Сразу скажем, что интерес к подобного рода программным решениям у нас возник не случайно. Всё дело в том, что 7 мая президент Владимир Путин подписал указ «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», обязующий все государственные ведомства и учреждения к упомянутому сроку перевести свои IT-системы на отечественный софт. Особый акцент глава государства сделал на обеспечении безопасности хранящихся и обрабатываемых в таких системах данных, защита которых особенно актуальна для военных и силовых структур, частенько оперирующих конфиденциальной информацией и составляющими гостайну сведениями, в том числе с грифом «совершенно секретно». Что на сегодняшний день таким организациям могут предложить российские компании – разработчики ПО? Давайте посмотрим.

Astra Linux Special Edition

Разработчик: НПО «Русские базовые информационные технологии» (РусБИТех)
Сайт продукта: astra-linux.ru

Программная платформа специального назначения для создания защищённых рабочих мест и автоматизированных систем любой сложности, обрабатывающих информацию ограниченного доступа. Astra Linux Special Edition оснащена развитыми средствами обеспечения информационной безопасности обрабатываемых данных, механизмами мандатного разграничения доступа, контроля замкнутости программной среды и защиты адресного пространства системных процессов, встроенными инструментами маркировки документов, регистрации событий, контроля целостности данных, а также прочими обеспечивающими защиту информации компонентами. ОС поддерживает работу с различным аппаратными платформами и может функционировать на системах с отечественными процессорами «Эльбрус», «Байкал-Т1» и «Комдив».

По заверениям разработчиков, Astra Linux Special Edition – единственная программная платформа, сертифицированная одновременно в системах ФСТЭК России, ФСБ, Минобороны РФ и позволяющая обрабатывать информацию ограниченного доступа, содержащую составляющие государственную тайну сведения с грифом не выше «совершенно секретно» в автоматизированных средствах всех министерств, ведомств и других учреждений Российской Федерации. Система включена в единый реестр российских программ для электронно-вычислительных машин и баз данных Минкомсвязи России, принята на снабжение Вооружённых Сил Российской Федерации и активно внедряется другими органами государственного управления, ведомствами и учреждениями.

Мобильная система Вооружённых cил (МСВС)

Разработчик: Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере им. В. В. Соломатина (ВНИИНС)
Сайт продукта: vniins.ru

Операционная система общего назначения, предназначенная для построения стационарных и мобильных защищённых автоматизированных систем. Принята на снабжение в Вооружённых Силах Российской Федерации в 2002 году. В основу МСВС положены ядро и компоненты Linux, дополненные дискреционной, мандатной и ролевой моделями разграничения доступа к информации, а также развитыми средствами аудита (протоколирования событий). Система функционирует на аппаратных платформах Intel (x86 и x86\_64), SPARC («Эльбрус-90микро»), MIPS, PowerPC64, SPARC64 и сертифицирована по требованиям безопасности информации Министерства обороны РФ и ФСБ России. В качестве рабочего окружения используется оконный менеджер ELK, стилизованный под Windows XP. Реализованные в МСВС средства защиты позволяют создавать на базе платформы автоматизированные системы, которые обрабатывают составляющие государственную тайну сведения, имеющие степень секретности «совершенно секретно».

ОС «Заря»

Разработчик: ФГУП «Центральный научно-исследовательский институт экономики, информатики и систем управления» («ЦНИИ ЭИСУ», входит в «Объединённую приборостроительную корпорацию»)
Сайт продукта: cniieisu.ru

Семейство программных платформ на ядре Linux, которые могут быть использованы как для создания защищённых рабочих станций в автоматизированных системах специального назначения, так и для работы в составе серверов, встраиваемых систем, центров обработки данных или отдельных программно-технических комплексов. Уровень секретности обрабатываемой информации — не выше «совершенно секретно». В ОС «Заря» имеются офисные приложения, инструменты обработки изображений, средства виртуализации и защиты информации, а также защищённый веб-браузер. Система сертифицирована Минобороны России, соответствует третьему классу защиты от несанкционированного доступа и второму уровню контроля отсутствия недекларированных возможностей. Платформа разработана по заказу Министерства обороны РФ и предназначена в первую очередь для силовых ведомств, предприятий военно-промышленного комплекса, а также коммерческих структур, работающих с государственной тайной и персональными данными.

ЗОСРВ «Нейтрино»

Разработчик: ООО «СВД Встраиваемые Системы»
Сайт продукта: kpda.ru

Защищённая операционная система реального времени (ЗОСРВ), построенная на базе платформы QNX Neutrino. Предназначена для создания вычислительных устройств и комплексов, к которым предъявляются повышенные требования по надёжности, отказоустойчивости и предсказуемости поведения. Система поддерживает широкий спектр аппаратных платформ с архитектурами Intel x86, ARM, PowerPC, MIPS, в том числе отечественные микропроцессорные решения «Эльбрус», КОМДИВ и «Мультикор». Особенности ЗОСРВ «Нейтрино»: архитектура на основе микроядра с динамически обновляемыми системными сервисами и драйверами, поддержка многоядерных процессоров, система контроля работоспособности для ранней диагностики отказов и автоматического восстановления сбойных компонентов, полноценный сетевой стек и поддержка технологии адаптивного квотирования ресурсов. Платформа соответствует требованиям руководящих документов Гостехкомиссии России по защите информации от несанкционированного доступа и имеет в своём активе сертификаты ФСТЭК и Минобороны России.

СУБД «Линтер Бастион»

Разработчик: компания «Релэкс»
Сайт продукта: linter.ru

Российская система управления базами данных, реализующая стандарт SQL:2003 (за исключением нескалярных типов данных и объектно ориентированных возможностей) и ведущая свою историю аж с 1980 года. СУБД «Линтер Бастион» имеет сертификат соответствия Минобороны и ФСТЭК России, включена в реестр отечественного ПО и гарантирует надёжную защиту информации от уровня «персональные данные» до уровня «совершенно секретно». Решение поддерживает работу в средах Windows, Linux, QNX и российских ОС «ЗОСРВ Нейтрино», Astra Linux Special Edition, «Альт Линукс», МСВС, включает средства многоуровневой защиты данных (контроль доступа, шифрование, аудит действий пользователей, удаление остаточной информации и др.) и предназначено для использования прежде всего в подразделениях Министерства обороны, Министерства внутренних дел РФ, в силовых структурах, а также на предприятиях, обеспечивающих государственный оборонный заказ. Система также может быть задействована для обработки и хранения информации в автоматизированных системах управления (АСУ ТП, SCADA, промышленных контроллерах, КИПиА и других), работающих в режиме реального времени.

СУБД «Заря»

Разработчик: ФГУП «ЦНИИ ЭИСУ»
Сайт продукта: cniieisu.ru

Сертифицированная Минобороны России система управления базами данных, предназначенная для обработки данных, составляющих государственную тайну, а также коммерческих и персональных сведений. СУБД «Заря» построена на базе свободной объектно-реляционной системы управления базами данных PostgreSQL и имеет в своём составе балансировщик нагрузки pgpool-II, механизмы мандатного разграничения доступа к данным, средства администрирования и драйверы JDBC/ODBC для взаимодействия с прикладным ПО. Функциональные возможности позволяют использовать СУБД «Заря» для создания отказоустойчивых территориально-распределённых хранилищ данных, в том числе для развёртывания высокопроизводительных систем управления данными, работающих в режиме реального времени на критически важных объектах. Также сообщается о поддержке платформы «1С:Предприятие».

Система управления событиями ИБ «Комрад»

Разработчик: Научно-производственное объединение «Эшелон»
Сайт продукта: npo-echelon.ru

Программный комплекс, совместимый с отечественными средствами защиты информации и предназначенный для централизованного управления событиями информационной безопасности (ИБ). Система «Комрад» позволяет IT-службам в режиме реального времени осуществлять централизованный мониторинг событий ИБ, выявлять инциденты информационной безопасности, оперативно реагировать на возникающие угрозы, а также выполнять требования, предъявляемые регуляторами к защите персональных данных, в том числе к обеспечению безопасности государственных информационных систем. В составе комплекса представлены инструменты сбора, обработки и аудита событий, средства аналитики и визуализации данных, механизмы оперативного оповещения об инцидентах (всплывающие уведомления, электронная почта, SMS) и другие функции, востребованные специалистами по информационной безопасности. Продукт сертифицирован ФСТЭК и Минобороны России, а также зарегистрирован в реестре отечественного ПО.

истема мониторинга каналов связи «Сокол»

Разработчик: компания «Воентелеком»
Сайт продукта: voentelecom.ru

Комплекс «Сокол», разработанный специально для нужд Минобороны России, ведомств силового блока и предприятий оборонно-промышленного комплекса, предназначен для мониторинга качественных характеристик каналов связи. Решение функционирует под управлением ОС Astra Linux Special Edition, использует свободную объектно-реляционную систему управления базами данных PostgreSQL, имеет открытый API (с поддержкой JSON-RPC 2.0), поддерживает протоколы Netflow, SNMP, Syslog, проверку соответствия канала связи договору SLA и одновременный мониторинг более чем 1000 узлов. Система мониторинга «Сокол» поддерживает работу с сетевыми устройствами и серверным оборудованием различных производителей, обладает высокой производительностью, достаточной для обработки больших объёмов данных, и может масштабироваться для крупных IT-инфраструктур. Комплекс оснащён веб-интерфейсом с надёжной аутентификацией пользователей и предоставляет гибкие права доступа для администраторов системы и операторов связи. Наряду с хранением данных и функциями их визуализации доступны построение карт сети, графиков, а также возможности анализа данных с целью своевременного оповещения о сбоях в IT-инфраструктуре.