УДК 004.056

Савелиев Я.И.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

Научный руководитель:
Пугин В.В.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

ОПЫТ ВНЕДРЕНИЯ РЕД ОС В ПГУТИ, ПОДХОДИТ ЛИ ОН ДЛЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?

Аннотация. В данной статье представлены различные методы защиты информации, реализованные в операционной системе РЕД ОС. Предлагаются вариации использования данной операционной системы и приводятся реальные примеры работы с РЕД ОС в учебном заведении

Ключевые слова: РЕД софт, информационная безопасность, отечественное ПО, РЕД ОС, Иинформационная безопасность вуза.

Современные информационные системы требуют надежных механизмов защиты. Операционная система РЕД ОС, разработанная компанией «РЕД СОФТ», предлагает широкий спектр инструментов и технологий. РЕД ОС – это российская операционная система общего назначения на

основе ядра Linux. Она предназначена для использования на серверах и рабочих станциях в различных организациях, включая государственные учреждения и коммерческие предприятия. В 2022 г. в целях реализации политики импортозамещения руководство Поволжского Государственного Университета Телекоммуникаций и Информатики (ПГУТИ) приняло решение о переводе ИТ-инфраструктуры вуза на российскую операционную систему. Проект также был нацелен на повышение опыта использования студентами и преподавательским составом вуза отечественного софта, а также его интегрирование в образовательный процесс [1]. Система имеет современные механизмы защиты информации, вот некоторые из них:

Принудительный контроль доступа: внедрение системы принудительного контроля доступа (SELinux) в операционной системе РЕД ОС в ВУЗе обеспечивает усиленную безопасность путем ограничения действий пользователей и программ в системе. SELinux реализует концепцию обязательного контроля доступа (MAC), где доступ к ресурсам системы регулируется на основе заранее определенных политик безопасности, что предотвращает несанкционированный доступ и минимизирует риски от уязвимостей в программном обеспечении [2]. Это особенно важно в образовательных учреждениях, где обрабатываются персональные данные студентов и сотрудников, а также проводятся экзамены и тестирования, требующие строгого контроля доступа к ресурсам.

Система изолированного запуска приложений: в рамках этой системы применяется Firejail – инструмент для изолированного запуска приложений, который ограничивает доступ программ к системным ресурсам, повышая безопасность и предотвращая потенциальные угрозы. Кроме того, используются технологии Flatpak и Snap, обеспечивающие создание изолированных сред для приложений, что способствует безопасному и контролируемому запуску программного обеспечения. Эти меры направлены на защиту данных и ресурсов университета, обеспечивая безопасную эффективную работу пользователей.

Flatpak и Snap предоставляют из себя системы для упаковки и распространения приложений в изолированных контейнерах. Они позволяют устанавливать и запускать приложения вместе со всеми необходимыми зависимостями, обеспечивая их работу независимо от основной системы. Это упрощает установку программ и повышает их безопасность.

Аудит: в РЕД ОС реализована система аудита, обеспечивающая мониторинг и регистрацию событий, связанных с безопасностью системы. В рамках этой системы используются различные механизмы, направленные на мониторинг и анализ событий [3]. В ПГУТИ аудит используется для защиты интеллектуальной собственности, предотвращения утечек конфиденциальной информации и обеспечения соответствия внутренним и внешним требованиям безопасности.

Контроль целостности системы: в ВУЗе контроль целостности системы может быть использован для защиты данных и обеспечения безопасности ИТ-инфраструктуры. Этот механизм позволяет отслеживать изменения в файловой системе и предотвратить несанкционированное изменение важных данных, таких как учебные материалы, отчеты, и личная информация студентов и сотрудников. Используя инструменты контроля, вуз может оперативно выявлять любые изменения в системе, что помогает вовремя обнаружить потенциальные угрозы или попытки несанкционированного доступа.

Организация доменной структуры: в университете использование доменной структуры РЕД ОС позволяет эффективно управлять учетными записями пользователей и контролировать доступ к различным сервисам. С помощью интеграции с решениями на базе FreeIPA и Samba DC [4], учебные заведения могут централизованно администрировать систему, отслеживать действия пользователей и обеспечивать единую авторизацию

Интеграция с криптографическими средствами: в ПГУТИ система РЕД ОС также используется для защиты данных с помощью отечественных криптографических средств, таких как КриптоПро CSP и VipNet CSP. Эти средства позволяют накладывать электронные подписи, шифровать и расшифровывать документы в соответствии с российскими стандартами безопасности, что необходимо для защиты конфиденциальной информации студентов и сотрудников [5]. Поддержка защищенных веб-соединений и совместимость с аппаратными средствами расширяют возможности защиты данных и обеспечивают безопасный доступ к государственным и корпоративным ресурсам.

Защищенный комплекс программ электронной почты: использование почтового клиента Evolution, встроенного в РЕД ОС, позволяет обезопасить переписку с помощью протоколов SSL, TLS и STARTTLS [3]. Шифрование с использованием GPG и S/MIME гарантирует защиту содержимого сообщений от несанкционированного доступа, что особенно важно при передаче научных данных, результатов экзаменов и других конфиденциальных материалов.

РЕД ОС остается актуальным решением в сфере информационной безопасности. Система сертифицирована ФСТЭК (Федеральная служба по техническому и экспортному контролю), что особенно важно для ВУЗов Минцфры, к которым и относится ПГУТИ [6]. Система оснащена современными криптографическими средствами и поддерживает отечественные стандарты защиты, что позволяет строить надежные информационные системы в условиях постоянного роста киберугроз.

Благодаря базе на Linux, РЕД ОС отличается гибкостью и надежностью, что облегчает ее интеграцию с другими решениями в области ИБ. Практический опыт эксплуатации в ПГУТИ показывает, что система успешно адаптируется под различные задачи, обеспечивая комплексную за-

щиту данных. Это делает отечественную ОС конкурентоспособным инструментом для создания эффективных и безопасных информационных систем.

Список использованных источников:

1. РЕД софт: сайт. URL: https://redos.red-soft.ru/about/news/novosti/pguti-rabotaet-na-red-os/ (дата обращения 22.04.2025).

2. Вермейлен С. Администрирование системы защиты SELinux. М.: ДМК Пресс, 2020.

3. База знаний РЕД ОС: сайт. URL: https://redos.red-soft.ru/base/ (дата обращения: 22.04.2025).

4. Samba.руководство системного администратора 2001 СПб: Электрон. библиотека. URL: https://clck.ru/3LbMqq (дата обращения 22.04.2025).

5. КриптоПро руководство: документ. URL: https://clck.ru/3LbN7A (дата обращения 22.04.2025).

6. Презентация РЕД СОФТ: документ. URL: https://clck.ru/3LbaTU (дата обращения 22.04.2025).

Saveliev Y.I.
Volga Region State University of
Telecommunications and Informatics, Samara

Scientific supervisor:
Pugin V.V.
Volga Region State University of
Telecommunications and Informatics, Samara

THE EXPERIENCE OF IMPLEMENTING RED OS IN PSUTI, IS IT SUITABLE FOR SOLVING INFORMATION SECURITY PROBLEMS?

Abstract. This article presents various information protection methods implemented in the RED OS operating system. Variations of the use of this operating system are proposed and real examples of working with the operating system in an educational institution are given.

Keywords: RED soft, Information security, domestic software, RED OS, Information security of the university.