абсолютный путь к библиотеке и передает системе только ее имя. В этом случае Windows ищет DLL в определенной последовательности каталогов, и, если какой-либо из них доступен на запись непривилегированному пользователю, появляется возможность разместить подмененную библиотеку с совпадающим именем и добиться выполнения ее кода с привилегиями процесса. В качестве иллюстрации приводится тестовый пример, демонстрирующий практическую эксплуатацию подмены и важность жесткого контроля прав на каталоги приложений.

В подразделе 3.3 «Закрепление в системе с помощью путей автозагрузки» описывается закрепление через механизмы автозапуска. Подчеркивается, что распространенной практикой является размещение объектов для закрепления в пользовательском или общесистемном каталоге автозагрузки. Windows инициирует запуск объектов, размещенных в этих директориях, при входе пользователя в систему, то есть помещение вредоносного исполняемого файла

в соответствующий каталог обеспечивает регулярный запуск без дополнительных механизмов.

В подразделе 3.4 «Закрепление в системе с помощью запланированных задач» раскрывается злоупотребление Планировщиком задач как механизмом устойчивого закрепления. Указывается, что задачи планировщика представлены файлами конфигурации, содержащими сведения о запускаемой команде или файле, условиях срабатывания и учетной записи, от имени которой выполняется задача. Планировщик задач может быть интересен злоумышленнику как для закрепления, так и в сценариях повышения привилегий, например, когда задача запускается от имени привилегированной учетной записи, и путь к исполняемому файлу указывает на объект в каталоге с избыточными правами на запись, что создает возможность его подмены.

В подразделе 3.5 «Маскировка вредоносных программ в файловой системе» рассматривается совокупность приемов сокрытия вредоносных объектов путем имитации легитимной активности и усложнения визуального обнаружения.

В разделе 4 «Формализация правил обнаружения аномалий» на основе рассмотренных техник атак сформулированы правила, нарушение которых интерпретируется как аномалия конфигурации файловой системы.

Правило 1 (Правило владения объектами в профилях пользователей). Если владельцем файла в профиле пользователя (директории вида $C{:}\backslash Users\backslash < user >$ и их подкаталоги) является учетная запись, не относящаяся ни к одной из категорий: сам владелец профиля; встроенная учетная запись администратора (RID 500); служебная системная учетная запись, то такое состояние файловой системы рассматривается как аномальное.

Правило 2 (Правило прав доступа к исполняемым файлам). Если у учетной записи, не относящейся ни к одной из категорий: сам владелец файла; встроенная учетная запись администратора (RID 500); служебная системная учетная запись, на рассматриваемый файл с одним из расширений (exe, dll, ps1,

vbs, bat, cmd, lnk), установлены права записи, такое состояние рассматривается как аномальное.

Правило 3 (Правило прав доступа в системных каталогах приложений и служб). Если для файла или каталога, расположенного в одном из каталогов: $C{:}\backslash Program\ Files$ и $C{:}\backslash Program\ Files\ (x86)$; $C{:}\backslash ProgramData$; $C{:}\backslash Windows\backslash system32$ и $C{:}\backslash Windows\backslash SysWOW64$; $C{:}\backslash Windows\backslash system32\backslash drivers$), обычному пользователю предоставлены права записи, такое состояние рассматривается как аномальное.

Правило 4 (Правило прав доступа для объектов автозагрузки и запланированных задач). Для объектов, связанных с механизмами автозагрузки или выполнением запланированных задач, предлагается считать аномальными следующие состояния:

1) для общесистемного каталога автозагрузки ($\%ProgramData\%\backslash Microsoft\backslash Windows\backslash Start\ Menu\backslash Programs\backslash Startup$) и объектов, связанных с запланированными задачами (каталоги $\%SystemRoot\%\backslash System32\backslash Tasks$, $\%SystemRoot\%\backslash SysWOW64\backslash Tasks$, $\%SystemRoot\%\backslash Tasks$, $\%SystemRoot\%\backslash System32\backslash Tasks\backslash Microsoft\backslash Windows$):

1.1) владельцем объекта является обычный пользователь или обычный пользователь обладает правами записи для данного объекта;

2) для пользовательского каталога автозагрузки ($\%APPDATA\%\backslash Microsoft\backslash Windows\backslash Start\ Menu\backslash Programs\backslash Startup$):

2.1) владельцем объекта является не тот пользователь, к профилю которого относится данный каталог;

2.2) любой другой обычный пользователь (отличный от владельца соответствующего профиля) обладает правами записи или модификации объекта.

Правило 5 (Правило для объектов, у которых неизвестный SID владельца). Файл или каталог рассматривается как аномальный, если в качестве его владельца указан идентификатор безопасности, который не может

быть сопоставлен ни одной существующей в системе учетной записи или группе.

Правило 6 (Правило обнаружения аномального размещения файлов на основе типичных путей). Файл рассматривается как аномально размещенный, если он расположен в каталоге, который для его владельца является статистически нетипичным. Под типичными путями в настоящей работе понимаются те области файловой системы, в которых данный пользователь, как правило, создает и модифицирует файлы: каталог профиля, рабочий стол, стандартные каталоги документов, временные папки и т.п.

В разделе 5 «Программная реализация анализа файловой структуры по идентификаторам пользователей в NTFS» описана реализация GUI-приложения на языке программирования высокого уровня C++. В основе лежит универсальный механизм обхода файловой системы, поверх которого реализованы восемь режимов работы, соответствующих поставленным задачам:

1) формирование списка SID, файлы владельцев которых присутствуют в указанном разделе;

2) формирование списка SID, тех владельцев, чьих файлов нет в указанном разделе;

3) формирование списка файлов с указанным (из сформированного ранее списка) SID владельца;

4) формирование списка файлов, доступных на запись пользователю с указанным SID;

5) формирование списка файлов, доступных на чтение пользователю с указанным SID;

6) формирование списка файлов с пустым ACL и, по запросу пользователя, удаление пустого ACL;

7) формирование статистики типовых путей размещения файлов для каждого пользователя;

8) сканирование системы на предмет возможных аномалий размещения файлов и нарушений прав доступа по заданным правилам.

Во всех режимах результаты сохраняются в CSV-файлы, а ввод и вывод параметров реализован через диалоговые окна. На рисунке 1 представлено основное окно разработанного приложения.

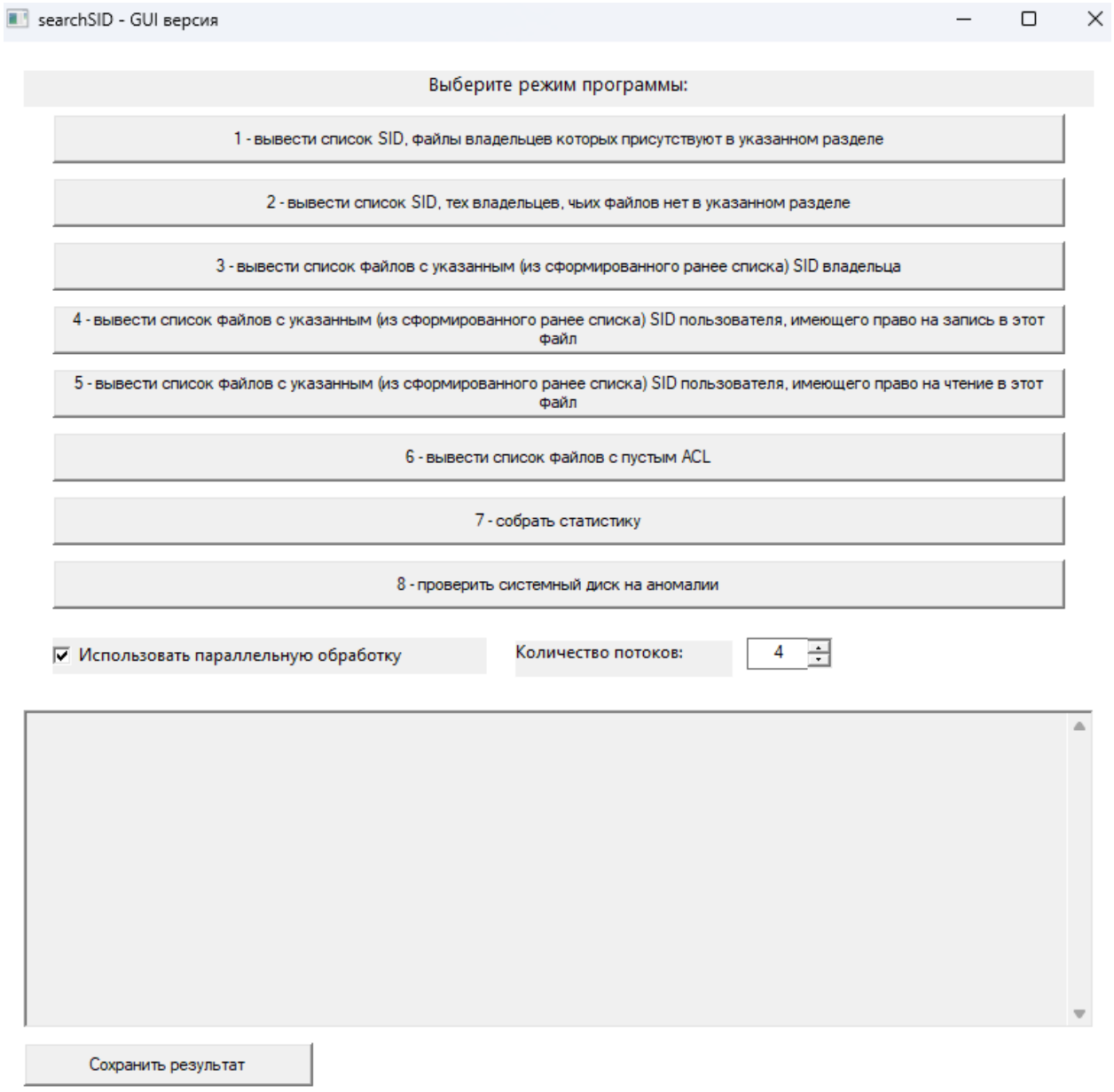

Рисунок 1 – Основное окно приложения

В разделе 6 «Практическая часть» приведены примеры запуска и проверки корректности всех реализованных режимов. Корректность подтверждается сопоставлением с системными данными и контрольными проверками.

ЗАКЛЮЧЕНИЕ

В ходе теоретической части работы были рассмотрены такие темы, как дескриптор безопасности, структура файловой системы NTFS и техники атак, связанные с аномальным размещением файлов и нарушениями прав доступа в Windows.

В ходе практической части был реализован анализ файловой структуры по идентификаторам пользователей в NTFS. Умения, полученные в ходе выполнения практической части являются важным навыком для администраторов компьютерных систем и технических специалистов в области информационной безопасности, так как этот навык позволяет управлять безопасностью компьютерной среды, обнаруживать потенциальные угрозы и предотвращать несанкционированный доступ к информации.

Таким образом, все поставленные задачи решены, цель работы достигнута.