ТЕХНИЧЕСКИЕ НАУКИ

ОПЕРАЦИОННАЯ СИСТЕМА SECUX LINUX С СИСТЕМОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ KIRTAPP

Колбанов Г.П.[1], Романов Д.А.[2], Белоусова Е.С.[3]

[1]Колбанов Григорий Павлович – учащийся
[2]Романов Дмитрий Алексеевич – учащийся
направления «Информационная безопасность»
УО «Национальный детский технопарк»
г. Минск
[3]Белоусова Елена Сергеевна – кандидат технических наук, доцент
кафедра защиты информации,
Белорусский государственный университет информатики и радиоэлектроники,
г. Гомель, Республика Беларусь

Аннотация: *в условиях растущих киберугроз и зависимости от зарубежных технологий разработка отечественных защищённых операционных систем становится приоритетной задачей. В статье представлена операционная система Secux Linux – инновационный дистрибутив, ориентированный на критически важные объекты информатизации (КВОИ), частные компании и обычных пользователей. Операционная система реализует безопасную схему загрузки с использованием TPM, Secure Boot и Unified Kernel Image, обеспечивая аппаратный корень доверия (Root of Trust). Для защиты данных применяются технологии шифрования, биометрическая аутентификация и мандатное управление доступом.*
Ключевые слова: *кибербезопасность, защищённая операционная система, TPM, Secure Boot, Unified Kernel Image, шифрование, биометрическая аутентификация.*

SECUX LINUX OPERATING SYSTEM WITH KIRTAPP BIOMETRIC AUTHENTICATION SYSTEM

Kolbanov G.P.[1], Romanov D.A.[2], Belousova E.S.[3]

[1]Kolbanov Grigory Pavlovich – student
[2]Romanov Dmitry Alekseevich – student
DIRECTION "INFORMATION SECURITY"
UO "NATIONAL CHILDREN'S TECHNOPARK",
MINSK
[3]Belousova Elena Sergeevna – candidate of technical sciences, associate professor
DEPARTMENT OF INFORMATION SECURITY BSUIR,
BELARUSIAN STATE UNIVERSITY OF INFORMATICS AND RADIOELECTRONICS
GOMEL, REPUBLIC OF BELARUS

Abstract: *in the context of growing cyber threats and dependence on foreign technologies, the development of domestic secure operating systems is becoming a priority task. The article presents the Secux Linux operating system - an innovative distribution aimed at critically important information technology objects, private companies and ordinary users. The operating system implements a secure boot scheme using TPM, Secure Boot and Unified Kernel Image, providing a hardware root of trust (Root of Trust). Encryption technologies, biometric authentication and mandatory access control are used to protect data.*
Keywords: *cybersecurity, secure operating system, TPM, Secure Boot, Unified Kernel Image, encryption, biometric authentication.*

УДК 004.056.5

В условиях цифровизации кибербезопасность становится ключевой задачей государственной политики. Критически важные объекты информатизации (КВОИ) [1] Беларуси зависят от надежности своей инфраструктуры, поэтому использование защищенных операционных систем необходимо для противодействия кибератакам и несанкционированному доступу.

Современные операционные системы (ОС), применяемые в госструктурах, нередко уязвимы и зависимы от зарубежных поставщиков. В условиях растущих киберугроз и санкций важно создавать отечественные решения, обеспечивающие безопасность и независимость. В приказе №66 Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 года установлено требование к КВОИ, по которому наша ОС подходит по пункту «обеспечение конфиденциальности и контроля целостности информации при ее хранении в информационной системе (средства предварительного шифрования)» для всех классов типовых информационных систем.

Существующие операционные системы, в том числе Astra Linux, могут содержать потенциальные уязвимости, которые делают их неподходящими для использования на критически важных объектах. Одним из ключевых недостатков является отсутствие проверки целостности на каждом этапе загрузки системы.

Кроме того, в большинстве существующих дистрибутивов Linux не используется модуль TPM (Trusted Platform Module) [2], что приводит к отсутствию аппаратного корня доверия. Это делает невозможным надежную проверку целостности системы и повышает риск компрометации на этапе загрузки. Использование TPM позволяет реализовать безопасную загрузку (Secure Boot [3]) и обеспечить защиту критически важных данных от кибератак нарушитей, обеспечивая аппаратный корень доверия (Root of Trust). Он выступает в роли доверенного хранилища криптографических ключей и выполняет контроль целостности загружаемых компонентов, предотвращая их подмену или модификацию злоумышленниками.

Особенно уязвимым является этап загрузки initramfs, который представляет собой промежуточную среду для монтирования корневой файловой системы и запуска системы. Поскольку initramfs не проверяется на подлинность в большинстве дистрибутивов Linux, нарушители могут внедрить вредоносный код, который будет выполнен до полной загрузки операционной системы, предоставляя доступ к конфиденциальной информации или возможность дальнейших кибератак (например перехват ключей шифрования диска, зашифрованного LUKS).

На основе вышесказанного становиться понятно, что для совершенствования системы информационной безопасности КВОИ и частных компаний требуется использование защищённых операционных систем с возможность шифрования диска, безопасной загрузки и двухфакторной аутентификации пользователя на основе его биометрических данных.

Целью данной работы являлось разработка ОС Secux Linux на основе ядра Arch Linux с функциями безопасной загрузки (Secure Boot), шифрования диска и биометрической аутентификацией и контроля пользователя.

В качестве основы было выбрано ядро Arch Linux благодаря его гибкости, rolling-модели обновлений и поддержке современных технологий. В качестве ядра в ОС Secux Linux используется linux-hardened (по умолчанию) с возможностью переключения на linux-lts и linux.

В рамках разработки Secux Linux была реализована безопасная схема загрузки, направленная на повышение надежности и защиты от кибератак на этапе инициализации системы. Основной акцент был сделан на усилении безопасности загрузочного процесса, выявленных уязвимостей, таких как возможность атак на initramfs и недостаточной проверки целостности на ранних стадиях загрузки.

ОС Secux Linux реализует проверку каждого этапа загрузки посредством:

– использование собственных ключей Secure Boot. Если устройство не поддерживает использование собственных ключей Secure Boot, для обратной совместимости присутствует возможность использования загрузчика shim, подписанного Microsoft;

– использование загрузчика systemd-boot вместо Grand Unified Bootloader (GRUB);
– использование подписанного Unified Kernel Image (UKI);
– использование Linux Unified Key Setup (LUKS) для шифрования раздела;
– использование TPM для проверки целостности компонентов системы вместе с политикой подписи PCR.

Для упрощения установки и настройки ОС Secux Linux был разработан интуитивно понятный установщик – Secux Linux Installer. Он позволяет установить систему в соответствии с различными потребностями пользователя.

На рисунке 1 представлена графическая оболочка ОС Secux Linux с запущенной программой Security Manager, системой биометрической аутентификации KIRTapp и успешным результатом шифрования диска.

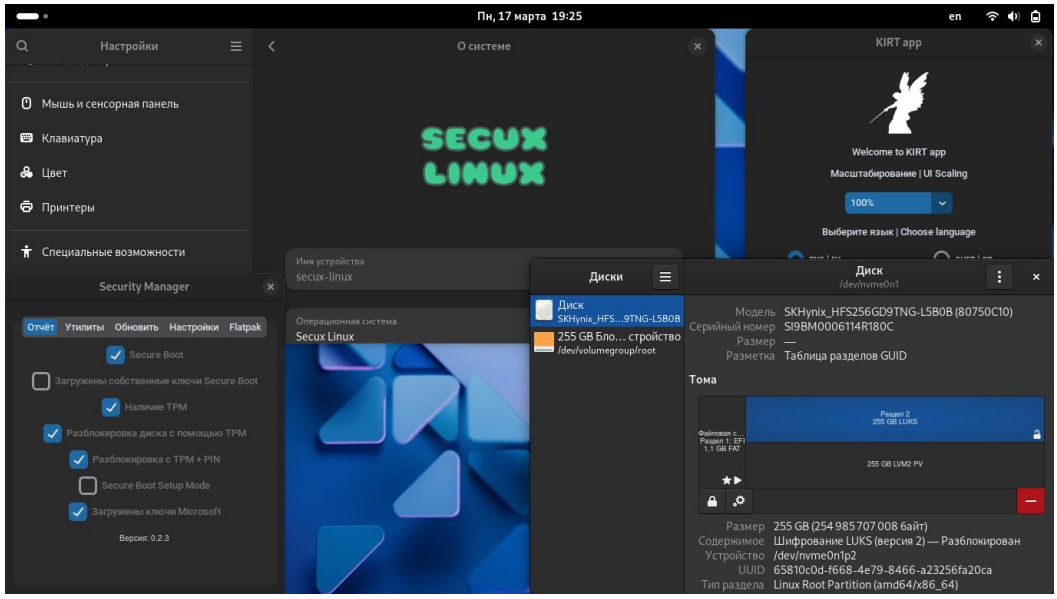

Рис. 1. Графическая оболочка ОС Secux Linux.

Security Manager отображает детальную информацию о состоянии безопасности системы и позволяет настроить авторазблокировку через TPM (с возможностью добавления PIN-кода по желанию), а также регулировать использование проверки PCR и политики их подписи. Кроме того Security Manager предоставляет возможность регистрации ключа восстановления и дополнительного пароля, а при необходимости – отключение этих функций.

В Secux Linux внедрена система биометрической аутентификации KIRTapp, которая проверяет лицо пользователя в фоновом режиме. Приложение имеет два режима работы: локальный и корпоративный. Локальный режим работы не требует использования стороннего сервера и сохраняет результаты аутентификации пользователя в лог-файлах локального устройства. Корпоративный режим работы требует наличия стороннего сервера, в базе данных (БД) которого будут сохраняться имена всех пользователей ОС в корпоративной сети и результаты их аутентификации во время работы (рисунок 2). Таким образом, в корпоративном режиме администратор может осуществлять удаленный мониторинг событий информационной безопасности и осуществлять контроль за пользователями.

```
f=# select * from users
;
 id |  username  |   name   | lastname |   post    |         email          | phone_number | status |     last_check
----+------------+----------+----------+-----------+------------------------+--------------+--------+---------------------
  1 | aivanov    | Aleksey  | IVANOV   | Manager   | aivanov@example.com    | +79031234567 | reg    | 2025-02-22 10:00:00
  2 | vpetrov    | Vladimir | PETROV   | Developer | vpetrov@example.com    | +79161234567 | reg    | 2025-02-21 14:30:00
  3 | spopov     | Sergey   | POPOV    | Designer  | spopov@example.com     | +79261234567 | reg    | 2025-02-20 08:15:00
  4 | nsidorov   | Nikolay  | SIDOROV  | Analyst   | nsidorov@example.com   | +79371234567 | reg    | 2025-02-19 17:45:00
  5 | dsmirnov   | Dmitry   | SMIRNOV  | Support   | dsmirnov@example.com   | +79451234567 | reg    | 2025-02-18 09:10:00
  6 | ekuznetsov | Evgeny   | KUZNETSOV| HR        | ekuznetsov@example.com | +79551234567 | reg    | 2025-02-17 12:05:00
  7 | fmorozov   | Fedor    | MOROZOV  | CEO       | fmorozov@example.com   | +79661234567 | reg    | 2025-02-16 16:20:00
  8 | gbelov     | Gennady  | BELOV    | Intern    | gbelov@example.com     | +79771234567 | reg    | 2025-02-15 11:30:00
  9 | hkotov     | Herman   | KOTOV    | Engineer  | hkotov@example.com     | +79881234567 | reg    | 2025-02-14 07:45:00
 10 | ilebedev   | Igor     | LEBEDEV  | Marketer  | ilebedev@example.com   | +79991234567 | reg    | 2025-02-13 15:55:00
(10 rows)

f=#
```

Рис. 2. Пример БД системы аутентификации KIRTapp.

В KIRTapp имеется фоновая служба, которая по умолчанию каждые 5 минут проводит повторную аутентификацию пользователя и фиксирует ее результат в лог-файлах локального устройства (локальный режим) или в БД (корпоративный режим). Если камера выключена, не доступна или пользователя нет за устройством фоновая служба системы аутентификации KIRTapp добавит в лог-файл сообщение о ошибке распознавания лицо пользователя и осуществит принудительный выход пользователя из системы (рисунок 3).

```
  GNU nano 8.3
2025-03-14 20:46:30 - INFO - The checking was successful
2025-03-14 20:51:43 - INFO - The checking was successful
2025-03-14 20:57:03 - INFO - The checking was failed
2025-03-14 21:02:33 - INFO - The checking was failed
2025-03-14 21:07:40 - INFO - The checking was failed
2025-03-14 21:13:03 - INFO - The checking was failed
2025-03-17 19:09:46 - INFO - The checking was successful
```

Рис. 3. Содержимое лог-файла в случае невозможности распознавания пользователя.

Дополнительными преимуществами ОС Secux Linux является возможность использования следующих систем:

1 Uncomplicated Firewall (UFW), который по умолчанию блокирует все входящие соединения.

2 AppArmor, который помогает предотвратить несанкционированный доступ к системным ресурсам, файлам и данным, обеспечивая строгую политику безопасности и уменьшая вероятность эксплуатации уязвимостей в приложениях.

3 Wayland, который предотвращает перехват ввода и вывод видео из других приложений.

4 Flatpak [4], которая позволяет запускать приложения в контейнерах с ограниченными правами доступа.

При попытке компрометации ОС Secux Linux появится предупреждение и процесс загрузки будет прерван. Результат при загрузке с включенным Secure Boot показан на рисунке 4. Результат при загрузке с выключенным Secure Boot или скомпрометированной прошивкой показан на рисунке 5.

```
Error loading \EFI\Linux\arch-linux.efi: Access denied
```

Рис. 4. Результат при загрузке с включенным Secure Boot.

Рис. 5. Результат при загрузке с выключенными Secure Boot или скомпрометированной прошивкой.

Системные требования для установки и работы операционной системы Secux Linux:
– оперативная память: 2 GB (рекомендуется 8 GB);
– процессор: одноядерный (рекомендуется четырехядерный);
– свободное дисковое пространство: 10 GB (рекомендуется 64 GB);
– поддержка UEFI;
– наличие TPM 2.0.

Таким образом, в статье было показано, что Secux Linux – это защищённая операционная система, разработанная в соответствии с требованиями нормативно-правовых актов Республики Беларусь к КВОИ. Данная операционная система рекомендуется для использования как в государственных и корпоративных структурах, так и для личного использования. Благодаря своей архитектуре и внедрённым технологиям защиты Secux Linux обеспечивает повышенный уровень безопасности процесса загрузки операционной системы, дискового пространства устройства и аутентификации пользователя.

Список литературы / References

1. Информационно-поисковая система (ИПС) «ЭТАЛОН-ONLINE» // ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ 20 февраля 2020 г. № 66 [Электронный ресурс]. URL: https://etalonline.by/document/?regnum=T62004470 (Дата обращения: 17.03.2025). (Дата обращения: 17.03.2025).
2. Документация Microsoft // Обзор TPM [Электронный ресурс]. URL: https://learn.microsoft.com/ru-ru/windows/security/hardware-security/tpm/switch-pcr-banks-on-tpm-2-0-devices (Дата обращения: 17.03.2025).
3. Документация Microsoft // Secure Boot [Электронный ресурс]. URL: https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot (Дата обращения: 17.03.2025).
4. Flatpak // О нас [Электронный ресурс]. URL: https://flatpak.org/about/ (Дата обращения: 17.03.2025).