УДК 004.056:378.016

АДАПТАЦИЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОД ТРЕБОВАНИЯ СТЕКА ОТЕЧЕСТВЕННЫХ ОС (НА ПРИМЕРЕ ASTRA LINUX)

А.И. Бердник

ООО «Альпиндустрия», г. Минск, Республика Беларусь

Аннотация. Переход государственных структур на доверенные программные решения, включая Astra Linux Special Edition, требует пересмотра подходов к обучению специалистов по информационной безопасности. В работе проанализированы противоречия между актуальными запросами работодателей и содержанием классических образовательных программ. Рассмотрены ключевые архитектурные особенности отечественной платформы, в частности механизмы мандатного управления доступом на базе встроенной подсистемы PARSEC. Предложены практические пути трансформации лабораторных практикумов для эффективного формирования профильных компетенций и сокращения периода адаптации молодых специалистов.

Ключевые слова: импортозамещение; Astra Linux; образовательные программы; информационная безопасность; мандатное управление доступом; компетентностный разрыв; подсистема PARSEC; технологический суверенитет; лабораторный практикум; подготовка кадров.

ADAPTATION OF INFORMATION SECURITY EDUCATIONAL PROGRAMS TO THE REQUIREMENTS OF DOMESTIC OS STACK (ON THE EXAMPLE OF ASTRA LINUX)

A.I. Berdnik

Alpindustria LLC, Minsk, Republic of Belarus

Abstract. The transition of state structures to trusted software solutions, including Astra Linux Special Edition, requires a revision of approaches to training information security specialists. The paper analyzes the contradictions between the current needs of employers and the content of classical educational programs. The key architectural features of the domestic platform are considered, in particular, the mandatory access control mechanisms based on the built-in PARSEC subsystem. Practical ways of transforming laboratory workshops to effectively form specialized competencies and reduce the adaptation period of young specialists are proposed.

Keywords: import substitution; Astra Linux; educational programs; information security; mandatory access control; competence gap; PARSEC subsystem; technological sovereignty; laboratory workshop; personnel training.

Введение

Стратегия цифрового развития и курс на технологический суверенитет диктуют необходимость перевода критически важной ИТ-инфраструктуры на доверенное программное обеспечение. Одной из базовых платформ в этом процессе выступает операционная система Astra Linux Special Edition. Однако академическая среда, в частности программы магистратуры, зачастую продолжает базироваться на изучении проприетарных зарубежных решений. Это формирует заметный разрыв между навыками, которые получают выпускники, и реальным стеком технологий, используемым работодателями в государственном секторе и на объектах критической информационной инфраструктуры. В связи с этим возникает острая необходимость адаптации учебных курсов по защите информации к архитектурным реалиям отечественных операционных систем.

Основная часть

Компетентностный разрыв в подготовке специалистов обусловлен фундаментальными архитектурными различиями платформ. Многолетнее использование Windows сформировало у студентов паттерны, опирающиеся исключительно на дискреционное управление доступом и графические инструменты администрирования.

Сравнительный анализ подходов к администрированию, определяющих специфику образовательных программ, представлен в таблице.

Сравнительный анализ подходов к администрированию безопасности
Comparative analysis of security administration approaches

Характеристика	Традиционный подход (на примере семейства Windows)	Импортозамещающий подход (на примере Astra Linux)
Базовая модель разграничения доступа	Дискреционная (списки ACL файловой системы NTFS)	Мандатная (подсистема PARSEC, встроенная в ядро)
Изоляция процессов и данных	Базовая изоляция на уровне сессий пользователей	Изоляция по мандатным уровням и категориям конфиденциальности
Управление программной средой	Преимущественно через групповые политики (GPO) и стороннее антивирусное ПО	Нативная замкнутая программная среда (ЗПС) с проверкой цифровых подписей (ELF-файлов)

Переход на новую парадигму требует глубокого понимания логики работы с мандатными метками, контекстом безопасности процессов и принципами доверенного сеанса. Специалист, обученный на зарубежных ОС, на практике не готов к настройке мандатного контроля целостности или администрированию встроенных средств защиты Astra Linux без стороннего ПО.

Для преодоления барьера требуется системный пересмотр лабораторного практикума. Ключевым принципом адаптации выступает полное погружение обучающихся в нативную среду ОС через интерфейс командной строки. Студенты должны изучить утилиты для работы с мандатными атрибутами (pdpl-file, pdp-ls), научиться настраивать графические киоски и организовывать замкнутую программную среду (ЗПС), блокирующую запуск файлов без соответствующих цифровых подписей.

Апробация обновленных модулей в магистерских дисциплинах показала высокую эффективность. Смещение фокуса оценочных средств на практическую локализацию инцидентов (например, выявление нарушения целостности файлов) улучшило результаты аттестации. Отчеты по практике подтверждают, что студенты четко осознают взаимосвязь архитектуры ОС и требований по защите информации.

Заключение

Переход ИТ-инфраструктуры на отечественные решения выявляет существенный компетентностный дефицит среди молодых специалистов, вызванный архитектурной спецификой мандатного управления доступом. Эффективная подготовка кадров для работы с Astra Linux невозможна без концептуальной перестройки образовательных программ. Системное внедрение в учебный процесс лабораторных практикумов, ориентированных на глубокое взаимодействие со встроенными механизмами защиты (включая подсистему PARSEC), позволяет значительно повысить уровень практической подготовки выпускников и ускорить их профессиональную адаптацию.

Список использованных источников

1. Буренин П. Н., Девянин П. Н., Колесников А. В. (2021) Безопасность операционной системы специального назначения Astra Linux Special Edition. Москва, Издательство «Горячая линия – Телеком».

2. Щербаков А. Ю. (2022) Современные операционные системы: архитектура и механизмы защиты. Москва, Издательство «Горячая линия – Телеком».

3. Смирнов С. Н. (2024) Импортозамещение в сфере информационных технологий: вызовы для системы высшего образования. Вестник педагогических наук. (2), 15–22.

References

1. Burenin P. N., Devyanin P. N., Kolesnikov A. V. (2021) Security of the Special Purpose Operating System Astra Linux Special Edition. Moscow, Goryachaya liniya – Telekom Publishing House (in Russian).

2. Shcherbakov A. Yu. (2022) Modern Operating Systems: Architecture and Security Mechanisms. Moscow, Goryachaya liniya – Telekom Publishing House (in Russian).

3. Smirnov S. N. (2024) Import Substitution in the Field of Information Technology: Challenges for the Higher Education System. Bulletin of Pedagogical Sciences. (2), 15–22 (in Russian).

Сведения об авторе

Бердник А.И., инженер электросвязи, ООО «Альпиндустрия», berdnik1326547@gmail.com.

Information about the author

Berdnik A.I., Telecommunications Engineer, Alpindustria LLC, berdnik1326547@gmail.com.