THE LINUX FOUNDATION
SILVER MEMBER

Научно-производственное объединение
РусБИТех
Открытое акционерное общество

СПРАВКА

ОБ ОСОБЕННОСТЯХ И ОСНОВНЫХ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЯХ ОПЕРАЦИОННОЙ СИСТЕМЫ

ASTRA LINUX
special edition

ОПЕРАЦИОННАЯ СИСТЕМА
СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

СОДЕРЖАНИЕ

НАЗНАЧЕНИЕ И СЕРТИФИКАТЫ

НАЗНАЧЕНИЕ ОПЕРАЦИОННОЙ СИСТЕМЫ

Операционная система специального назначения «Astra Linux Special Edition» (далее – ОС СН) предназначена для создания на ее основе автоматизированных систем в защищенном исполнении, обрабатывающих информацию до степени секретности «совершенно секретно» включительно.

СЕРТИФИКАТЫ СООТВЕТСТВИЯ

ОС СН соответствует требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992 г.) — **по 3 классу и 2 уровню** контроля отсутствия недекларированных возможностей согласно руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999 г.).

ОС СН может использоваться в составе автоматизированных систем класса защищенности до 1Б включительно, обрабатывающих информацию до степени сектретности «совершенно секретно» включительно.

Минобороны России

№ 1339 от 24.09.2010. Действителен до 2018 г.

Приказом Министра обороны Российской Федерации № 475 в 2013 году ОС СН принята на снабжение Вооруженных Сил Российской Федерации

ФСТЭК России

№ 2557 от 27.01.2012. Действителен до 2018 г.

ФСБ

СФ/014-2579 от 20.03.2015. Действителен до 2018 г.

Встроенные средства защиты спроектированы и разработаны совместно с Академией ФСБ России.

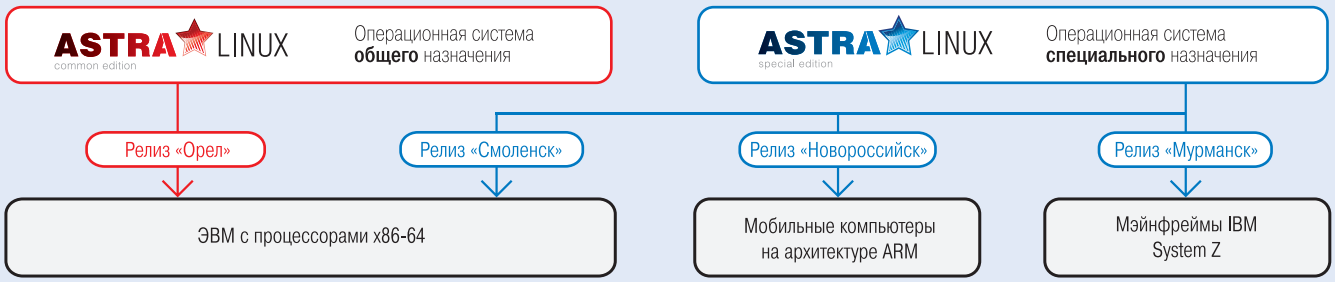
ОС СН соответствует требованиям ФСБ России к программному обеспечению, используемому в информационных и телекоммуникационных системах специального назначения, и требованиям по защите информации от несанкционированного доступа с использованием средств криптографической защиты информации в автоматизированных информационных системах, расположенных на территории Российской Федерации, 1 класса, и может использоваться для обработки информации, содержащей сведения, составляющую государственную тайну, до степени секретности «совершенно секретно» включительно.

Виды защищаемой информации

Коммерческая тайна | Персональные данные | Государственная тайна

СВИДЕТЕЛЬСТВА И ПАТЕНТ

СВИДЕТЕЛЬСТВА



№ 2009615665

№ 2009616752

№ 2014618600

№ 2014618809

ПАТЕНТ

Патент на изобретение «Способ обеспечения безопасности информационных потоков в защищенных информационных системах с мандатным и ролевым управлением доступом».

№ 2525481 (RU)

Патентообладатели: ОАО «НПО РусБИТех», Девянин П.Н.

Автор: Девянин П.Н.

Заявка № 2012146550

Приоритет изобретения: 01.11.2012

Опубликовано: 10.05.2014, Бюл. № 13. 12 с.: ил.

МПК G06F21/62

ЗАКАЗЧИКИ

МИНИСТЕРСТВА, ВЕДОМСТВА, АГЕНТСТВА И СПЕЦИАЛЬНЫЕ СЛУЖБЫ

- Минобороны России
- ФСБ России
- ФСО России
- МВД России
- Внутренние войска МВД России
- ФСИН России
- ФТС России
- ГУСП
- Роскосмос

ВУЗЫ

- Более 6000 бесплатных лицензий

МЕЖВЕДОМСТВЕННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ГАС ГОЗ

НАЦИОНАЛЬНЫЙ ЦЕНТР УПРАВЛЕНИЯ ОБОРОНОЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Виды защищаемой информации

Коммерческая тайна	Персональные данные	Государственная тайна

ГОСКОРПОРАЦИИ

- СВР России
- ФСТ России
- Росатом
- Ростех

ПРЕДПРИЯТИЯ ОБОРОННО-ПРОМЫШЛЕННОГО КОМПЛЕКСА

Виды защищаемой информации

Коммерческая тайна | Персональные данные | Государственная тайна

ПРОГРАММНЫЕ ПЛАТФОРМЫ

ПОДДЕРЖИВАЕМОЕ ОБОРУДОВАНИЕ

Обеспечивается функционирование операционной системы «Astra Linux Special Edition» на различных видах вычислительной техники

Требуется государственное регулирование взаимодействия с производителями оборудования и комплектующих

** при необходимости установки на специальную технику требуется дополнительная сертификация ОС СН*

Виды защищаемой информации

Коммерческая тайна	Персональные данные	Государственная тайна

ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НСД ДЛЯ АС

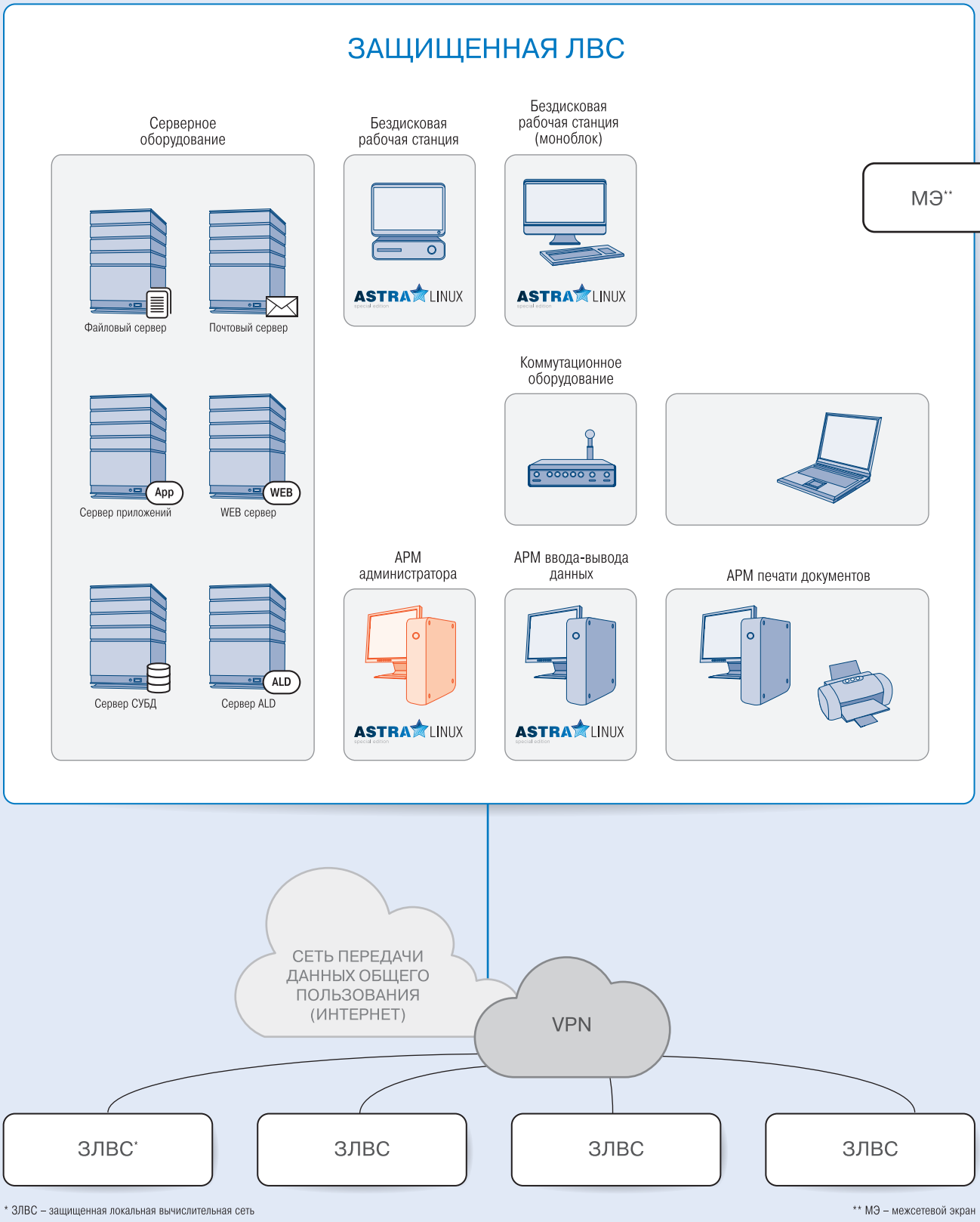
ПОДСИСТЕМЫ И ФУНКЦИИ	ТРЕБОВАНИЯ	Уровень защищаемой информации	Совсекретно							
						Секретно				
					ДСП					
			Перс.данные							
		РЕАЛИЗАЦИЯ	1Д	2Б	3Б	1Г	1В	3А	2А	1Б
1. Подсистема управления доступом										
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:	Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;	Astra Linux								
- в систему	Должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной не менее восьми буквенно-цифровых символов;	Astra Linux	+	+	+	+	+	+	+	+
- к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	Должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по физическим адресам (номерам);	Astra Linux				+	+		+	+
- к программам	Должна осуществляться идентификация программ;	Astra Linux				+	+		+	+
- к томам, каталогам, файлам, записям, полям записей	Должна осуществляться идентификация томов, каталогов, файлов, записей, полей записей по именам;	Astra Linux				+	+		+	+
1.2. Управление потоками информации	Должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.	Astra Linux					+		+	+
2. Подсистема регистрации и учета										
2.1. Регистрация и учет:										
- входа (выхода) субъектов доступа в (из) систему (узел сети)	Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. *В параметрах регистрации указываются:* дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы; результат попытки входа: успешный или неуспешный - несанкционированный; идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа; код или пароль, предъявленный при неуспешной попытке;	Astra Linux + АПМДЗ «Максим»	+	+	+	+	+	+	+	+
- выдачи печатных (графических) выходных документов	Должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа - фактически выданного количества листов в графе «Брак»). *В параметрах регистрации указываются:* дата и время выдачи (обращения к подсистеме вывода); спецификация устройства выдачи [логическое имя (номер) внешнего устройства]; краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа; идентификатор субъекта доступа, запросившего документ; объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи успешный (весь объем), неуспешный;	Astra Linux + доп. ПО управления выводом на печать (разработка ОАО «НПО РусБИТех»)				+	+	+	+	+
- запуска (завершения) программ и процессов (заданий, задач)	Должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. *В параметрах регистрации указываются:* дата и время запуска; имя (идентификатор) программы (процесса, задания); идентификатор субъекта доступа, запросившего программу (процесс, задание); результат запуска (успешный, неуспешный - несанкционированный);	Astra Linux				+	+		+	+
- доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	Должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. *В параметрах регистрации указываются:* дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная; идентификатор субъекта доступа; спецификация защищаемого файла; имя программы (процесса, задания, задачи), осуществляющей доступ к файлу; вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);	Astra Linux				+	+		+	+
- доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. *В параметрах регистрации указываются:* дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная; идентификатор субъекта доступа; спецификация защищаемого объекта [логическое имя (номер)]; имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту; вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);	Astra Linux + АПМДЗ «Максим»				+	+		+	+
изменения полномочий субъектов доступа	Должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. *В параметрах регистрации указываются:* дата и время изменения полномочий; идентификатор субъекта доступа (администратора), осуществившего изменения; идентификатор субъекта, у которого проведено изменение полномочий и вид изменения (пароль, код, профиль и т.п.); спецификация объекта, у которого проведено изменение статуса защиты и вид изменения (код защиты, уровень конфиденциальности);	Astra Linux + АПМДЗ «Максим»					+			+
создаваемых защищаемых объектов доступа	Должен осуществляться автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;	Astra Linux					+		+	+
2.2. Учет носителей информации	Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки; Учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема); Должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;	Орг. меры	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;	Astra Linux				+	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	Должна осуществляться сигнализация попыток нарушения защиты на терминал администратора и нарушителя.	Astra Linux + доп. ПО отображения событий (разработка ОАО «НПО РусБИТех»)					+			+
3. Криптографическая подсистема										
3.1. Шифрование конфиденциальной информации	Должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные портативные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться принудительная очистка областей внешней памяти, содержавших ранее незашифрованную информацию;								+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	Доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;									
3.3. Использование аттестованных (сертифицированных) криптографических средств	Должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.								+	+
4. Подсистема обеспечения целостности										
4.1. Обеспечение целостности программных средств и обрабатываемой информации	Должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом: целостность СЗИ НСД проверяется по контрольным суммам всех компонент СЗИ как в процессе загрузки, так и динамически в процессе работы АС; целостность программной среды обеспечивается качеством приемки программных средств в АС, предназначенных для обработки защищенных файлов;	Astra Linux + АПМДЗ «Максим»	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;	Орг. меры	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	Должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;	Орг. меры					+		+	+
4.4. Периодическое тестирование СЗИ НСД	Должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;	Astra Linux	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также оперативное восстановление функций СЗИ НСД при сбоях;	Орг. меры	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	Должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.	Орг. меры					+	+	+	+

Виды защищаемой информации

Коммерческая тайна | **Персональные данные** | **Государственная тайна**

ОБЛАСТЬ ПРИМЕНЕНИЯ. СОЗДАНИЕ ЗАЩИЩЕННЫХ ТЕРРИТОРИАЛЬНО

СЕГМЕНТ ОБРАБОТКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ



* ЗЛВС – защищенная локальная вычислительная сеть

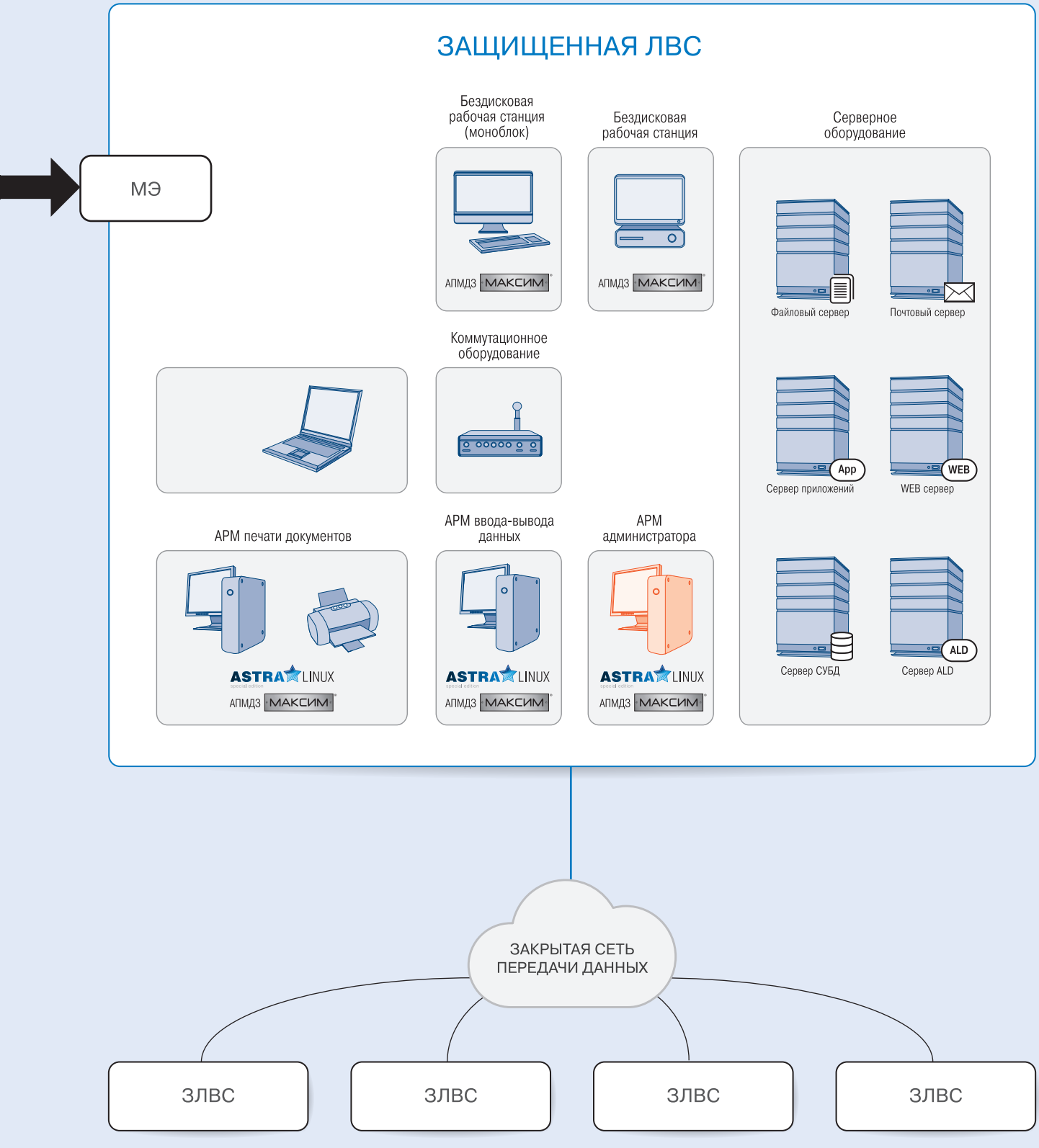
** МЭ – межсетевой экран

Виды защищаемой информации

Коммерческая тайна	Персональные данные	Государственная тайна

РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

СЕГМЕНТ ОБРАБОТКИ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ



ОСНОВНЫЕ КОМПОНЕНТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ

ОС СН «Astra Linux Special Edition»

Виды защищаемой информации

Коммерческая тайна | Персональные данные | Государственная тайна

ОСНОВНЫЕ КОМПОНЕНТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ

ЗАЩИЩЕННЫЙ ПРОГРАММНЫЙ КОМПЛЕКС ОРГАНИЗАЦИИ ЕДИНОГО ПРОСТРАНСТВА ПОЛЬЗОВАТЕЛЕЙ И РЕСУРСОВ ЛВС (ДОМЕН ALD)

- АДМИНИСТРИРОВАНИЕ ДОМЕНА ALD СРЕДСТВАМИ УПРАВЛЕНИЯ
- УПРАВЛЕНИЕ РАЗГРАНИЧЕНИЕМ ДОСТУПА К ВНЕШНИМ НОСИТЕЛЯМ
- СКВОЗНАЯ АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ
- АУДИТ И РЕГИСТРАЦИЯ СОБЫТИЙ
- ЦЕНТРАЛИЗОВАННОЕ ХРАНЕНИЕ АТРИБУТОВ ПОЛИТИКИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
- ИНТЕГРАЦИЯ В ДОМЕН ALD ЗАЩИЩЕННЫХ СЕРВЕРОВ СУБД, ЭЛЕКТРОННОЙ ПОЧТЫ, ГИПЕРТЕКСТОВОЙ ОБРАБОТКИ ДАННЫХ, ПЕЧАТИ И СРЕДСТВ МАРКИРОВКИ ДОКУМЕНТОВ

РАБОТА С МУЛЬТИМЕДИА И ИЗОБРАЖЕНИЯМИ

- ПРОГРАММЫ ДЛЯ ВОСПРОИЗВЕДЕНИЯ АУДИО И ВИДЕО ФАЙЛОВ
- РЕДАКТОР РАСТРОВОЙ ГРАФИКИ
- ЗАПИСЬ ОПТИЧЕСКИХ ДИСКОВ
- ПРОГРАММА СКАНИРОВАНИЯ И РАБОТЫ С WEB-КАМЕРОЙ

РАБОТА С ДОКУМЕНТАМИ (LIBREOFFICE)

- ТЕКСТОВЫЙ РЕДАКТОР
- РЕДАКТОР ЭЛЕКТРОННЫХ ТАБЛИЦ
- РЕДАКТОР ПРЕЗЕНТАЦИЙ
- РЕДАКТОР ВЕКТОРНОЙ ГРАФИКИ
- РЕДАКТОР ФОРМУЛ

ОСОБЕННОСТИ ОРГАНИЗАЦИИ ДОМЕНА ALD

Домен Astra Linux Directory (ALD) представляет собой набор средств для организации работы пользователей в локально вычислительной сети (ЛВС) на платформе ОС СН. В основу положен доменный принцип построения ЛВС, при котором все логически связанные сетевые ресурсы и пользователи объединяются в единую систему идентификации и аутентификации с централизованным управлением политикой безопасности в соответствии с правилами мандатного разграничения доступа информации. При этом пользователь получает возможность взаимодействия как с другими пользователями сети, так и с сетевыми ресурсами.

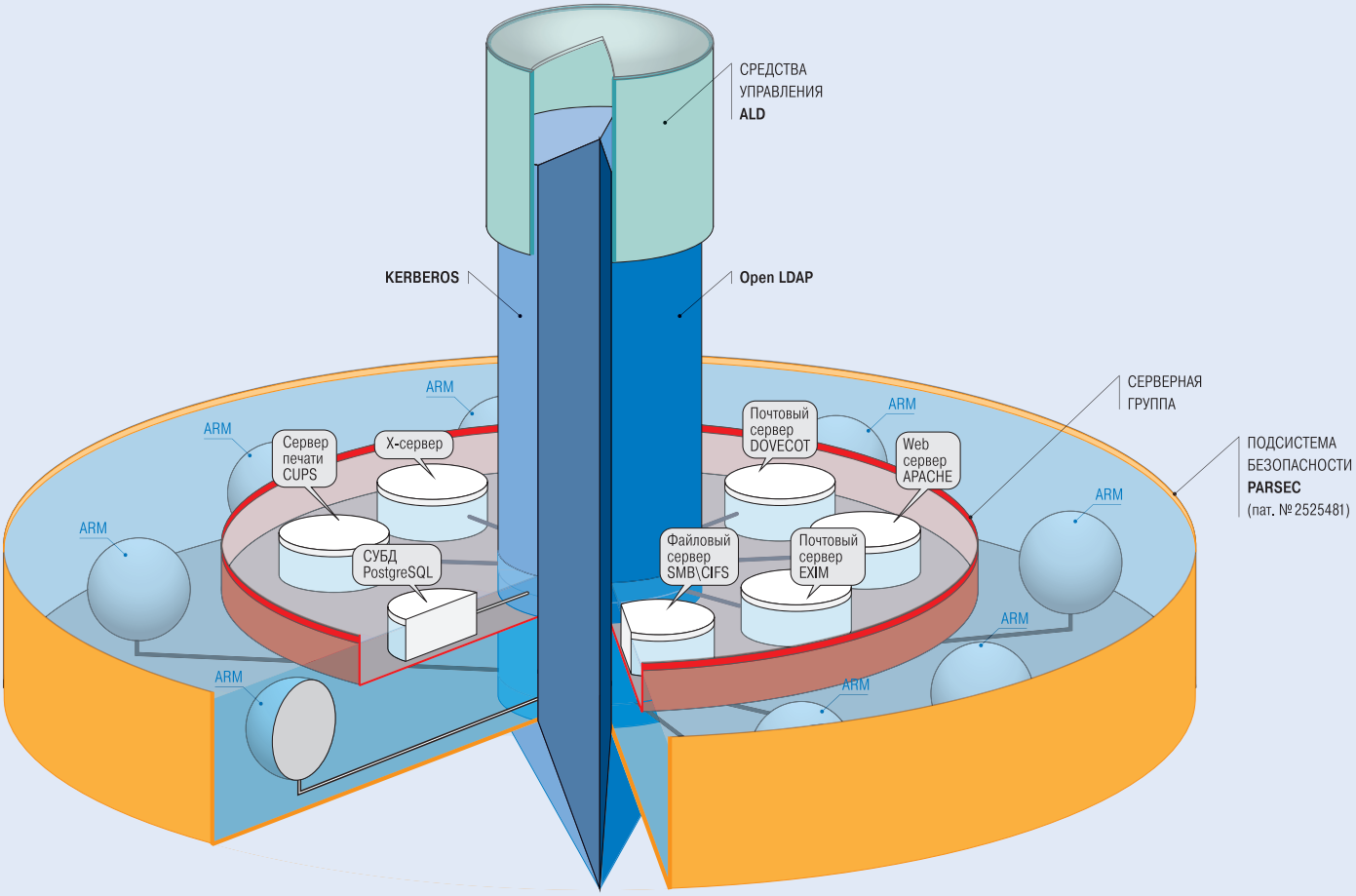


СХЕМА ОРГАНИЗАЦИИ ДОМЕНА ALD

Система управления доменом ALD построена на технологиях LDAP, Kerberos 5, CIFS и интегрирована со средствами защиты информации от НСД из состава ОС СН. Система управления доменом ALD обеспечивает сквозную аутентификацию для входа в защищенную серверную группу и автоматическую настройку всех необходимых файлов конфигурации служб, а также предоставляет удобный интерфейс администрирования.

СЕТЕВЫЕ СРЕДСТВА

С помощью утилит администрирования домена ALD возможно выполнение следующих административных действий:

БАЗОВЫЕ СЕТЕВЫЕ СЛУЖБЫ

TCP/IP

- ✓ адресация пакетов
- ✓ маршрутизация
- ✓ организация подсетей
- ✓ проверка и отладка сети

NFS

Служба сетевого доступа к файловым системам удаленных серверов и компьютеров

Сервер единого времени

Синхронизация времени компьютеров в локально-вычислительной сети

FTP

Служба файлового обмена

Фильтр сетевых пакетов

Контроль сетевого трафика, проходящего через данный компьютер:

- ✓ фильтрация пакетов
- ✓ трансляция сетевых адресов
- ✓ прозрачное проксирование

DNS

Служба доменных имен

DHCP

Сервер динамической конфигурации сети

SSH

Клиент-серверная система для организации защищенных туннелей между двумя и более компьютерами

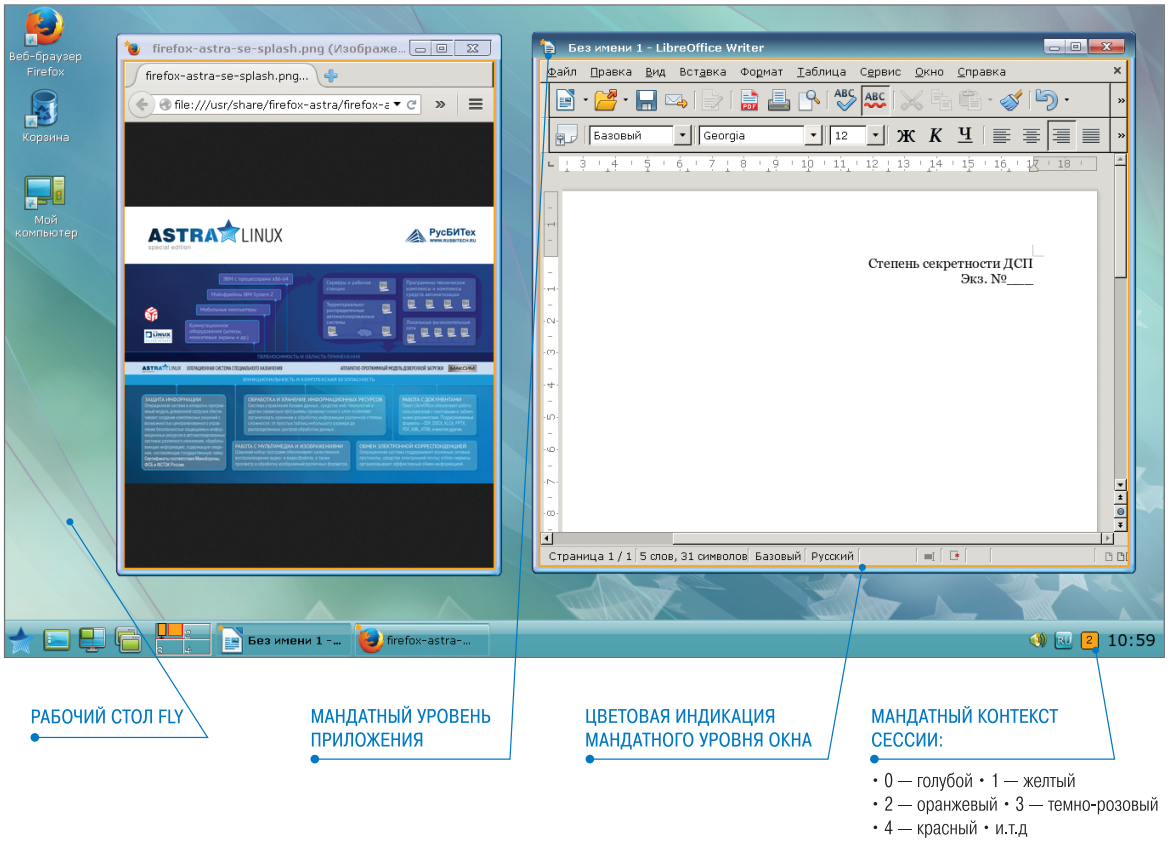
Сетевая защищенная файловая система

Организация защищенных файловых серверов с файловой системой CIFS, работающая по протоколу SMB/CIFS.

ЗАЩИЩЕННАЯ ГРАФИЧЕСКАЯ СИСТЕМА FLY

Задача обеспечения защищенного графического интерфейса пользователя в ОС СН решается с использованием клиент-серверной архитектуры X Window. Для предотвращения реализации угроз нарушения конфиденциальности и целостности информации в обход мандатного разграничения доступа, применяется технология запуска собственного графического сеанса в соответствии с мандатным контекстом (сочетанием уровня и категорий) сессии.

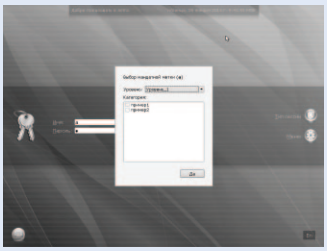
В состав защищенной графической системы ОС СН входит рабочий стол пользователя FLY, интегрированный с внедренными в X-сервер механизмами защиты информации и обеспечивающий отображение мандатного контекста сессии:



Другим ключевым свойством рабочего стола FLY является возможность его масштабирования. При необходимости рабочий стол FLY можно перевести в режим работы планшетного компьютера. При этом все приложения запускаются в полноэкранном режиме, а управление ими осуществляется с помощью сенсорного экрана.

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

При графическом входе в систему пользователь выбирает в специальном диалоге уровень и категорию конфиденциальности. После этого вся его графическая сессия будет выполняться в режиме выбранной совокупности уровня секретности и/или категории. Одновременно пользователем может быть выполнено несколько входов в разных режимах. При таком подходе сессии изолированы и передача информации между ними невозможна.



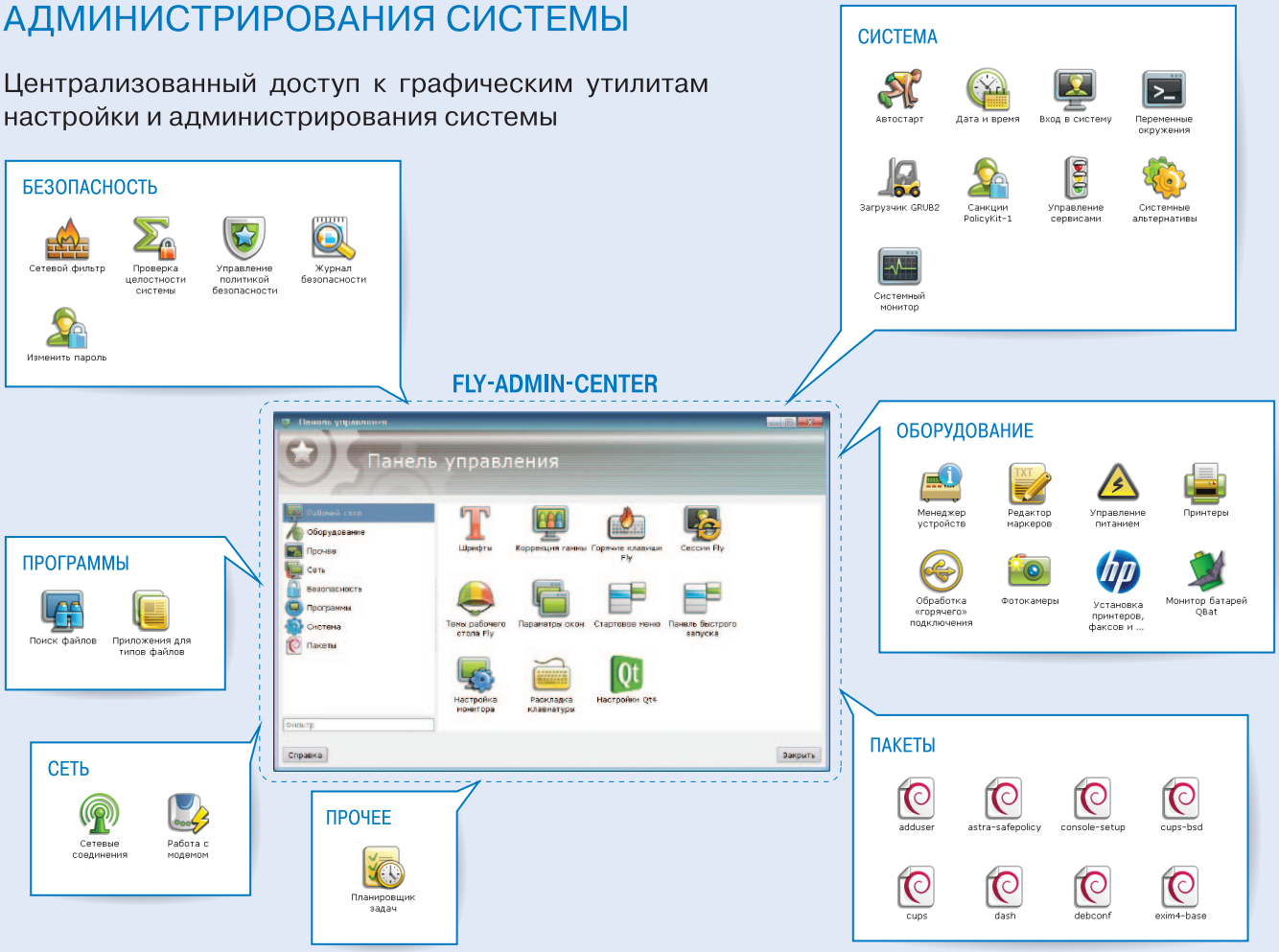
Виды защищаемой информации

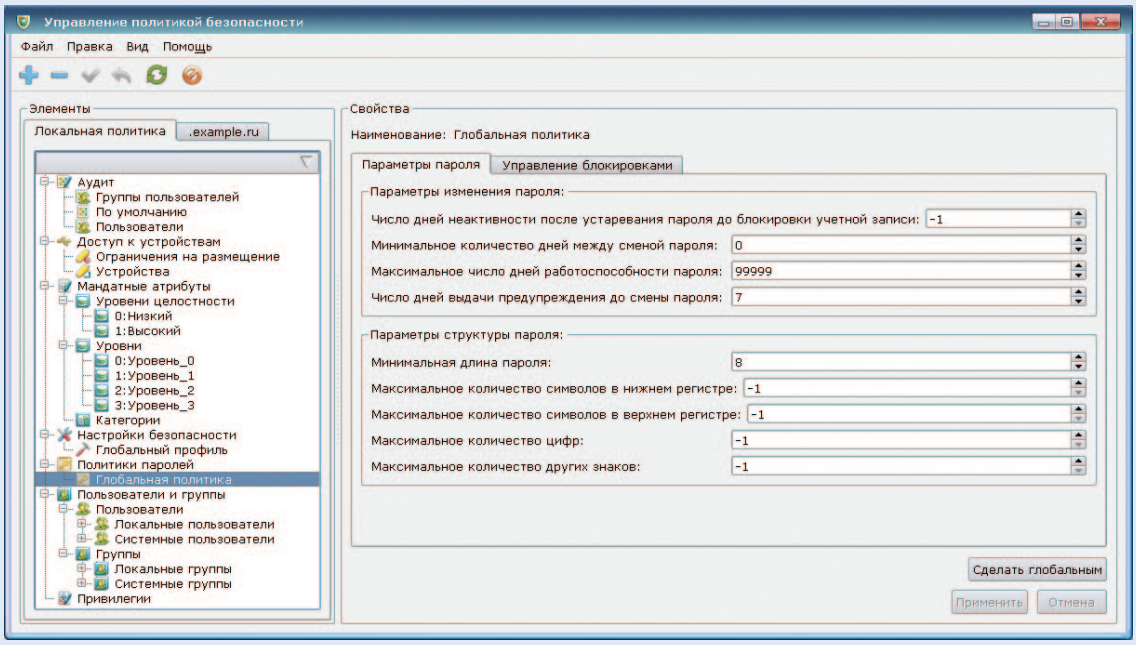
Коммерческая тайна | Персональные данные | Государственная тайна

ЗАЩИЩЕННАЯ ГРАФИЧЕСКАЯ СИСТЕМА FLY

ОСНОВНЫЕ ГРАФИЧЕСКИЕ УТИЛИТЫ ДЛЯ АДМИНИСТРИРОВАНИЯ СИСТЕМЫ

Централизованный доступ к графическим утилитам настройки и администрирования системы





Виды защищаемой информации

Коммерческая тайна	Персональные данные	Государственная тайна

ЗАЩИЩЕННАЯ ГРАФИЧЕСКАЯ СИСТЕМА FLY

ОСНОВНЫЕ ГРАФИЧЕСКИЕ УТИЛИТЫ ДЛЯ АДМИНИСТРИРОВАНИЯ СИСТЕМЫ

fly-admin-center — панель управления

1 **fly-admin-cron** — планировщик задач

2 **fly-admin-device-manager** — управление системными устройствами

3 **fly-admin-dhcp** — настройка сервера DHCP

fly-admin-dm — настройка входа в систему

4 **fly-admin-ftp** — настройка сервера FTP

fly-admin-int-check — проверка целостности системы

fly-admin-kiosk — создание и настройка профилей для режима «киоск»

Synaptic — управление программными пакетами

5 **fly-admin-printer** — настройка серверов печати и локальных принтеров

fly-admin-scan — проверка установленных сканеров

fly-admin-gamma — установка цветового баланса монитора

fly-admin-smc — управление локальной политикой безопасности и в домене ALD (управление протоколированием, привилегиями и мандатными атрибутами пользователей, работа с пользователями и группами, настройка доступа к внешним устройствам)

fly-admin-wicd — настройка сетевых соединений

fly-admin-date — установка даты и времени

fly-admin-policykit — настройка полномочий

fly-admin-viewaudit — поиск и просмотр записей системы протоколирования

6 **fly-admin-firewall** — мастер настройки сетевого фильтра

fly-admin-xhost — настройка удаленного доступа к X-серверу

fly-admin-hotkeys — установка клавиш быстрого доступа

fly-mimeapps-service — установка приложений для типов файлов

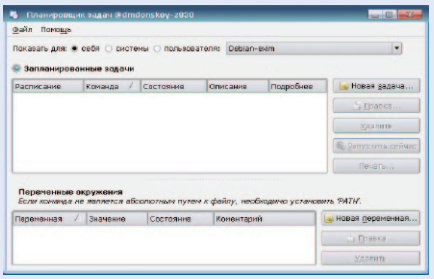
fly-randr — утилита настройки монитора и многомониторного режима

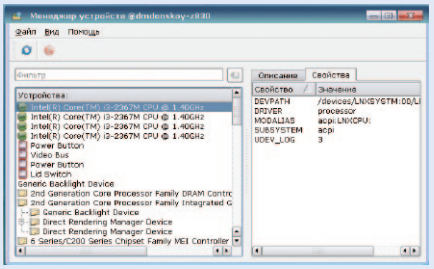
fly-admin-theme — утилита настройки тем рабочего стола и режимов переключения рабочий стол/планшет

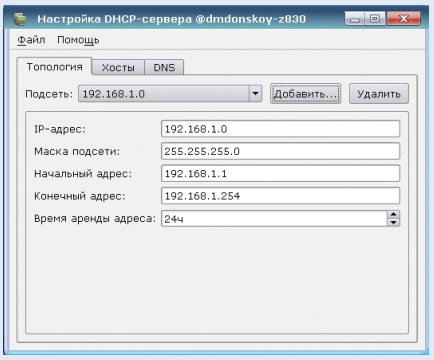
fly-menuedit — настройка меню «Пуск» и «Панель быстрого запуска»

fly-admin-samba — утилита управления общими папками Samba

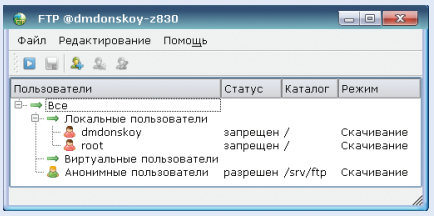
fly-admin-marker — редактор маркировки страниц, выводимых на печать


1

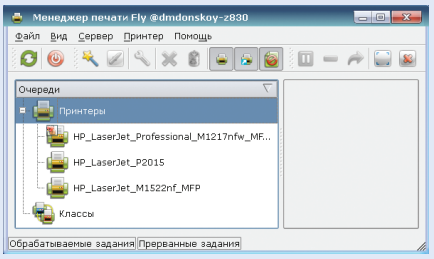

2



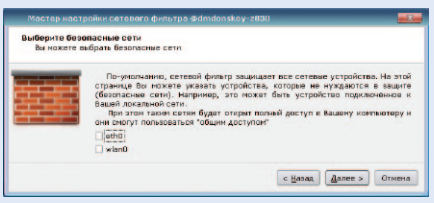
3



4



5



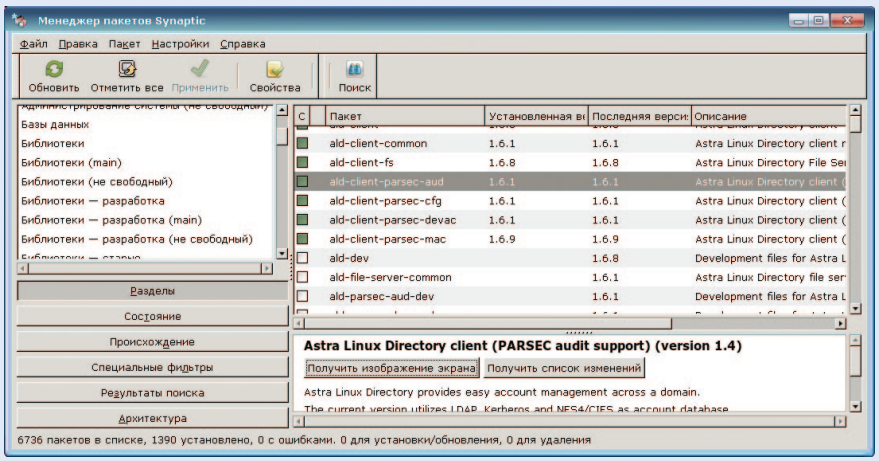
6

Виды защищаемой информации

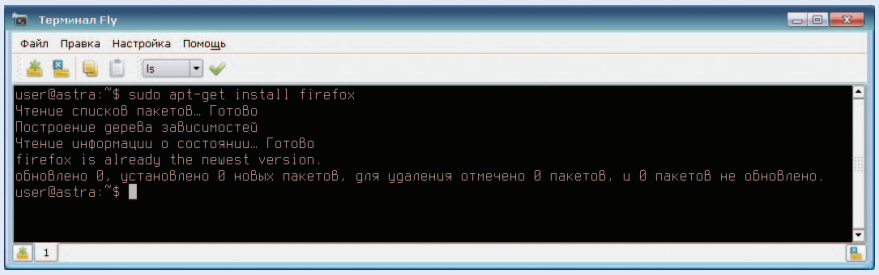
Коммерческая тайна | Персональные данные | Государственная тайна

УПРАВЛЕНИЕ ПРОГРАММНЫМИ ПАКЕТАМИ

В ОС СН используются программные пакеты в формате «deb». Для управления пакетами в режиме командной строки (или в эмуляторе терминала в графическом режиме) предназначены набор команд нижнего уровня dpkg и комплекс программ высокого уровня apt-get и aptitude.



По умолчанию обычный пользователь не имеет права использовать эти инструменты. Для всех операций с пакетами необходимы права администратора.

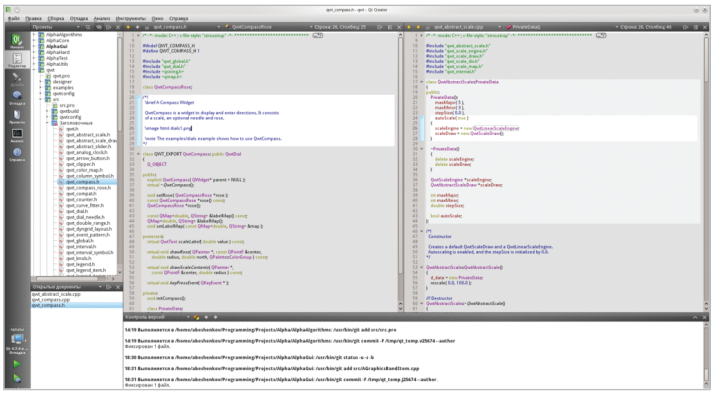


Мониторинг системы в процессе установки и ведение журнала установки позволяют корректно удалить приложение, ставшее ненужным.

Средства управления пакетами обеспечивают возможность автоматизированной установки обновлений ОС СН.

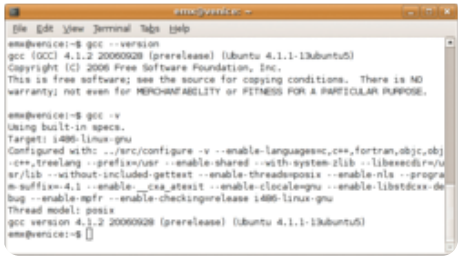
СРЕДСТВА РАЗРАБОТКИ

Кроссплатформенная свободная IDE для разработки на C, C++ и QML включает в себя графический интерфейс отладчика и визуальные средства разработки интерфейса.



Основная задача Qt Creator — упростить разработку приложения с помощью фреймворка Qt на разных платформах.

Набор компиляторов GCC для различных языков программирования



Отладчик GDB предлагает обширные средства для слежения и контроля за выполнением компьютерных программ.

ASTRA LINUX special edition

Операционная система специального назначения

Версия 1.2	Версия 1.3	Версия 1.4
Ядро 2.6.34 libc 2.7 GCC 4.3 QT 4.6	Ядро 3.2.0 libc 2.13 GCC 4.7 QT 4.8.3	Ядро 3.16.0 libc 2.13 GCC 4.7.2 QT 5.3.0

ЗАГОЛОВОЧНЫЕ ФАЙЛЫ

БИБЛИОТЕКИ

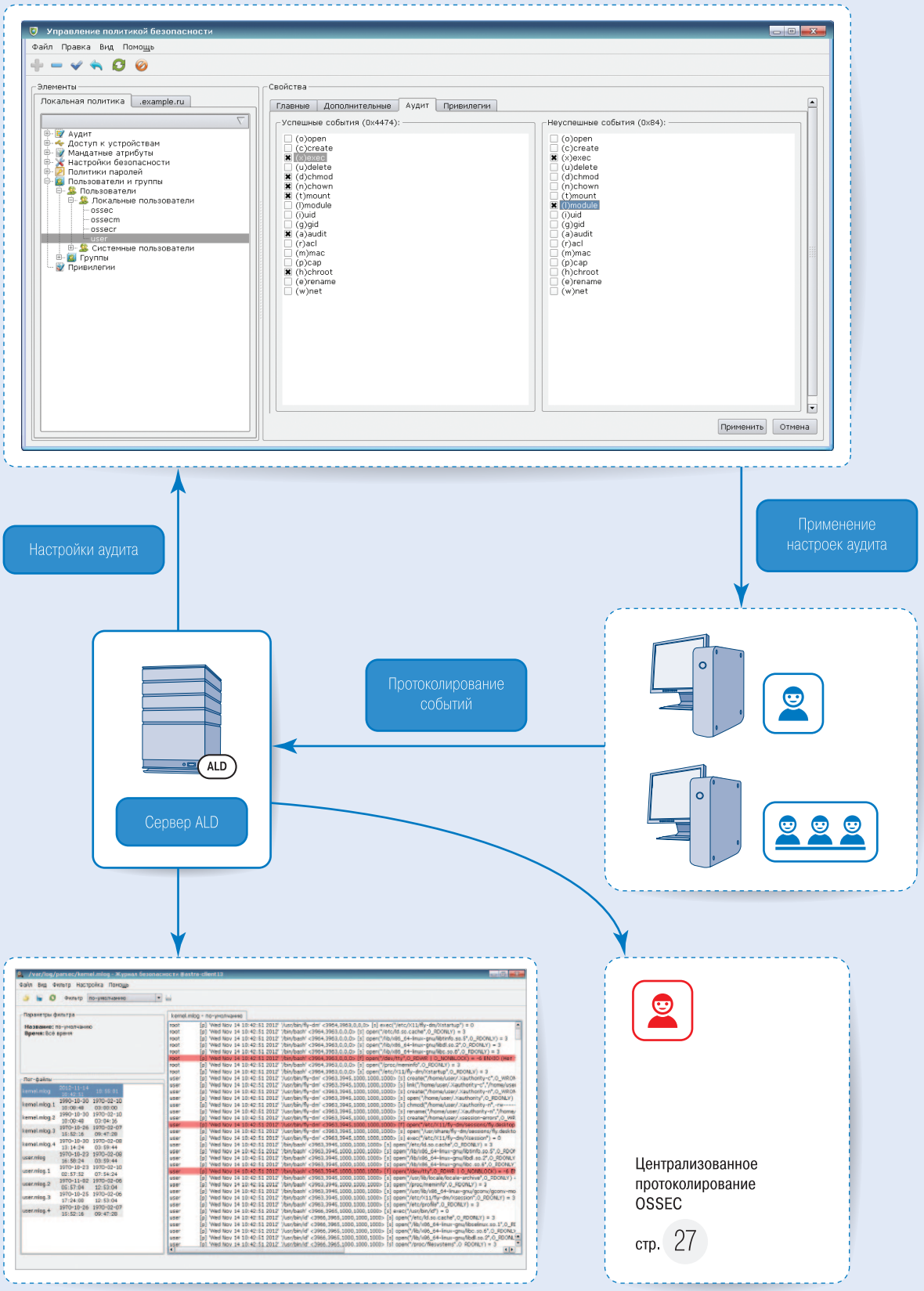
УТИЛИТЫ

Виды защищаемой информации

Коммерческая тайна | Персональные данные | Государственная тайна

АУДИТ И ЖУРНАЛИРОВАНИЕ СОБЫТИЙ

НАСТРОЙКА ПАРАМЕТРОВ АУДИТА

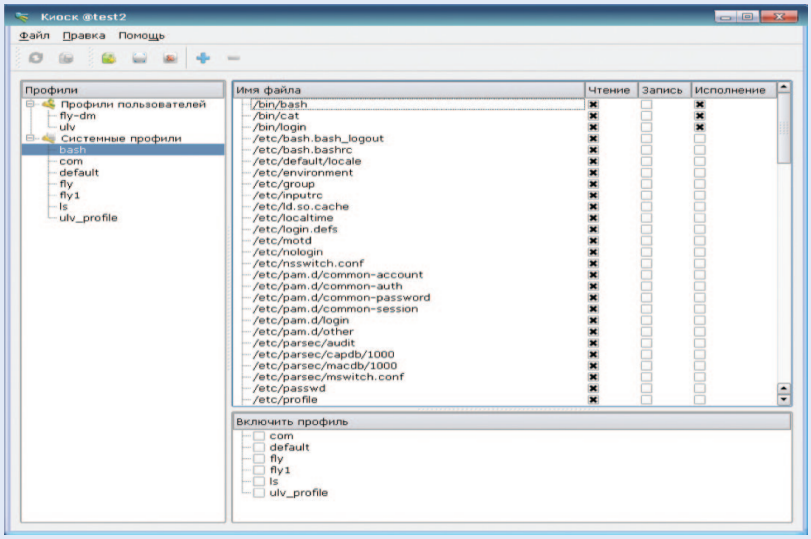


стр. 27

РЕЖИМ «КИОСК»

РЕЖИМ «КИОСК»

Режим «киоск» служит для ограничения прав пользователей в системе. Степень этих ограничений задается маской «киоск», которая накладывается на права доступа к файлу и проверяется при любой попытке пользователя получить к нему доступ. Маска «киоск» применяется только к обычным файлам. К директориям, сокетам и т. д. маска не применяется.



В режиме «киоск» пользователь не имеет возможности запустить ни одну системную программу, так как эти действия замаскированы (запрещены). В ОС СН предусмотрены средства, которые позволяют устанавливать и задавать права доступа пользователя к определенным файлам и приложениям.

РАБОТА В ТЕРМИНАЛЬНОМ РЕЖИМЕ

ТОНКИЕ КЛИЕНТЫ

Организация сетевой работы посредством размещения всех пользовательских приложений и данных в Едином пространстве пользователей, доступ к которому осуществляется с компьютеров-терминалов.

ТОНКИЕ КЛИЕНТЫ С АПМДЗ

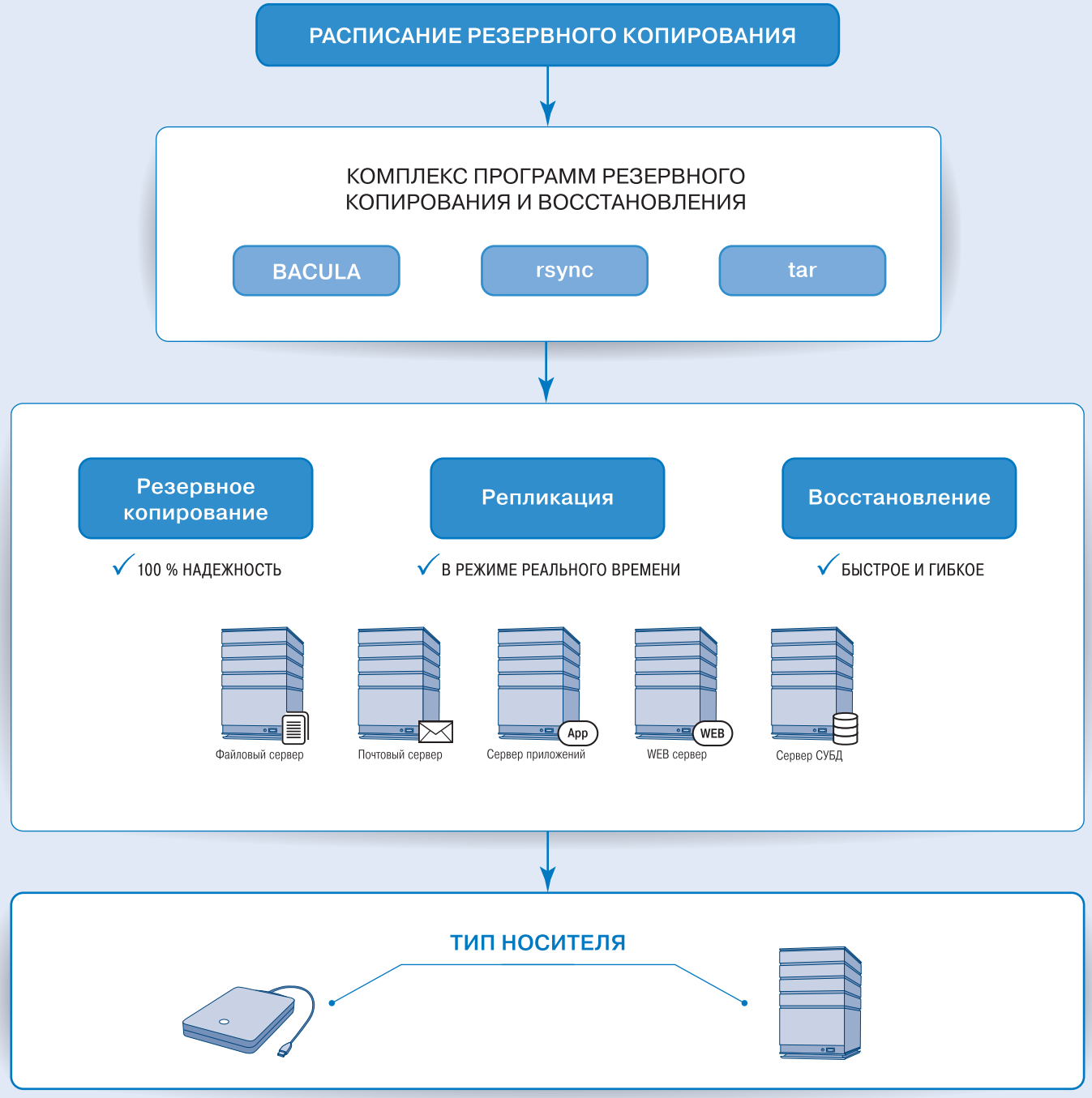
Ключевой особенностью данного решения является уменьшение нагрузки на ЛВС предприятия, т.к образ операционной сети не загружается с терминального сервера, а загружается с доверенного носителя АПМДЗ.

Подробнее на стр.36

РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

Для решения задачи надежного восстановления в результате сбоев и отказов оборудования в ОС СН реализованы:

- ✓ автоматическое выполнение в процессе перезагрузки после сбоя программы проверки и восстановления файловой системы;
- ✓ средства резервного копирования и восстановления операционной системы;
- ✓ средства резервного копирования и восстановления СУБД.

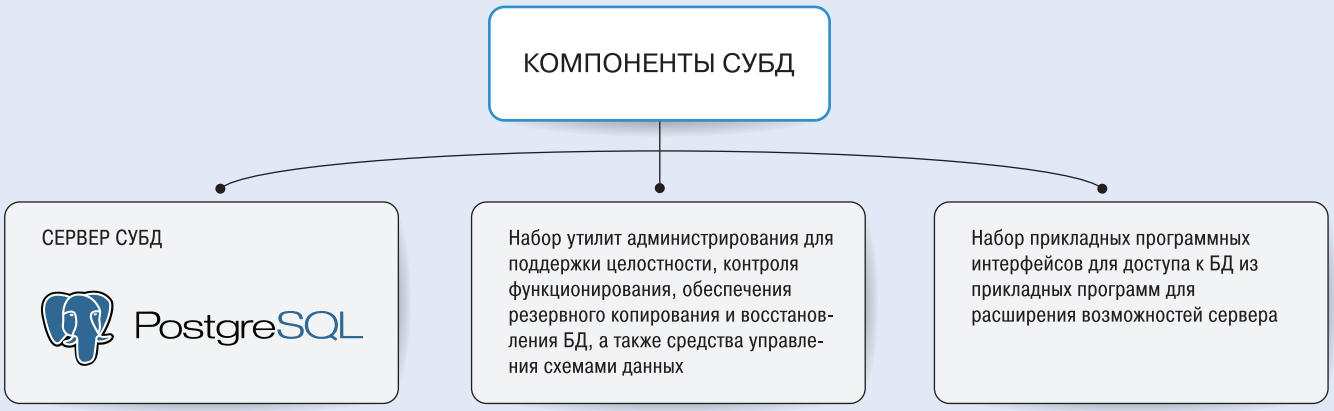


ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

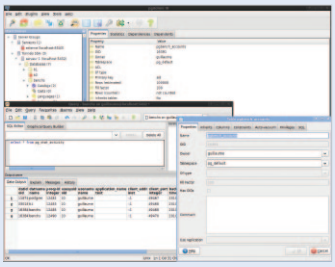
Защищенная система управления базами данных из состава операционной системы специального назначения «Astra Linux Special Edition» с интегрированными средствами защиты информации (далее – СУБД) предназначена для создания информационных и управляющих систем для работы как с конфиденциальной информацией, так и с информацией, содержащей сведения, составляющие государственную тайну.

СУБД построена на основе открытой архитектуры и поддерживает большинство современных технологий организации, хранения и управления данными на основе реляционной модели, включая стандартные и расширенные инструкции SQL, хранимые процедуры, вложенные запросы, управление транзакциями, расширенный состав типов хранимых данных и использование типов, определенных пользователем. Помимо этого, СУБД обеспечивает хранение и работу с XML документами и поддерживает полнотекстовый поиск.



ПОДДЕРЖКА КОНФИДЕНЦИАЛЬНОСТИ ХРАНИМЫХ ДАННЫХ

- ✓ защищенность по третьему классу защиты информации от НСД для средств вычислительной техники (СВТ) и второму уровню контроля отсутствия недекларированных возможностей (НДВ) по требованиям руководящих документов по обеспечению защиты информации;
- ✓ идентификация и аутентификация субъектов доступа для получения доступа к БД централизованными средствами управления доступа операционной системы;
- ✓ дискреционное разграничение доступа субъектов доступа к объектам БД (таблицы, схемы, функции, триггеры, подключаемые языки задания функций, виды, счетчики);
- ✓ мандатное разграничение доступа субъектов доступа к объектам БД (таблицы, виды);
- ✓ предотвращение возможностей несанкционированного ввода и вывода информации из БД;
- ✓ регистрация попыток доступа к СУБД и объектам БД;
- ✓ регистрация попыток изменения схем данных;
- ✓ регистрация попыток изменения правил разграничения доступа.



УТИЛИТА PGADMIN 3. Пользователями СУБД могут являться пользователи домена Astra Linux Direcory, что позволяет обеспечить доступ к серверам СУБД через сетевые сервисы (например, WEB-сервер) на основе единой политики безопасности информации с использованием сквозной аутентификации.

Виды защищаемой информации

Коммерческая тайна | Персональные данные | Государственная тайна

ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

КОНТРОЛЬ И ОБЕСПЕЧЕНИЕ БЕСПЕРЕБОЙНОГО ФУНКЦИОНИРОВАНИЯ

- ✓ обеспечение целостности БД на уровне SQL;
- ✓ резервное копирование и восстановление БД;
- ✓ контроль функционирования;
- ✓ построение высоконадежных систем с использованием современных технологий репликации, кластеризации и балансировки нагрузки;
- ✓ протоколирование работы.

ХАРАКТЕРИСТИКИ POSTGRE SQL

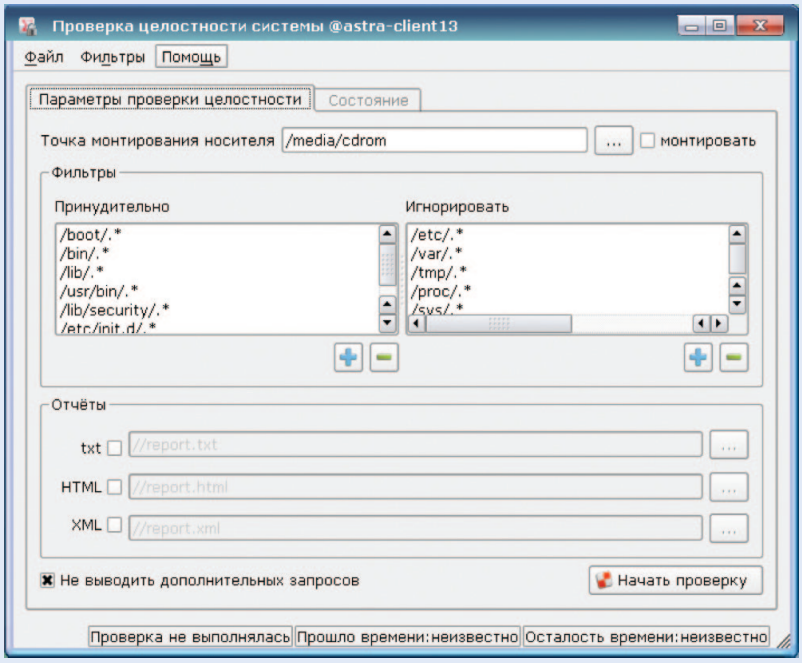
Максимальный размер БД	Не ограничен
Максимальный размер таблицы	32ТБ
Максимальный размер строки	1,6 ТБ
Максимальный размер поля	1ГБ
Максимальное количество строк в таблице	Не ограничено
Максимальное количество столбцов в таблице	250-1600
Максимальное количество индексов в таблице	Не ограничено
Соответствие стандартам SQL	ANSI-SQL:2011
Максимальная длина наименований объектов	Увеличена до 256 байт
Поддержка различных методов индексирования	compound, unique, partial, and functional : B-tree, R-tree, hash, GiST (Generalized Search Tree)
Поддержка средств создания хранимых процедур и триггеров	Java, Perl, Python, Ruby, Tcl, C/C++, PL/pgSQL
Поддержка интерфейсов средств разработки	Java (JDBC), ODBC, Perl, Python, Ruby, C, C++, PHP, Lisp, Scheme, Qt
Обеспечение отказоустойчивости	Резервное копирование и восстановление. Асинхронная и синхронная репликация данных (в том числе и двунаправленная).
Средства администрирования	Утилиты коммандной строки администрирования. Графическая утилита разработки БД и управления доступом.
Механизмы аутентификации	- парольная, LDAP, RADIUS; - PAM (Pluggable Authentication Modules); - Ident, Peer; - Kerberos, SSPI, GSSAPI; - сертификаты.

ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

КОНТРОЛЬ ЦЕЛОСТНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ, ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В ОС СН реализован многоуровневый контроль целостности программного обеспечения:

- ДИСТРИБУТИВ
- ФАЙЛОВАЯ СИСТЕМА
- ЦИФРОВАЯ ПОДПИСЬ ИСПОЛНЯЕМЫХ ФАЙЛОВ
  Механизм создания замкнутой среды



Для контроля целостности разработана и включена в состав ОС СН библиотека libgost, в которой реализована функция хэширования (одностороннего криптографического преобразования) в соответствии с ГОСТ Р 34.11-94. Данная библиотека используется в средствах контроля целостности дистрибутива и в средствах контроля целостности файловой системы.

Контроль целостности дистрибутива обеспечивается методом расчета контрольной суммы и сравнения полученного значения с эталонным. Для обеспечения контроля целостности объектов файловой системы ОС СН (в том числе, средств защиты информации) в состав дистрибутива входит файл gostsums.txt со списком контрольных сумм всех файлов, входящих в пакеты программ дистрибутива. Процесс генерации содержимого этого файла интегрирован в процесс производства диска с дистрибутивом ОС СН. Для выполнения проверки соответствия контрольных сумм файлов в системе эталонным контрольным суммам разработана специальная графическая утилита «fly-admin-int-check».

Кроме того, контроль целостности операционной системы, прикладного программного обеспечения и средств защиты информации обеспечивается набором программных средств, который предоставляет возможность периодического (с использованием системного планировщика заданий «cron») вычисления контрольных сумм файлов и соответствующих им атрибутов с последующим сравнением полученных значений с эталонными.

В ОС СН реализован механизм, обеспечивающий проверку неизменности и подлинности загружаемых исполняемых файлов в формате ELF (Executable and Linkable Format). Проверка производится на основе цифровой подписи, реализованной в соответствии с ГОСТ Р 34.10-2001 и внедряемой в исполняемые ELF-файлы в процессе сборки ОС СН.

Предусмотрена возможность предоставления сторонним разработчикам средств для внедрения цифровой подписи в исполняемые файлы разрабатываемого ими программного обеспечения.

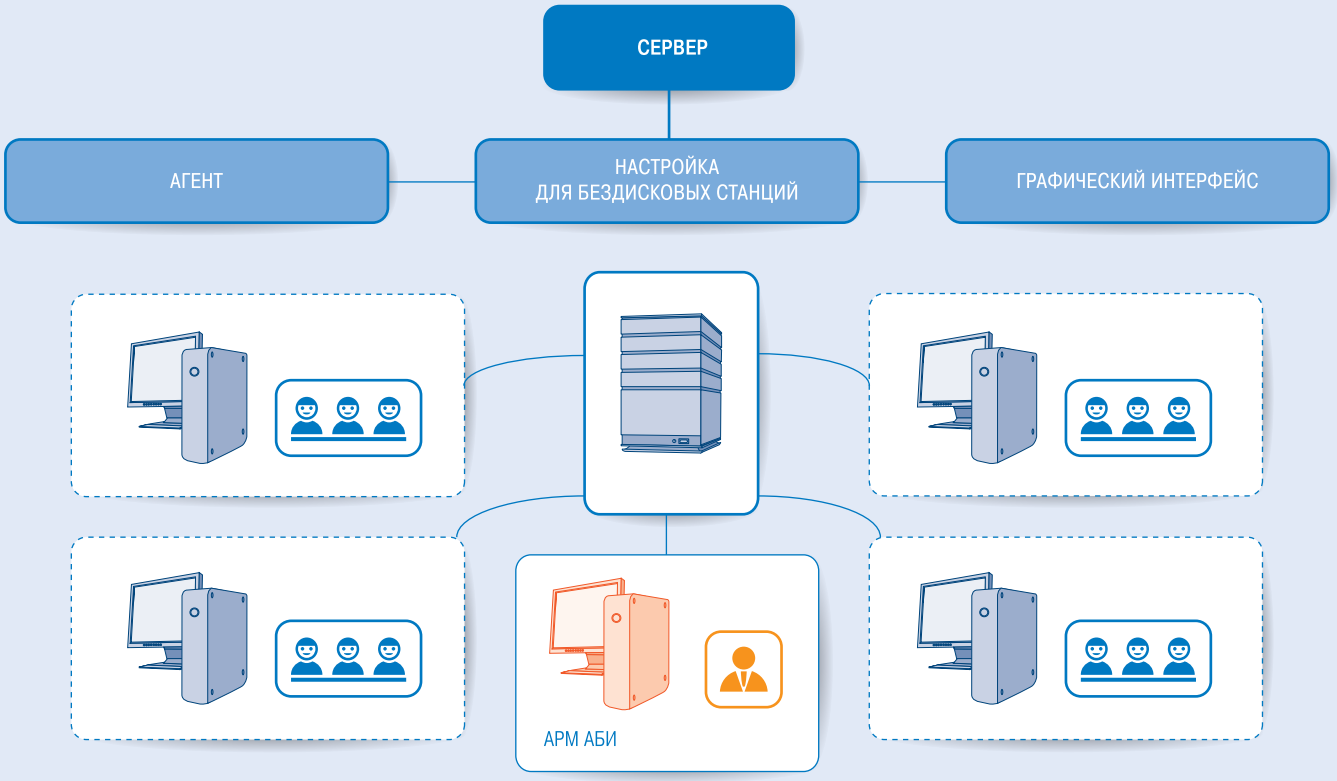
Виды защищаемой информации

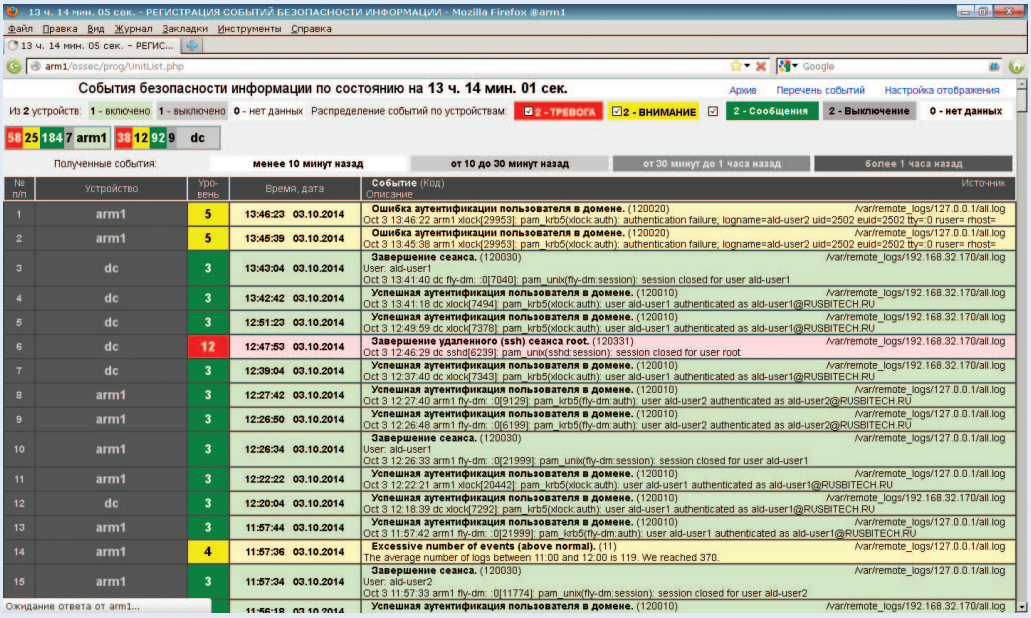
Коммерческая тайна | Персональные данные | Государственная тайна

СРЕДСТВА ЦЕНТРАЛИЗОВАННОГО ПРОТОКОЛИРОВАНИЯ

В ОС СН реализована собственная подсистема протоколирования, осуществляющая регистрацию событий в двоичные файлы. В библиотеках безопасности реализован прикладной программный интерфейс для использования подсистемы протоколирования. Средства централизованного аудита обеспечивают сбор и представление администратору безопасности сети информации о событиях безопасности в автоматизированной системе.

Для решения задач централизованного сбора и анализа журналов протоколирования (журналов аудита) в ОС СН реализованы:



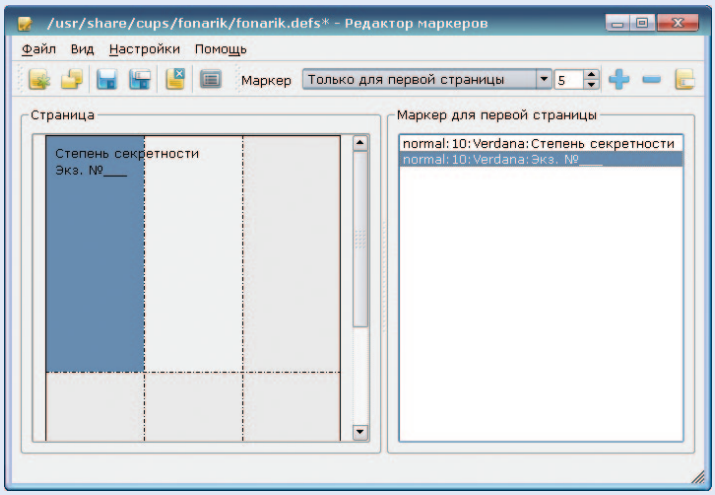


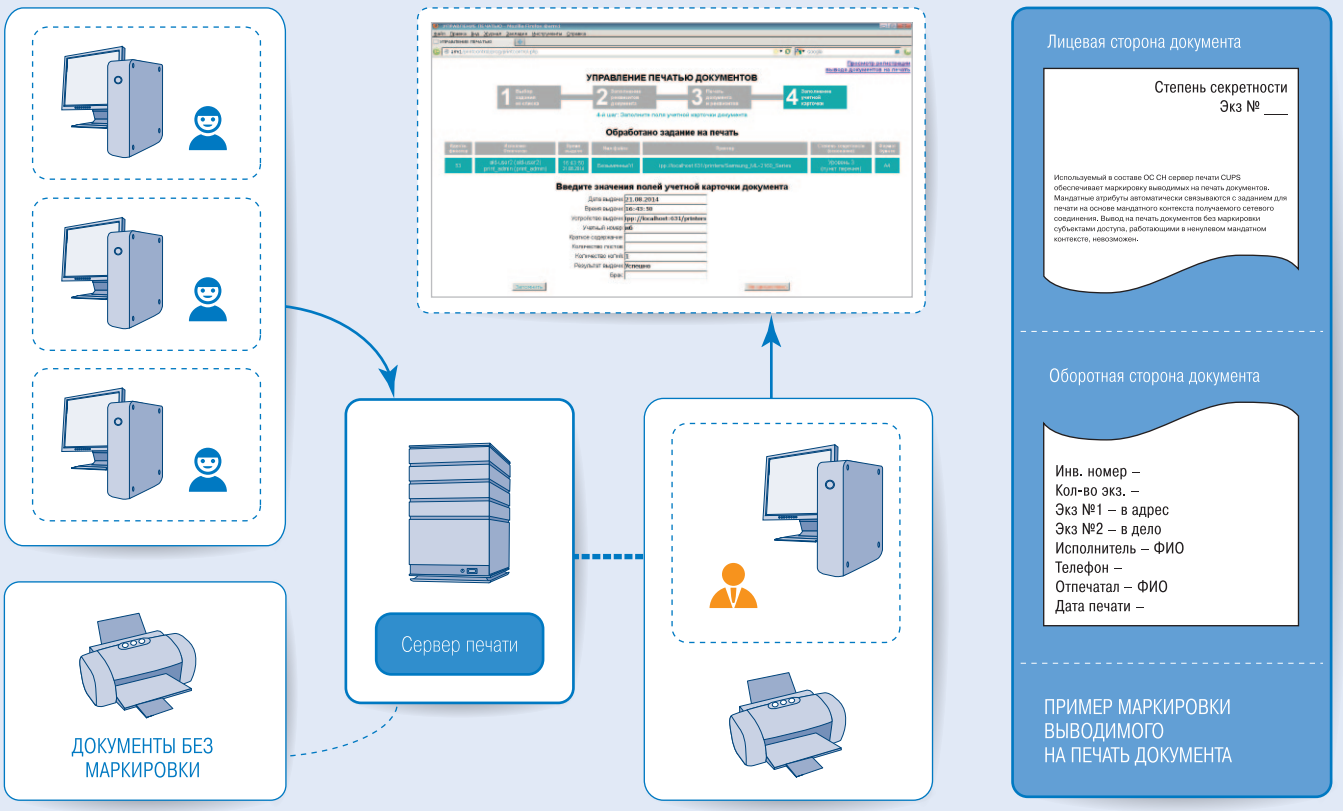
ПЕЧАТЬ И МАРКИРОВКА ДОКУМЕНТОВ

ЗАЩИЩЕННЫЙ КОМПЛЕКС ПРОГРАММ ПЕЧАТИ И МАРКИРОВКИ ДОКУМЕНТОВ

Решение задачи маркировки документов при выводе на печать основано на использовании защищенного сервера печати. Мандатные атрибуты автоматически связываются с заданием печати на основе мандатного контекста сетевого соединения. Вывод на печать документов без маркировки возможен только в нулевом мандатном контексте.

Маркировка документов осуществляется при печати документов на основе модифицируемых файлов шаблонов, содержащих информацию об атрибутах маркировки и их положение на странице.





Виды защищаемой информации

Коммерческая тайна	Персональные данные	Государственная тайна

ГИПЕРТЕКСТОВАЯ ОБРАБОТКА ДАННЫХ

ЗАЩИЩЕННЫЙ КОМПЛЕКС ПРОГРАММ ГИПЕРТЕКСТОВОЙ ОБРАБОТКИ ДАННЫХ

Решение задачи гипертекстовой обработки данных реализовано с помощью использования защищенного комплекса программ, который включает в себя web-сервер Apache и браузер Mozilla Firefox, доработанные для интеграции с ядром и базовыми библиотеками ОС СН с целью обеспечения мандатного разграничения доступа при организации удаленного доступа к информационным ресурсам в информационных и управляющих системах, в которых осуществляется хранение, обработка и передача информации ограниченного доступа.

При обслуживании запросов пользователей web-сервер переключается в соответствующий мандатный контекст безопасности пользователя. Доступ к защищаемой информации разграничивается средствами расширенной подсистемы безопасности PARSEC.

ИНТЕГРАЦИЯ С ЯДРОМ ОС СН И БАЗОВЫМИ БИБЛИОТЕКАМИ ДЛЯ ОБЕСПЕЧЕНИЯ РАЗГРАНИЧЕНИЯ ДОСТУПА

РЕАЛИЗАЦИЯ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ

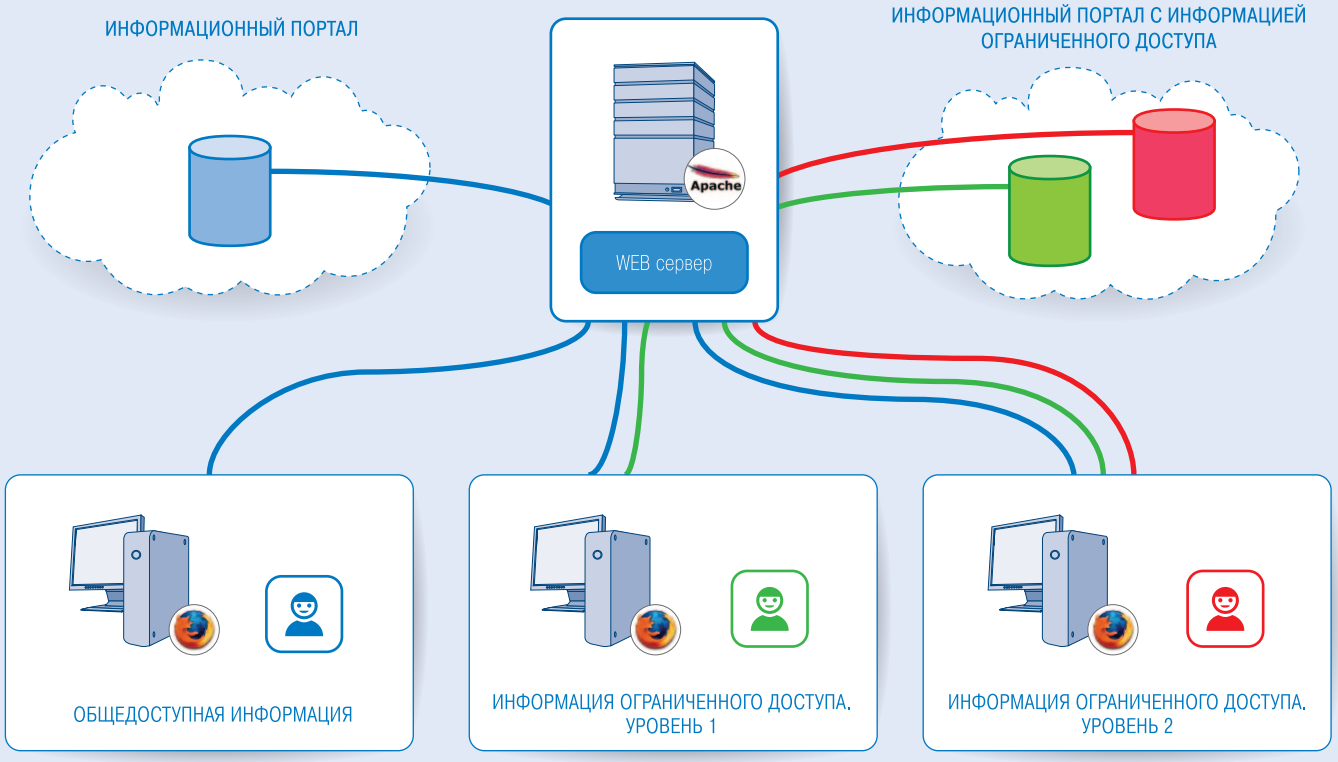
Серверная часть

Apache

Надёжный и гибкий в конфигурации HTTP-сервер, который позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д.

Клиентская часть

Браузер с широкими возможностями настройки: пользователь может устанавливать дополнительные темы, изменяющие внешний вид программы, плагины и расширения, добавляющие новый функционал.



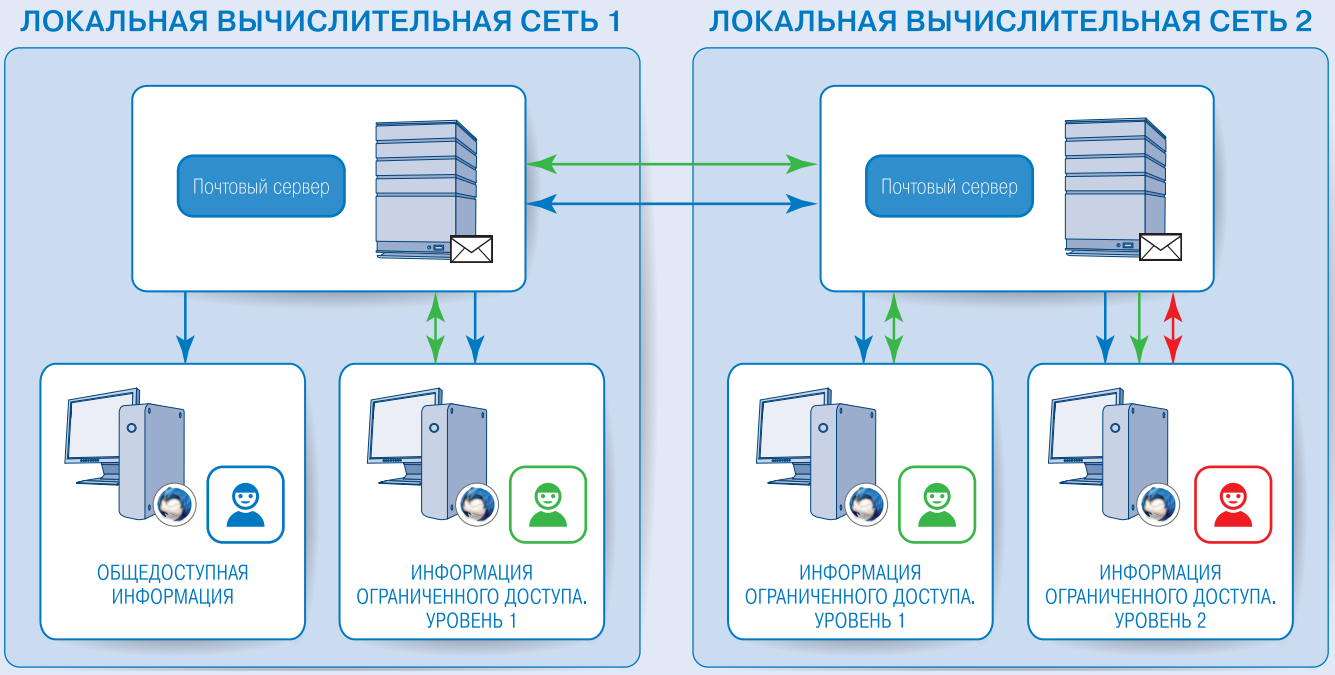
Виды защищаемой информации

Коммерческая тайна | Персональные данные | Государственная тайна

ЭЛЕКТРОННАЯ ПОЧТА

ЗАЩИЩЕННЫЙ КОМПЛЕКС ПРОГРАММ ЭЛЕКТРОННОЙ ПОЧТЫ

Решение задачи обмена сообщениями электронной почты реализовано на основе защищенного комплекса программ электронной почты. Используется сервер электронной почты, состоящий из агента передачи электронной почты Exim4, агента доставки электронной почты Dovecot и клиента электронной почты Thunderbird, доработанных для реализации следующих дополнительных функциональных возможностей:



Защищенный комплекс электронной почты обеспечивает идентификацию и аутентификацию доменных пользователей.

РЕАЛИЗОВАННЫЕ ФУНКЦИИ СЗИ ОТ НСД

ИЗОЛЯЦИЯ МОДУЛЕЙ

Ядро ОС СН обеспечивает собственное изолированное адресное пространство для каждого процесса в системе. Такой механизм изоляции основан на страничном механизме защиты памяти, а также на механизме трансляции виртуального адреса в физический, поддерживаемый модулем управления памятью.

РЕАЛИЗОВАННЫЕ ФУНКЦИИ СЗИ ОТ НСД

ОЧИСТКА ОПЕРАТИВНОЙ И ВНЕШНЕЙ ПАМЯТИ С ГАРАНТИРОВАННЫМ УДАЛЕНИЕМ ФАЙЛОВ

Ядро ОС СН гарантирует, что обычный непривилегированный процесс не получит данные чужого процесса, если это явно не разрешено правилами разграничения доступа. Это означает, что средства межпроцессного взаимодействия контролируются с помощью правил разграничения доступа, и процесс не может получить неочищенную память (как оперативную, так и дисковую).

В ОС СН реализована очистка неиспользуемых блоков файловой системы непосредственно при их освобождении.

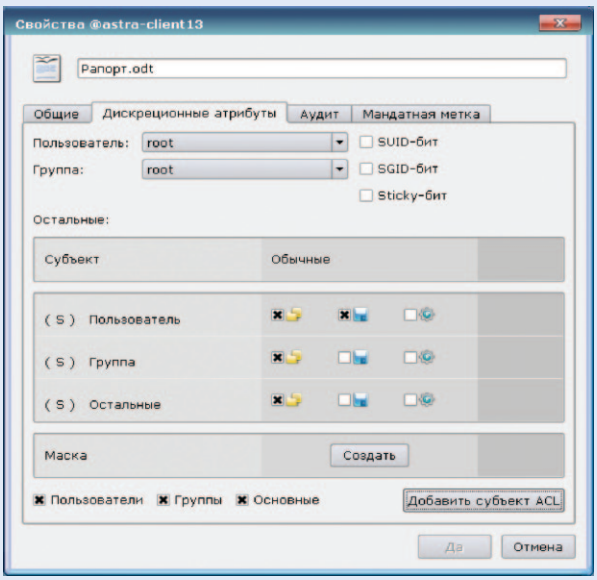
ЗАЩИТА РАБОЧЕЙ ПАМЯТИ («СТЕК» И «КУЧА») ОТ ВЫПОЛНЕНИЯ

В ОС СН для исполняемых файлов используется формат, позволяющий установить режим доступа к сегментам в адресном пространстве процесса: чтение, запись и выполнение. Централизованная система сборки программного обеспечения гарантирует установку минимального режима, необходимого для функционирования программного обеспечения. Например, для сегмента кода установлен режим «чтение и выполнение», для сегментов «стек» и «куча» – режим «чтение и запись». Кроме того, существует возможность использования технологии NOT EXECUTE BIT, поддерживаемой современными процессорами.

РЕАЛИЗОВАННЫЕ ФУНКЦИИ СЗИ ОТ НСД

ДИСКРЕЦИОННОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА

Механизм дискреционного разграничения доступа обеспечивает проверку дискреционных правил разграничения доступа (ДПРД), формируемых в виде базовых правил разграничения доступа (ПРД) ОС семейства Linux, формируемых в виде идентификаторов субъектов (идентификатор пользователя — UID и идентификатор группы — GID), имеющих доступ к объекту (чтение, запись, исполнение). Кроме того, для формирования ДПРД используются списки контроля доступа (Access control list — ACL) и механизм системных привилегий ОС семейства Linux.

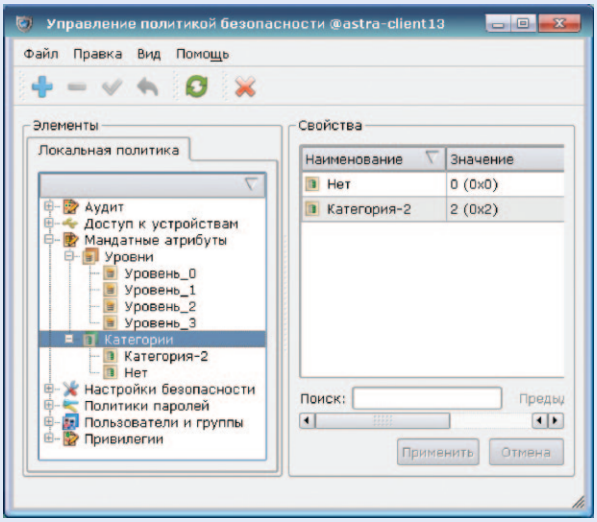


В состав ОС СН входят защищенные комплексы программ СУБД, электронной почты и гипертекстовой обработки данных.

В защищенных комплексах программ электронной почты и гипертекстовой обработки данных защищаемыми объектами являются объекты файловой системы. Дискреционное разграничение доступа к ним обеспечивается также, как и к прочим объектам файловой системы.

МАНДАТНОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА

Механизм мандатного разграничения доступа реализован, как и механизм дискреционного разграничения доступа, в ядре ОС и СУБД. Решение о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (чтение, запись, исполнение), мандатного контекста безопасности, связанного с каждым субъектом, и мандатной метки, связанной с объектом.



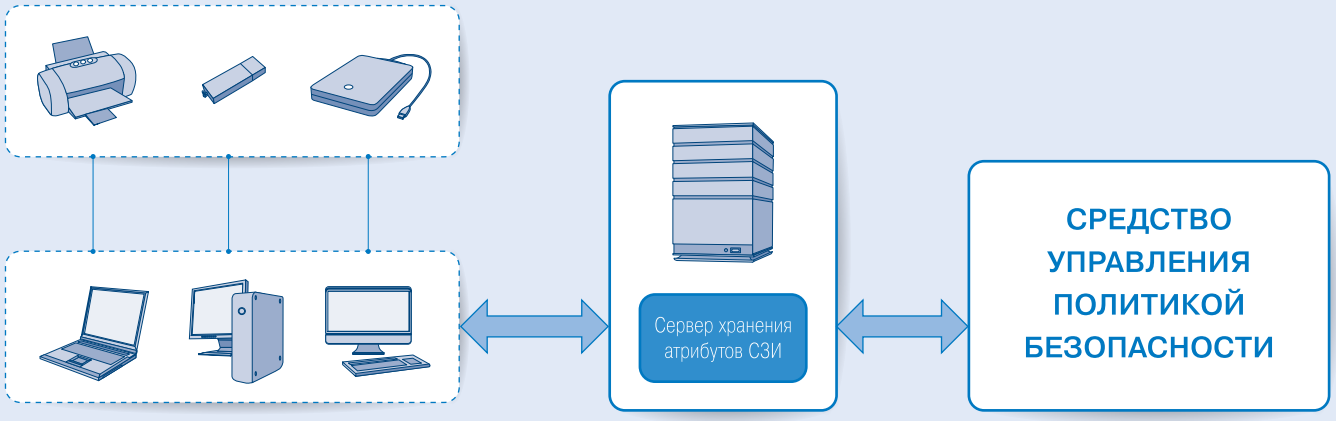
Сетевые соединения рассматриваются как средство межпроцессного взаимодействия, поэтому должны подвергаться мандатному контролю доступа. Для этого в сетевые пакеты протокола IPv4 в соответствии со стандартом RFC1108 внедряются мандатные метки, соответствующие метке объекта (сокета).

Мандатное разграничение доступа в защищенных комплексах программ гипертекстовой обработки данных, электронной почты и в других сервисах реализовано на основе программного интерфейса библиотек подсистемы безопасности PARSEC.

РАЗГРАНИЧЕНИЕ ДОСТУПА К ВНЕШНИМ УСТРОЙСТВАМ

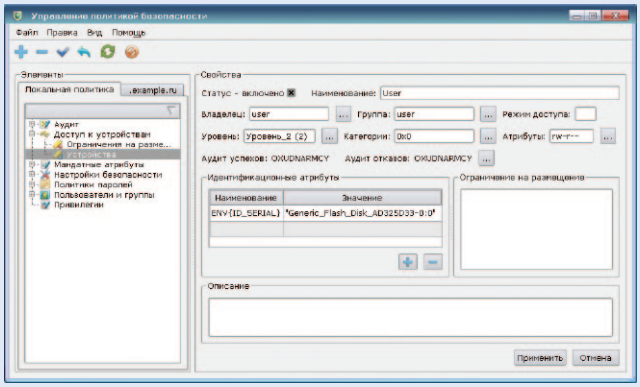
СРЕДСТВА РАЗГРАНИЧЕНИЯ ДОСТУПА К ВНЕШНИМ УСТРОЙСТВАМ

Оригинальная система разграничения доступа к внешним съемным устройствам предназначена для предотвращения несанкционированного подключения пользователями внешних устройств.



СРЕДСТВО УПРАВЛЕНИЯ ПОЛИТИКОЙ БЕЗОПАСНОСТИ

Обеспечивает учет подключаемых устройств и съемных носителей в системе, установку дискреционных и мандатных атрибутов доступа пользователей к устройствам и создание дополнительных правил доступа к устройству (например, ограничение на подключение устройства только в определенный USB-порт)



АЛГОРИТМ ДОСТУПА УЧТЕННОГО УСТРОЙСТВА К ИНФОРМАЦИИ

Мандатный уровень flash накопителя

Мандатный уровень документа	0	1	2	3
0	Ч З М	М	М	М
1	Ч М	Ч З М	М	М
2	Ч М	Ч М	Ч З М	М
3	Ч М	Ч М	Ч М	Ч З М

Ч – чтение
З – запись
М – монтирование

СРЕДСТВА ОГРАНИЧЕНИЯ ПРАВ ДОСТУПА К СТРАНИЦАМ ПАМЯТИ

Средства ограничения прав доступа к страницам памяти реализованы на основе набора изменений PaX для ядра операционной системы, который обеспечивает предоставление наименьших привилегий для процессов при доступе к сегментам памяти в собственном адресном пространстве.

Главной функциональной возможностью набора изменений PaX для ядра операционной системы является защита исполняемого кода в адресном пространстве. Эта защита использует технологии бита запрета исполнения в процессоре (NX-бит) для предотвращения выполнения произвольного кода.

РЕШАЕМЫЕ ЗАДАЧИ

- ИНТЕГРАЦИЯ С ЯДРОМ ОС СН И БАЗОВЫМИ БИБЛИОТЕКАМИ ДЛЯ ОБЕСПЕЧЕНИЯ РАЗГРАНИЧЕНИЯ ДОСТУПА
- ЗАПРЕТ СОЗДАНИЯ ИСПОЛНЯЕМЫХ ОБЛАСТЕЙ ПАМЯТИ
- ЗАПРЕТ ПЕРЕМЕЩЕНИЯ СЕГМЕНТА КОДА
- ЗАПРЕТ СОЗДАНИЯ ИСПОЛНЯЕМОГО СТЕКА
- РАНДОМИЗАЦИЯ АДРЕСНОГО ПРОСТРАНСТВА ПРОЦЕССА

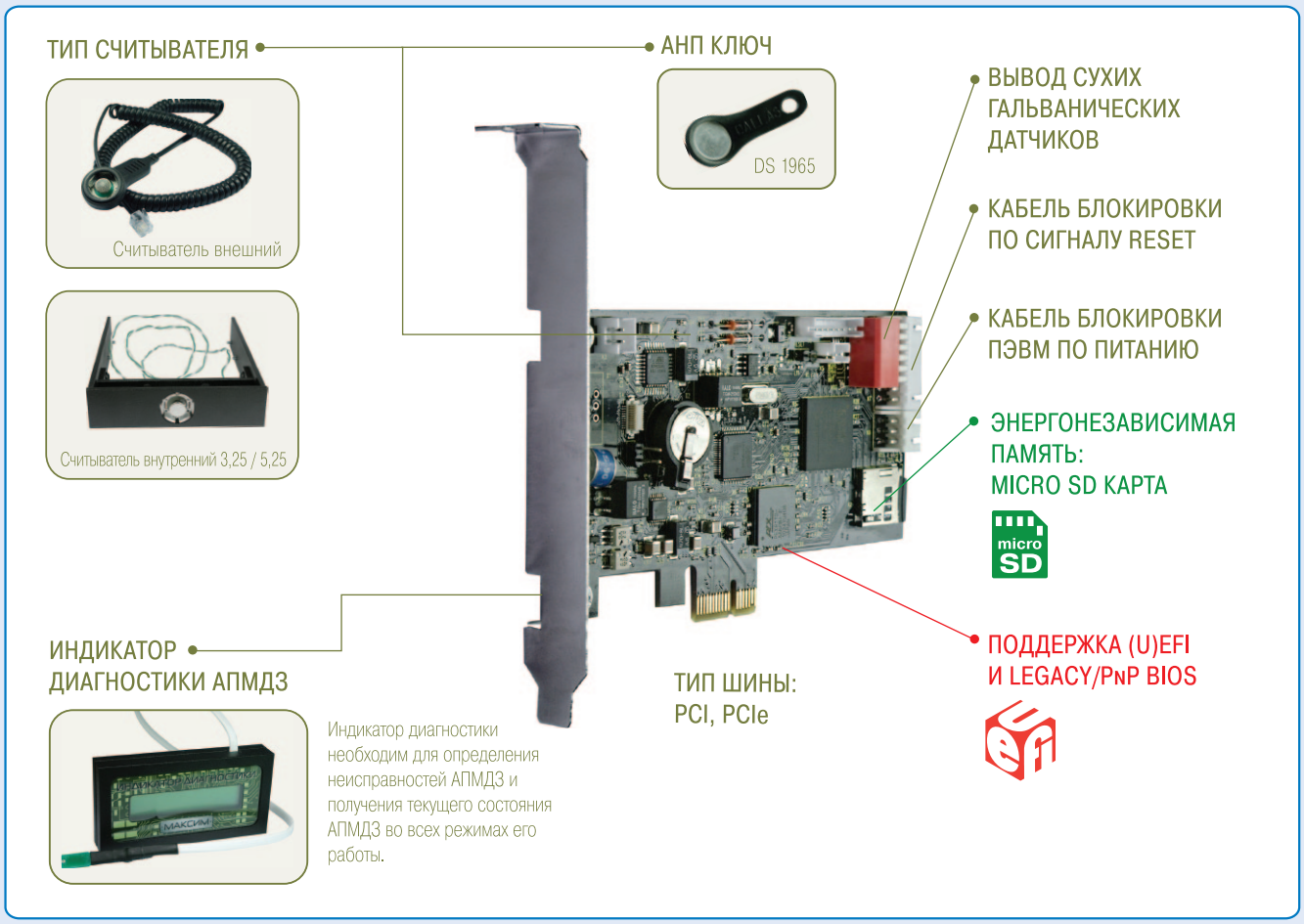
Набор изменений PaX предотвращает выполнение произвольного кода на основе контроля доступа к сегментам памяти следующих типов: «чтение», «запись», «исполнение» – или их комбинации. Комбинация «запись» и «исполнение» запрещена.

ПРИМЕНЕНИЕ ОС СН С АПМДЗ «МАКСИМ-М1»

АПМДЗ «МАКСИМ-М1» (изделие М-643М1) — аппаратно-программный модуль доверенной загрузки, обеспечивающий защиту от НСД к информации до степени секретности «совершенно секретно» включительно, обрабатываемой на рабочей станции, путем обеспечения загрузки доверенной ОС и реализации надежного контроля доступа к техническим средствам рабочей станции.

АПМДЗ «МАКСИМ-М1» соответствует требованиям ФСБ России к АПМДЗ ЭВМ по классу 1Б. Сертификат соответствия № СФ/027-1879 от 29 июня 2012 г.

КОМПЛЕКТ ПОСТАВКИ АПМДЗ «МАКСИМ-М1»



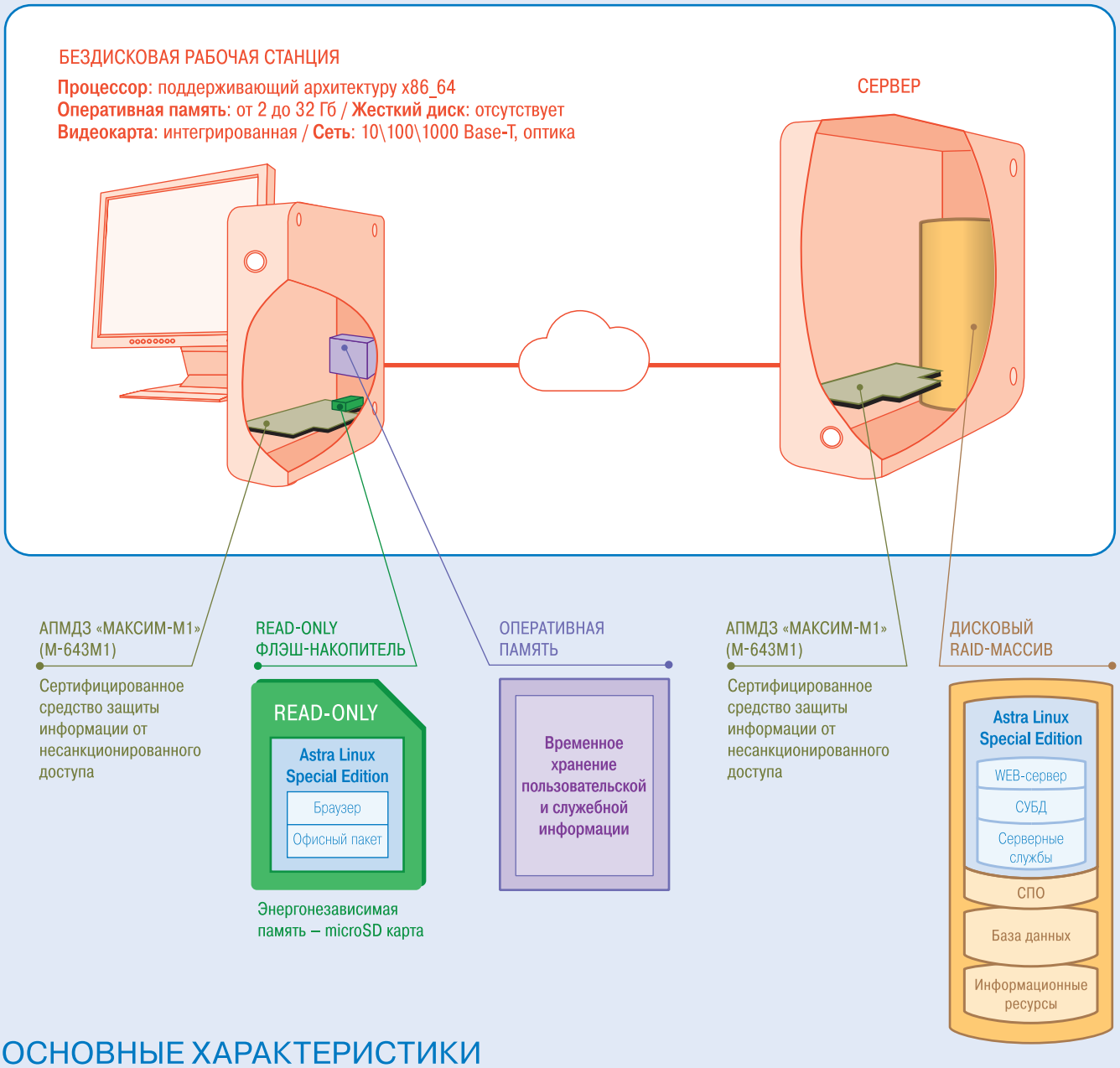
ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- ✓ двухфакторная идентификация и аутентификация пользователей до загрузки ОС;
- ✓ ведение защищенных от стирания журналов регистрации событий;
- ✓ контроль целостности областей оперативной памяти;
- ✓ контроль целостности служебных областей жестких дисков;
- ✓ контроль целостности файлов и служебного журнала для файловых систем FAT16/FAT32/NTFS/Ext2/Ext3/Ext4;
- ✓ поддержка форматов таблиц MBR/GPT жестких дисков.

ПРИМЕР СОЗДАНИЯ БЕЗДИСКОВЫХ РАБОЧИХ СТАНЦИЙ

Унифицированное решение предназначено для создания защищенных автоматизированных систем, обрабатывающих информацию до грифа «совершенно секретно» включительно.

Ключевой особенностью комплекса является отсутствие на носителях информации ограниченного доступа (вся информация хранится на сервере).



ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

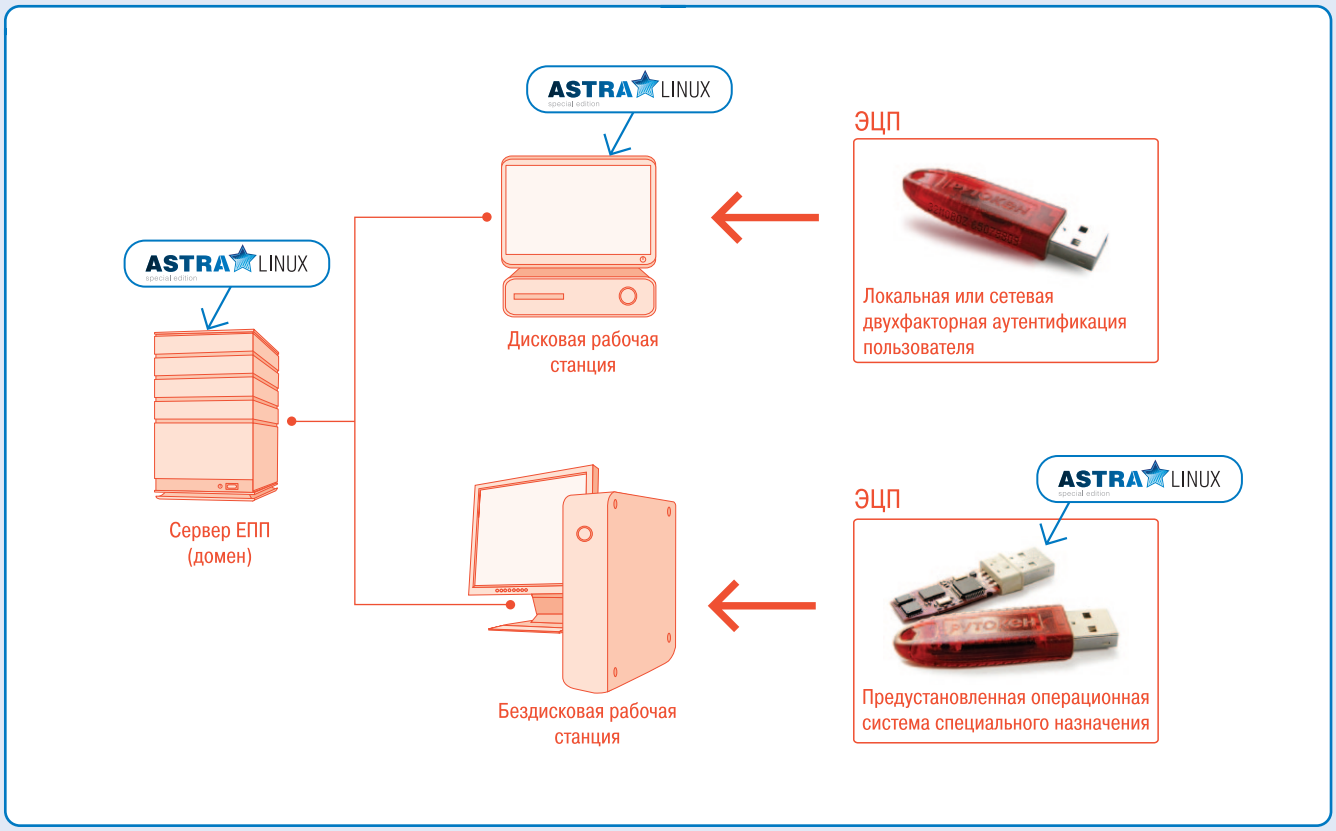
- ✓ модульная аппаратная и программная платформа;
- ✓ средства защиты информации, сертифицированные ФСБ России, ФСТЭК России и Минобороны России;
- ✓ мобильность и компактность;
- ✓ высокая производительность;
- ✓ бездисковая рабочая станция;
- ✓ легкость организации рабочего места;
- ✓ быстрая замена АРМ в случае поломки.

Виды защищаемой информации

Коммерческая тайна | Персональные данные | Государственная тайна

ЗАГРУЗКА И РАБОТА ДОВЕРЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ

Загрузка ОС СН «Astra Linux Special Edition» с флэш-накопителя предназначена для безопасного доступа пользователей в информационные системы, а также для создания бездисковых рабочих станций.



- ✓ Загрузка и работа доверенной среды с флэш-накопителя
- ✓ Двухфакторная аутентификация пользователя
- ✓ Мобильность и компактность
- ✓ Создание бездисковых рабочих станций

В настоящий момент это решение реализовано на основе выпускаемых компанией Актив-Софт идентификаторов «Rutoken», которые служат для строгой двухфакторной аутентификации, защиты электронной переписки, установления защищенных соединений (VPN, SSL), проведения финансовых транзакций и криптографической защиты информации. Другая разновидность идентификатора «Rutoken RF» позволяет одновременно использовать его как для доступа в помещения, так и к ресурсам автоматизированных систем.

ОБУЧЕНИЕ

Обучение предназначено для выработки у сотрудников навыков по эффективному решению задач администрирования операционной системы специального назначения «Astra Linux Special Edition». Во время обучения рассматриваются основы администрирования, управление ресурсами и сетевым взаимодействием, построение защищенных информационных систем, а также механизмы обеспечения безопасности систем под управлением ОС СН. Обучение проводится специалистами практиками ЗАО «НПО «Эшелон» при сотрудничестве со специалистами ОАО «НПО «РусБИТех».

Программа обучения утверждена Министерством обороны Российской Федерации: 015. Администрирование операционной системы специального назначения «Astra Linux Special Edition»

ПРОГРАММА КУРСА

Раздел 1. Основы администрирования ОС СН «Astra Linux Special Edition»
- Инсталляция ОС СН
- Загрузка и завершение работы ОС СН
- Базовые команды администрирования

Раздел 2. Управление ресурсами ОС СН «Astra Linux Special Edition»
- Управление процессами в ОС СН
- Файловая система ОС СН
- Управление пользователями
- Планирование запуска процессов
- Резервное копирование
- Syslog и файлы журналов

Раздел 3. Управление сетевым взаимодействием в ОС СН «Astra Linux Special Edition»
- Работа с сетевыми интерфейсами
- Маршрутизация
- Система доменных имен
- Организация электронной почты

Раздел 4. Построение защищенных информационных систем на базе ОС СН «Astra Linux Special Edition»
- Развертывание защищенного Web-сервера на основе Apache
- Конфигурация системы управления базами данных PostgreSQL

Раздел 5. Механизмы обеспечения безопасности систем под управлением ОС СН «Astra Linux Special Edition»
- Базовые механизмы безопасности в ОС Linux
- Ключевые особенности ОС СН «Astra Linux Special Edition» по реализации требований безопасности информации
- Межсетевое экранирование в ОС Linux
- Тестирование защищенности информационных систем под управлением ОС СН«Astra Linux Special Edition»

КОНТАКТЫ ЦЕНТРА ОБУЧЕНИЯ

Адрес: 107023, г. Москва, ул. Электрозаводская, д. 24
Многоканальный телефон: +7(495) 223-23-92 (доб. 342)
Бесплатный звонок из любого региона России: 8-800-100-05-02 (доб. 342)

УСЛОВИЯ ЛИЦЕНЗИРОВАНИЯ И КОМПЛЕКТ ПОСТАВКИ

Приобретение программного продукта — это приобретение лицензии (неисключительного права) на его использование по принципу «одна лицензия на одно средство вычислительной техники».

- ✓ Дистрибутив не разделен на серверную часть и клиентскую версию. **Дистрибутив сертифицирован как единое целое.**
- ✓ **Не нужно отдельно лицензировать** службы\сервисы сервера и клиентские лицензии, обращающиеся к службам\сервисам серверов приложений, СУБД, электронной почты.
- ✓ **Срок предоставления лицензии** на право использования операционной системы — **НЕ ОГРАНИЧЕН**. Это означает, что не нужно ежегодно продлевать лицензию на право ее использования.

Поставляется в товарной упаковке в виде набора материальных носителей.
Цены действительны с 1 января по 31 декабря 2015 года.

Формат поставки			Стоимость	
			Конечный пользователь	Дистрибьютор / дилер
BOX		• Диск установочный • Диск с документацией • Формуляр	**21300* рублей** Дополнительный комплект лицензий: 11715* руб./лицензия	**17040* рублей**
OEM		• Диск установочный • Формуляр		**12780* рублей**
Средства разработки Подробнее на стр.20		• Диск со средствами разработки библиотеки компилятор GCC среда разработки Qt-Creator заголовочные файлы отладчик GDB утилиты	**1065 рублей**	**745.50 рублей**

* Лицензионное вознаграждение НДС не облагается на основании п/п 26 п. 2 ст. 149 Налогового кодекса Российской Федерации и указаний Минфина России.

ДИСК С ДОКУМЕНТАЦИЕЙ ВКЛЮЧАЕТ В СЕБЯ:

- Описание применения
- Руководство администратора
- Руководство по комплексу средств защиты (часть 1)
- Руководство пользователя
- Руководство администратора БД
- Руководство по комплексу средств защиты (часть 2)

Виды защищаемой информации

Коммерческая тайна	Персональные данные	Государственная тайна

ТЕСТИРОВАНИЕ И БЕСПЛАТНЫЕ ЛИЦЕНЗИИ

УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ ОС СН НА ТЕСТИРОВАНИЕ

Для оценки функциональности и возможности применения экземпляр ОС СН с документацией может быть предоставлен бесплатно на срок до 3-х месяцев на основании официального письма-запроса. Передаваемый экземпляр ОС СН изготавливается в соответствии с техническими условиями, проверяется ОТК и упаковывается после проведения приемо-сдаточных испытаний, предусмотренных техническими условиями. Экземпляру присваивается заводской номер, но формуляр при этом не выдается. При положительном решении и применении ОС СН формат коробки BOX может не возвращаться и после заключения соответствующего лицензионного договора (для конечного пользователя, дилера или дистрибьютора) последует передача формуляра с отметками ОТК в Ваш адрес. Экземпляр программы также может поставляться с приемкой «5». В лицензионном договоре также определяется дополнительное количество ЭВМ, на которых необходимо установить и эксплуатировать ОС СН с указанием стоимости лицензионного вознаграждения.

За более подробной информацией необходимо обращаться в отдел продаж.

Условия предоставления ОС СН на тестирование.

БЕСПЛАТНЫЕ ЛИЦЕНЗИИ ДЛЯ ВУЗОВ

ОАО «НПО РусБИТех» с 2013 года запустило специальную программу для государственных учебных заведений. Целью специальной программы является организация учебного процесса с использованием сертифицированной операционной системы специального назначения «Astra Linux Special Edition»

Для создания учебных классов осуществляется безвозмездное предоставление неисключительного права использования операционной системы. Службой технической поддержки оказывается содействие в вопросах установки и настройки операционной системы.

Операционная система поставляется путем заключения лицензионного договора о предоставлении неисключительного права на ее использование на необходимом количестве ЭВМ. Сам экземпляр операционной системы передается в товарной упаковке, в состав которой входит установочный диск и диск с эксплуатационной документацией.

За более подробной информацией необходимо обращаться в отдел продаж.

Условия предоставления бесплатных лицензий для ВУЗов, типовой лицензионный договор для ВУЗов, образец письма-запроса на получение бесплатных лицензий.

http://astralinux.ru/partners/vuzam.html

КОНТАКТНАЯ ИНФОРМАЦИЯ:

Сектор продаж / Тел.: +7 (495) 648-06-53 / Факс: +7 (495) 648-06-39 / E-mail: sales@rusbitech.ru

Служба техподдержки / Тел.: +7 (495) 648-15-30 / E-mail: support@rusbitech.ru

ПАРТНЕРЫ

ERP-системы

ООО «1С», г. Москва

ООО «Телеформ ИС», г. Москва

Корпорация «Галактика», г. Москва

Информационно-справочные системы

ЗАО «Кодекс», г.Санкт-Петербург

ЗАО «КонсультантПлюс», г.Москва

Системы управления базами данных

ЗАО НПП «РЕЛЭКС», г. Воронеж

SAP Hana
ООО «САП СНГ»

Компания «TMaxSoft», СУБД Tibero

Системы документооборота

ООО «Арта», г.Санкт-Петербург

(УЭК) Универсальные электронные карты

Группа компаний «ISBC», г. Зеленоград

«Группа компаний «Микрон», г. Зеленоград

Средства антивирусной защиты

ЗАО «Лаборатория Касперского», г. Москва

ООО «Доктор Веб», г.Москва

ASTRA LINUX special edition

ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Геоинформационные системы

ОАО «НИИАА», г.Москва

ЗАО КБ «Панорама», г.Москва

Системы IP-телефонии и видеоконференцсвязи

MIND, г. Москва

Компания «ITooLabs», г. Тула

Средства контроля защищенности

ООО «СЛ Девелопмент», г. Новосибирск

ЗАО НПО «Эшелон», г. Москва

Средства аутентификации

Компания «Аладдин Р.Д.», г. Москва

ЗАО «Актив-софт», г. Москва

Средства виртуализации и «облачные» решения

Северное ПКБ, г. Санкт-Петербург

Средства криптографической защиты

ОАО«ИнфоТеКС», г. Москва

ООО «КРИПТО-ПРО», г. Москва

ООО «ЛИССИ-Крипто», г. Юбилейный

КОНТАКТНАЯ ИНФОРМАЦИЯ

Виды защищаемой информации

Коммерческая тайна	Персональные данные	Государственная тайна

КОНТАКТЫ

На протяжении всего срока эксплуатации операционной системы специального назначения «Astra Linux Special Edition» Вы получаете бесплатную техническую поддержку по вопросам установки и первоначальной настройки.

ОТЕЧЕСТВЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION»

Особенности и основные функциональные возможности отечественной операционной системы

АППАРАТНО-ПРОГРАММНЫЙ МОДУЛЬ ДОВЕРЕННОЙ ЗАГРУЗКИ «МАКСИМ-М1»

Справка об особенностях и основных функциональных возможностях АПМДЗ «Максим-М1»

КОНТАКТНАЯ ИНФОРМАЦИЯ

СЕКТОР ПРОДАЖ

117105, г.Москва,
Варшавское ш., д.26
Тел.: +7 (495) 648-06-53
Факс: +7 (495) 648-06-39
E-mail: sales@rusbitech.ru
http://www.astra-linux.ru

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

117105, г.Москва,
Варшавское ш., д.26, стр.11
Тел.: +7 (495) 648-15-30
Факс: +7 (495) 648-06-39
E-mail: support@rusbitech.ru
http://www.astra-linux.ru

Научно-производственное объединение
РусБИТех
Открытое акционерное общество

ВАШ НАДЁЖНЫЙ И КОМПЕТЕНТНЫЙ ПАРТНЁР

117105, Россия, г. Москва, Варшавское шоссе, д. 26
Тел.: +7 (495) 648-06-40 / Факс.: +7 (495) 648-06-39
E-mail: mail@rusbitech.ru / Сайт: www.rusbitech.ru