

УДК 004.451.9

Сравнительный анализ обеспечения информационной безопасности в операционных системах Windows и Linux

Илюхин Илья Юрьевич

ilya.ilyukhin12@yandex.ru

КФ МГТУ им. Н.Э. Баумана, Калуга, Россия

Приведен сравнительный анализ обеспечения информационной безопасности в операционных системах. В связи процессом импортозамещения и на основе анализа популярности операционных систем, основное внимание уделяется Windows и Linux. В качестве сравнительных компонентов рассматриваются: модели безопасности обеих операционных систем, процесс идентификации пользователя в системах, списки контроля доступа и модуль аудита безопасности. Предоставлена статистика атак за период 2022–2024 гг., отображающая рост инцидентов как в системе Linux, так и в системах семейства Windows.

Ключевые слова: операционная система, обеспечение безопасности, Windows, Linux, список контроля доступа, аудит безопасности

Статья посвящена сравнению обеспечения защищенности в ОС Windows и Linux. В ней описаны основные элементы выбранных операционных систем.

Под операционной системой или ОС понимают комплекс программ, который необходим для взаимодействия ресурсов компьютера как между собой, так и с пользователем. Прежде всего ОС является интерфейсом для связи аппаратных средств компьютера с установленными на нем приложениями. В состав любой операционной системы входят следующие пять компонентов:

- ядро — основа ОС, контролирующая функционирование приложений и внутренних элементов компьютера, таких как процессор, видеокарта, материнская плата и т. д.;

- модуль команд — элемент, взаимодействующий с пользовательскими командами и гарантирующий их выполнение;

- набор драйверов — совокупность программного обеспечения для правильной работы компьютерных комплектующих и операционной системы;

- GUI — это графический пользовательский интерфейс операционной системы, который отображается пользователю во время работы с компьютером и помогает ему взаимодействовать с ПО.

Среди наиболее популярных операционных систем являются Windows и Linux. Windows — это семейство ОС для персональных компьютеров, разработанное компанией Microsoft. Существует множество версий Windows, каждая из которых имеет свои особенности и функции, покрывающая различные нужды пользователей.

Linux является названием для UNIX-подобных систем, которые функционируют на основе одноименного ядра. В сравнении с Windows, Linux не

имеет единой комплектации, она поставляется в различных наборах дистрибутивов. Каждый отдельный дистрибутив предоставляет ряд решений для различных пользовательских задач.

В связи с ростом количества атак на вышеперечисленные операционные системы, задачи связанные с обеспечением безопасности личных данных и конфиденциальной информации становятся приоритетными для каждого пользователя и предприятия. Только в период с января 2022 по апрель 2024 г. число атак на UNIX-подобные системы выросло в 85 раз, в то время как на ОС семейства Windows это число возросло в 3,8 раза, что связано с резким переходом на отечественные Linux системы [1]. На рис. 1 представлена статистика объектов атак злоумышленников за периоды 2022, 2023 и первый квартал 2024 г. [2].

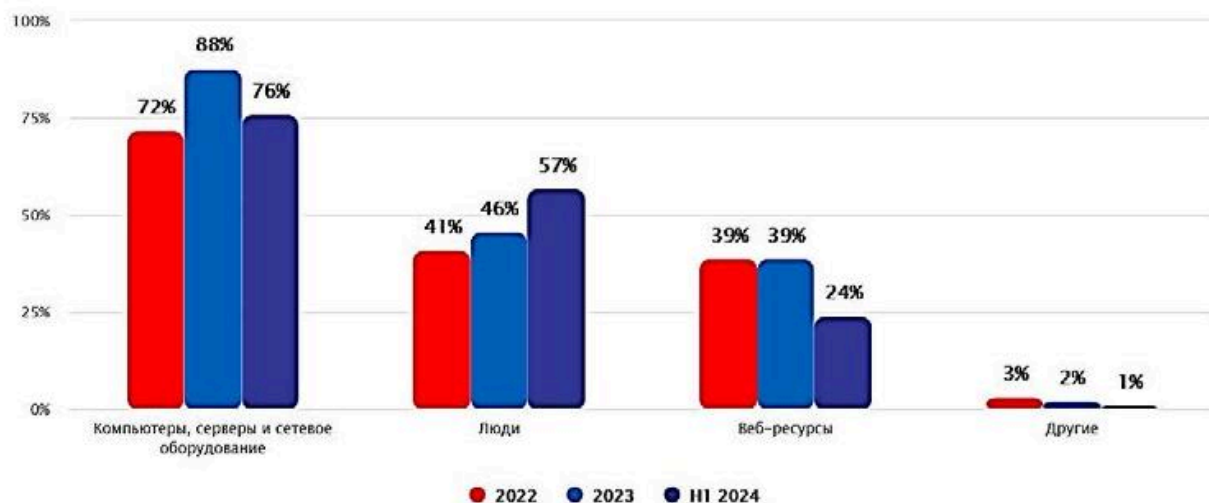


Рис. 1. Статистика объектов атак злоумышленников

Учитывая доминирующее положение Windows и Linux на рынке, для пользователей выбор будет производиться из этих ОС. В связи с этим, актуальной задачей является проведение сравнительного анализа ОС Windows и Linux в сфере обеспечения информационной безопасности.

Для сравнения средств обеспечения защищенности необходимо изучить модель безопасности каждой из представленных ОС.

Модель безопасности. Модель безопасности Windows — это совокупность процессов пользователя и режима ядра, которые контролируют компоненты безопасности ОС. Базовая модель безопасности ОС Windows изображена на рис. 2.

Монитор безопасности — основной элемент модели, выполняющий проверку защищенности и разрешение субъектов на работу с объектами. Также компонент обеспечивает работу с правами пользователей.

Подсистема проверки подлинности локальной системы безопасности. Данный процесс запускает LSASS.exe, который производит проверку подлинности пользователей и обновляет журнал событий сообщениями аудита безопасности. Необходимые настройки и параметры для корректной работы под-

системы находятся в базе данных LSASS, которая хранится в реестре. Также в эту БД входят данные о том, кто может проводить проверку подлинности попыток входа в систему, и какие пользователи имеют доступ к системе.

Администратор учетных данных в системе защиты — это служба, отвечающая за управление базой данных, содержащей имена пользователей и определяет группы на машине.

База данных SAM. Включает в себя информацию о локальных пользователях, описывая их группы, пароли и другие необходимые компоненты. Данная БД не хранит данные о пользователях на контроллерах домена, за исключением учетной записи администратора. Эта база данных хранится в ветке реестра HKLM/SAM.

Пакеты аутентификации содержат DLL файлы, которые включены в процесс LSASS. Данные DLL файлы реализуют политику проверки подлинности, т. е. выполняют аутентификацию пользователей через проверку соответствует ли введенное имя пользователя и пароль, и возвращает процессу LSASS в случае успешной проверки информацию, уточняющую пользовательские привилегии.

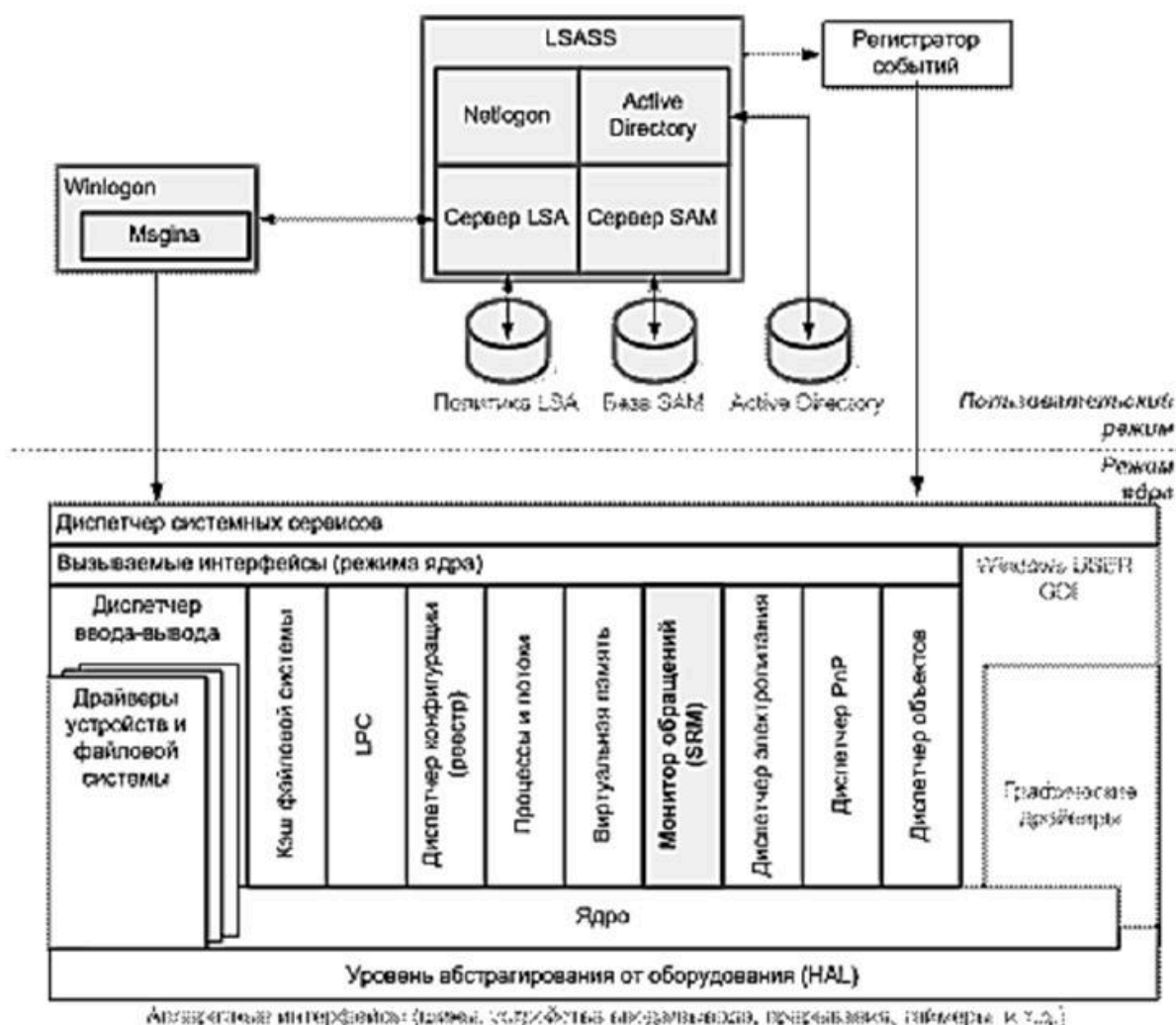


Рис. 2. Модель безопасности Windows

Пользовательский интерфейс входа в систему. Процесс, который отображается перед запуском самой ОС. Он показывает пользователям графический интерфейс, который предоставляет пользователю возможность удобной и понятной авторизации.

Драйвер устройства безопасности ядра. Библиотека функций режима ядра, которые используются для обмена данными с LSASS другими компонентами безопасности режима ядра.

В отличие от Windows, ОС Linux модель безопасности имеет другое представление. Она является совокупностью процессов и служб, организующих защищенную среду для ядра. В ее состав входят такие компоненты, как:

- **подключаемые модули аутентификации** — это набор разделяемых библиотек, используемых для динамической проверки подлинности пользователя в приложениях или в системе. Набор объединяет несколько модулей низкоуровневой аутентификации в высокоуровневый API, который обеспечивает поддержку динамической аутентификации приложений. Схема и настройки аутентификации указываются администратором в директории `/etc/pass` либо в файле `/etc/conf`;

- **управление учетными записями пользователей** является фундаментальным аспектом Linux, который включает в себя создание, изменение и удаление учетных записей пользователей, а также управление привилегиями пользователей и правами доступа;

- **компонент управления паролями** — это модуль, позволяющий взаимодействовать с пользовательскими паролями, т. е. создавать новый пароль, редактировать его и сбрасывать;

- **компонент управления сеансами** — модуль, взаимодействующий с сеансами входа в сеть. Компонент регулирует запуск и завершение пользовательского сеанса и делает необходимые записи в журнал инициализированных сеансов.

Рассмотрев вышеперечисленные компоненты модели безопасности каждой из операционных систем, можно сделать вывод, что ОС имеют различные компоненты, но схожий принцип разделения системы безопасности на отдельные модули делает обе ОС стабильнее и проще.

Идентификация. Вторым компонентом сравнительного анализа является идентификация, под которой понимается процесс проверки личности пользователя в системе. Рассматривая идентификацию в рамках ОС Windows, необходимо знать, что идентификатором здесь является значение непостоянной длины, которое определяет пользователя системы безопасности и хранится в `HKLM\Security`.

Идентификатор или SID — Security Identifier всегда начинается на букву S и представлен в следующем формате [3]:

S-1-5-21-7623811015-3361044348-030300820-1013

SID имеет следующую структуру:

- строка SID;
- версия спецификации SID;

- идентификатор прав доступа — показывает, кто создал эту сторону;
- идентификатор домена;
- относительный идентификатор RID — указывает на то, сколько SID уже есть в системе.

В Linux распознавание пользователя осуществляется по имени пользователя во время авторизации, далее имя пользователя сопоставляется с идентификационным номером (UID), которое либо автоматически, либо при помощи администратора присваивается пользователю. Данная пара имя_пользователя: UID находится в файле `/etc/passwd` [4]. Также любая группа сопоставляется со своим GID — Group Identifier.

Несмотря на то, что идентификаторы имеют разное представление в системе и хранятся они в разных местах, сам процесс распознавания пользователя одинаков.

Список контроля доступа. Третьим компонентом для сравнительного анализа будет рассматриваться список контроля доступа или же СКД. Под СКД понимают совокупность правил, контролирующих, возможность субъекта, будь то пользователь или система, получить разрешение на взаимодействие с необходимыми ресурсами и проверяющих, каким уровнем обладает это разрешение.

В структуре СКД систем Microsoft Windows, можно выделить два типа СКД: DACL и SACL. Основной частью каждой СКД являются записи управления доступом — ACE, хранящие в себе информацию о наличии разрешения у субъекта на работу с выбранным объектом. ACE состоит из четырех параметров:

- SID, который определяет доверенное лицо;
- маска доступа, определяющая какой доступ есть у доверенного лица;
- флаг, обозначающий тип ACE;
- битовые флаги, может ли дочерний объект наследовать ACE от первичного.

В DACL, дискреционном СКД, выделяется 4 типа записей управления доступом: есть доступ, доступ отсутствует, объект разрешен, объект запрещен. Первые два типа определяют имеет ли субъект возможность взаимодействовать с объектом или нет, два других же определяют может ли объект существовать или не может.

SACL, системный СКД, содержит в себе 2 типа ACE: записи системного аудита и записи объекта системного аудита. В данном случае ACE определяют выполняемые операции субъектами над объектами и проверяют, могут ли данные субъекты пользоваться выбранными операциями. Любая попытка выполнения операции, успешная или, наоборот, неудачная, записывается в журнал аудита.

В современных дистрибутивах Linux хоть и присутствует СКД, контроль доступа, в основном, обеспечивается через файловую систему. Это связано с тем, что настройка СКД проблематична и несет за собой ряд проблем, таких как низкая производительность файловой системы и некорректная работа

с программами, не поддерживающими СКД. Также следует отметить, что СКД становятся тяжело управляемыми из-за большого количества записей.

Говоря о контроле доступа через файловую систему необходимо знать, что он собой представляет. Данный контроль означает, что при работе с файлами и директориями файловая система использует определенные атрибуты. Они регулируют уровень и возможность взаимодействия пользователя и группы с необходимыми ресурсами. К таким атрибутам можно отнести имя файла, биты доступа, идентификатор пользователя и идентификатор группы, изображенные на рис. 3.

```

mial@HackWare:~/test
[File  Правка  Вид  Поиск  Терминал  Справка]
[mial@HackWare test]$ ls -l
итого 32760
-rw-rw-r-- 1 mial users 262144 авг 18 15:04 custom-x.cramfs.img
-rw-r--r-- 1 mial users 3466800 авг 31 11:15 data
-rw-r--r-- 1 mial users 1376192 авг 31 11:15 data.lzma
-rw-r--r-- 1 mial users 6205991 авг 31 14:06 filesystem.squashfs
drwxr-xr-x 3 mial users 4096 авг 31 11:45 filesystem.squashfs.extracted
-rw-r--r-- 1 mial users 6784000 авг 18 15:16 General_IPC_XM530_R80X20-PQ_WIFI_XM711.711.Nat.dss.Onvifs_V5.00.R02.20210818_all.zip
-rw-rw-r-- 1 mial users 758 авг 18 15:04 InstallDesc
-rw-r--r-- 1 mial users 7602236 окт 19 2017 'Keenetic-II-V2.06(AAFG.0)C3.bin'
-rw-rw-r-- 1 mial users 1310720 авг 18 15:04 romfs-x.cramfs.img
-rw-rw-r-- 1 mial users 194560 авг 18 15:04 u-boot.bin.img
-rw-rw-r-- 1 mial users 65600 авг 18 15:04 u-boot.env.img
-rw-r--r-- 1 mial users 64 авг 31 11:02 uImage-header.bin
-rw-rw-r-- 1 mial users 1572864 авг 18 15:04 uImage.img
-rw-r--r-- 1 mial users 3621 авг 31 14:06 unsquashfs_all.sh
-rw-rw-r-- 1 mial users 4653056 авг 18 15:04 user-x.cramfs.img
[mial@HackWare test]$

```

Рис. 3. Атрибуты файлов

Нельзя не упомянуть СКД в Linux, хотя он и редко используется. В данной ОС выделяется два типа СКД: DAC, означающий, что пользователь сам выбирает у кого есть разрешение на работу с выбранным объектом, и MAC, где разрешения определяются в политике доступа.

В обеих ОС реализован процесс предоставления доступа для работы с ресурсами. Если в Windows это реализовано через полноценные СКД, то Linux определяет привилегии через атрибуты файлов, однако в редких случаях тоже используется СКД.

Аудит безопасности. Четвертым элементом обеспечения ИБ является аудит. Аудит — это процесс, определения состояния системы после проверки безопасности. Отчеты проведенного аудита показывают какой пользователь, когда и при каких условиях обращался к определенным ресурсам.

Аудит в ОС Windows может проводится двумя способами: вручную и автоматизировав этот процесс. Ручной аудит подразумевает сканирование си-

стемы без автоматизированных команд, обычный опрос персонала и проверка физического доступа к системе [5]. Иной подход позволяет выполнять вышеперечисленные действия при помощи подходящих программ, таких как локальная политика безопасности, интерфейс которой изображен на рис. 4.

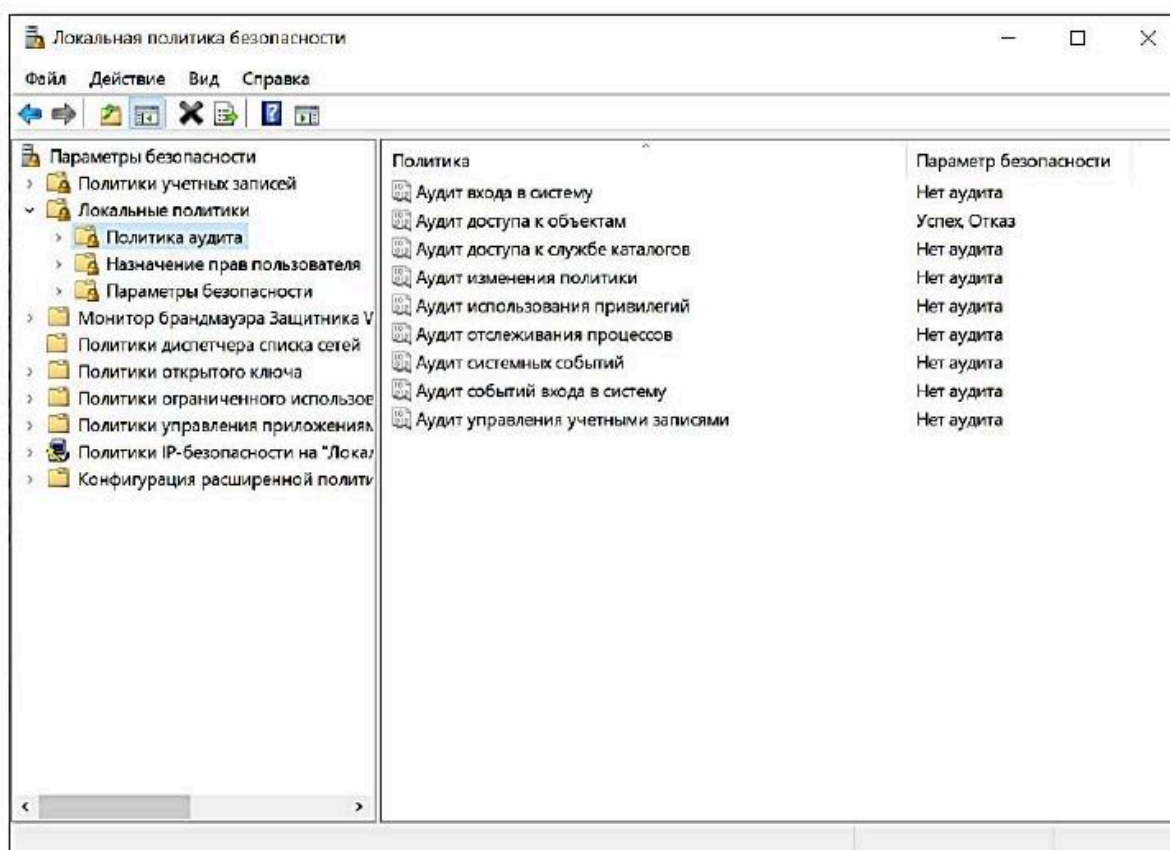


Рис. 4. Интерфейс локальной политики безопасности

В Windows аудит безопасности можно провести на следующих событиях:

- вход в учетную запись, проверка входа и выхода пользователя системы;
- доступ к объекту, т. е. анализ наличия разрешения у субъекта на взаимодействие с объектом;
- изменение политики аудита, т. е. анализ любых изменений в политиках аудита;
- учетные записи, т. е. проверка изменения данных учетных записей.

В Linux аудит состоит из компонентов, один из которых находится в ядре — `kauditd`, второй в пользовательском пространстве — `auditd` (рис. 5) [6].

Процесс аудита безопасности выполняется следующим образом. Пользовательские приложения отправляют вызов `syscall` в компонент ядра `Kauditd`. В ядре осуществляется проверка, какому из модулей соответствует приложение пользовательского пространства, к которым относятся:

- `User` — события, связанные с пользователем;
- `Task` — события, связанные с системными процессами;
- `Exclude` — события, которые не относятся к аудиту;

- Filesystem — события, связанные с изменениями в файловой системе;
- Exit — события завершения процессов.

Далее через протокол взаимодействия между пользователем и ядром — netlink, информация о событиях передается в фоновый процесс Auditd, который записывает зафиксированные действия в журнал событий аудита.

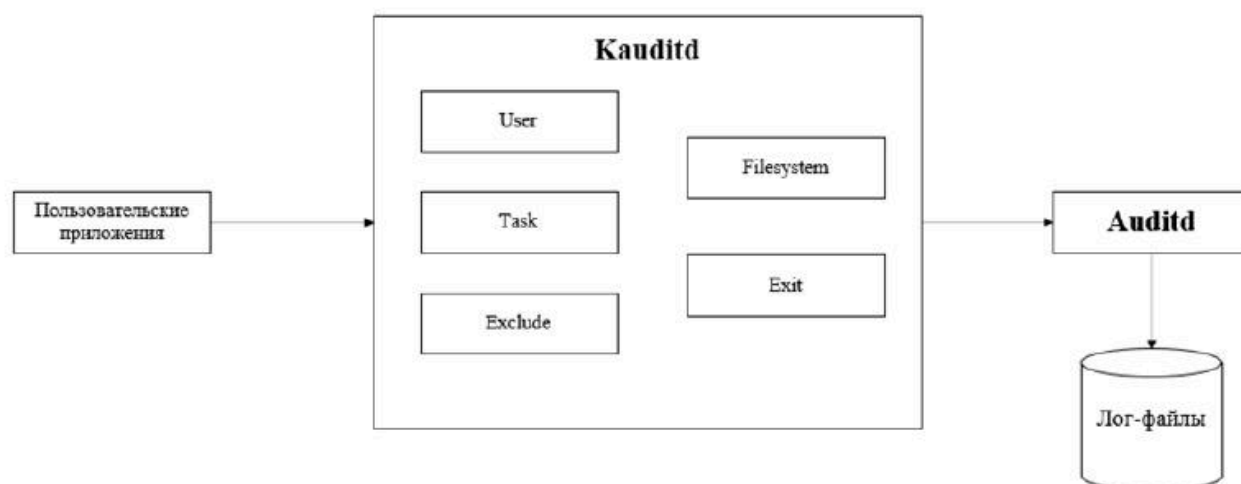


Рис. 5. Система аудита в ОС Linux

Следует отметить, что основным отличием в аудите безопасности данных ОС является то, что любое событие в Linux проходит через аудит в пространстве ядра, в отличие от ОС семейства Windows.

Заключение. В ходе проведенного анализа были рассмотрены основные компоненты обеспечения информационной безопасности в ОС Windows и Linux. Обе ОС имеют схожие механизмы обеспечения безопасности, однако методы реализации отличаются. Принципиальным отличием является то, что Windows включает свои средства в работу ядра, в то время как Linux использует пользовательские процессы. При этом каждая из операционных систем адекватно защищает данные, но выбор ОС зависит от конкретных задач пользователя или предприятия.

Литература

- [1] Число атак на российские Linux выросло в 85 раз. URL: https://www.cnews.ru/news/top/2024-08-30_populyarnost_novyh_rossijskih (дата обращения 31.10.2024).
- [2] Киберугрозы в государственном секторе. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/kiberugrozy-v-gosudarstvennom-sektore/#id1> (дата обращения 01.11.2024).
- [3] Идентификаторы безопасности SID. URL: https://sysadminium.ru/kak_ustroen_windows-sid/ (дата обращения 04.11.2024).
- [4] Идентификация и аутентификация пользователей при работе подсистемы разграничения доступа в ОС Linux. URL: https://www.okbsapr.ru/library/publications/kanner_2012_3/?ysclid=m2wcoekupg933727777 (дата обращения 04.11.2024).

- [5] What is Security Audit for Windows? URL: <https://www.geeksforgeeks.org/what-is-security-audit-for-windows/> (дата обращения 02.11.2024).
- [6] Основы аудита. Настраиваем журналирование важных событий в Linux. URL: <https://xakep.ru/2021/09/16/linux-audit/> (дата обращения 02.11.2024).

Comparative analysis of information security in Windows and Linux operating systems

Ilyukhin I.Y. ilya.ilyukhin12@yandex.ru

BMSTU (KB), Kaluga, Russia

This work provides a comparative analysis of information security in operating systems. Due to the import substitution process and based on the analysis of the popularity of operating systems, the focus is on Windows and Linux. The following comparative components are considered: security models of both operating systems, the process of user identification in systems, access control lists and the security audit module. Attack statistics for the period 2022–2024 are presented, reflecting the growth of incidents in both Linux and Windows systems.

Keywords: operating system, security, Windows, Linux, access control list, security audit