



Научно-производственное объединение  
**РусБИТех**  
Акционерное общество

## СПРАВКА

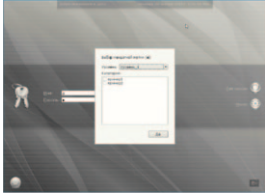
ОБ ОСОБЕННОСТЯХ И ОСНОВНЫХ  
ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЯХ  
ОПЕРАЦИОННОЙ СИСТЕМЫ



ОПЕРАЦИОННАЯ СИСТЕМА  
СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

**ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ**

15  
стр.



**ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС**

16  
стр.



**УПРАВЛЕНИЕ ПРОГРАММНЫМИ ПАКЕТАМИ**

18  
стр.



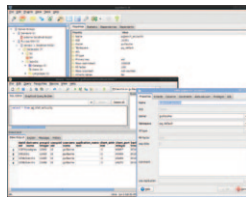
**НАДЕЖНОЕ ВОССТАНОВЛЕНИЕ ДАННЫХ**

22  
стр.



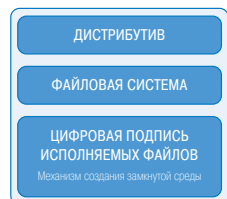
**ОБЕСПЕЧЕНИЕ ДОСТУПА К БД**

23  
стр.



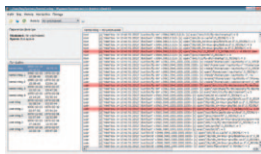
**КОНТРОЛЬ ЦЕЛОСТНОСТИ ДАННЫХ**

25  
стр.



**РЕГИСТРАЦИЯ СОБЫТИЙ**

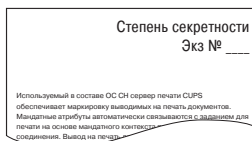
26  
стр.



**МАРКИРОВКА ДОКУМЕНТОВ ПРИ ВЫВОДЕ НА ПЕЧАТЬ**

27  
стр.

Лицевая сторона документа



**WEB-ТЕХНОЛОГИИ**

28  
стр.



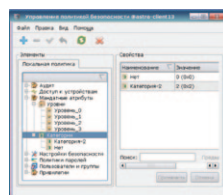
**ОБМЕН СООБЩЕНИЯМИ ЭЛЕКТРОННОЙ ПОЧТЫ**

29  
стр.



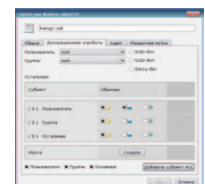
**МАНДАТНОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА**

31  
стр.



**ДИСКРЕЦИОННОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА**

31  
стр.



## СОДЕРЖАНИЕ

### ОБЩИЕ ПОЛОЖЕНИЯ

Назначение . . . . .	2
Сертификаты соответствия . . . . .	2
Патенты и свидетельства . . . . .	3
Заказчики . . . . .	4

### ПЛАТФОРМЫ И ОБЛАСТЬ ПРИМЕНЕНИЯ

Программные платформы . . . . .	6
Поддерживаемое оборудование . . . . .	6
Требования по защите информации от НСД для АС . . . . .	7
Область применения . . . . .	8

### СОСТАВ И ОСНОВНЫЕ КОМПОНЕНТЫ

Основные компоненты . . . . .	10
Особенности организации домена . . . . .	13
Сетевые средства . . . . .	14

### СЗИ ОТ НСД

Реализованные функции СЗИ от НСД . . . . .	30
Разграничение доступа к внешним устройствам . . . . .	32

### ВНЕДРЕНИЕ И ОБУЧЕНИЕ

Применение ОС СН с АПМДЗ «Максим-М1» . . . . .	34
Пример создания бездисковых рабочих станций . . . . .	35
АПМДЗ «Максим-А1» . . . . .	36
Загрузка и работа доверенной операционной системы . . . . .	38
Обучение . . . . .	39

### ВИРТУАЛИЗАЦИЯ

Виртуализация и управление . . . . .	40
--------------------------------------	----

### ПОСТАВКИ И ТЕСТИРОВАНИЕ

Условия предоставления ОС СН на тестирование . . . . .	42
Бесплатные лицензии для ВУЗов . . . . .	42

### КОНТАКТНАЯ ИНФОРМАЦИЯ

Сектор продаж . . . . .	42
Техническая поддержка . . . . .	42



## 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 недеklarированных возможностей согласно руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (Гостехкомиссия России, 1999 г.).

ОС СН может использоваться в составе автоматизированных систем класса защищенности до 1Б включительно, обрабатывающих информацию до степени секретности «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

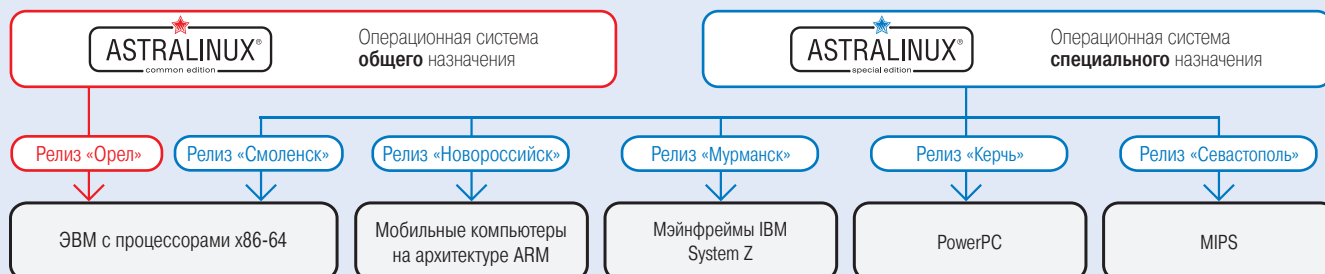
СФ/014-2579 от 20.03.2015. Действителен до 2018 г.

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.



## СВИДЕТЕЛЬСТВА И ПАТЕНТ

### СВИДЕТЕЛЬСТВА



### ПАТЕНТ

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

№ 2525481 (RU)

Патентообладатели: АО «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



### ЕДИНЫЙ РЕЕСТР

#### Минкомсвязь России



Включена в Единый реестр российских программ для электронных вычислительных машин и баз данных Минкомсвязи России



#### РОСАТОМ

В 2015 году ОС включена в отраслевой стандарт госкорпорации

## ЗАКАЗЧИКИ

### МИНИСТЕРСТВА, ВЕДОМСТВА, АГЕНТСТВА И СПЕЦИАЛЬНЫЕ СЛУЖБЫ



● Минобороны России



● ФСБ России



● ФСО России



● МВД России



● ФСИН России



● ФТС России



РОСКОСМОС

● Роскосмос

### ВУЗЫ

● Более 10000  
бесплатных  
лицензий



### МЕЖВЕДОМСТВЕННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ГАС ГОЗ

### НАЦИОНАЛЬНЫЙ ЦЕНТР УПРАВЛЕНИЯ ОБОРОНОЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

## ГОСКОРПОРАЦИИ



● **Внутренние  
войска МВД  
России**



● **Росатом**



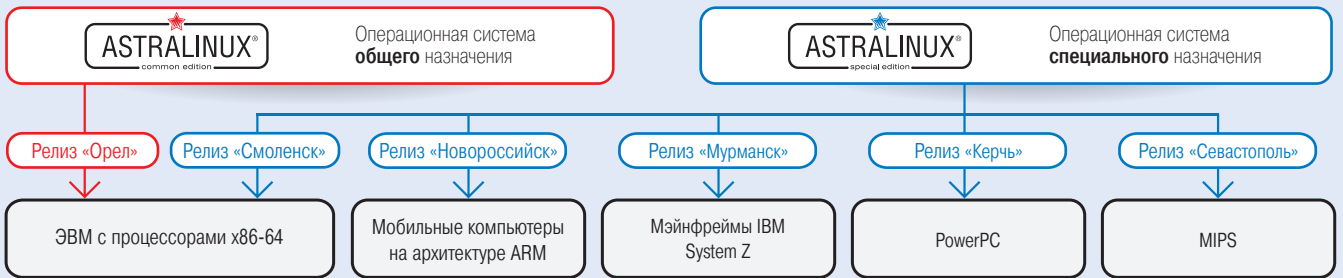
● **Ростех**



## ПРЕДПРИЯТИЯ ОБОРОННО-ПРОМЫШЛЕННОГО КОМПЛЕКСА



## 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



КОЛЛЕКТИВ РАЗРАБОТЧИКОВ:  
• 200 СПЕЦИАЛИСТОВ  
• СРЕДНИЙ ВОЗРАСТ 34 ГОДА



ЕЖЕГОДНО ОСУЩЕСТВЛЯЕТСЯ  
ВЫПУСК НОВОЙ ВЕРСИИ



КОНТРОЛЬ КАЧЕСТВА  
ОСУЩЕСТВЛЯЕТСЯ С ПРИВЛЕЧЕНИЕМ  
ЭКСПЕРТОВ ФСБ РОССИИ И РАН



НЕПРЕРЫВНАЯ ТЕХНИЧЕСКАЯ  
ПОДДЕРЖКА И СОПРОВОЖДЕНИЕ

# ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НСД ДЛЯ АС

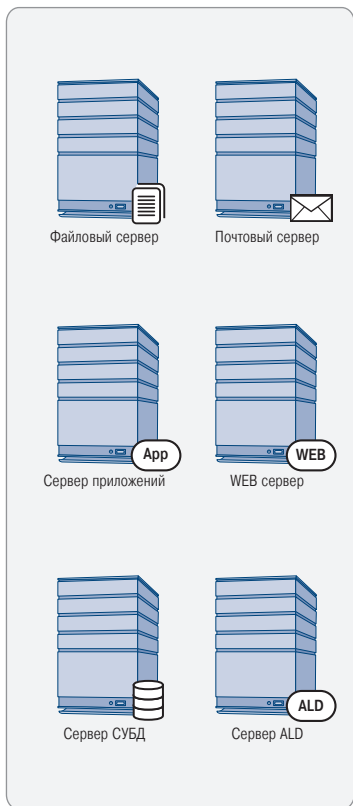
ПОДСИСТЕМЫ И ФУНКЦИИ	ТРЕБОВАНИЯ	Уровень защищаемой информации	Совсекретно							
			Секретно							
			ДСП							
			Перс. данные							
РЕАЛИЗАЦИЯ	1Д	2Б	3Б	1Г	1В	3А	2А	1Б		
<b>1. Подсистема управления доступом</b>										
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:	Должен 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					+		+	
<b>2. Подсистема регистрации и учета</b>										
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 аппаратного отключения АС. <i>В параметрах регистрации указываются:</i> 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 «твёрдую» 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 выданной документом 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»). <i>В параметрах регистрации указываются:</i> 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 АО «НПО РубСБТех»)»				+	+	+	+	
- запуска (завершения) программ и процессов (заданий, задач)	Должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. <i>В параметрах регистрации указываются:</i> 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. <i>В параметрах регистрации указываются:</i> 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. <i>В параметрах регистрации указываются:</i> 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. <i>В параметрах регистрации указываются:</i> 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, иницируемых 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 записью в любую освобождаемую область памяти, используемую 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 АО «НПО РубСБТех»)»					+		+	
<b>3. Криптографическая подсистема</b>										
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 переносимые носители данных (дискеты, микрофлэш и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться принудительная очистка областей внешней памяти, содержащих 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.								+	
<b>4. Подсистема обеспечения целостности</b>										
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 программных средств 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 приема 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					+	+	+	

ОБЛАСТЬ ПРИМЕНЕНИЯ. СОЗДАНИЕ ЗАЩИЩЕННЫХ ТЕРРИТОРИАЛЬНО

СЕГМЕНТ ОБРАБОТКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ЗАЩИЩЕННАЯ ЛВС

Серверное оборудование



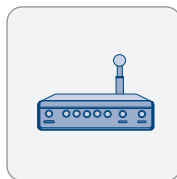
Бездисковая рабочая станция



Бездисковая рабочая станция (моноблок)



Коммутационное оборудование



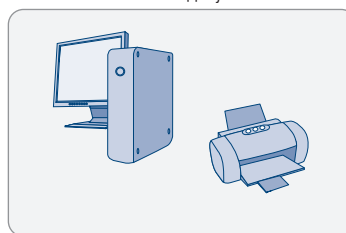
АРМ администратора



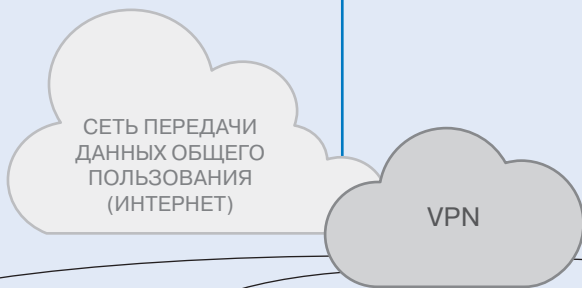
АРМ ввода-вывода данных



АРМ печати документов



МЭ\*\*



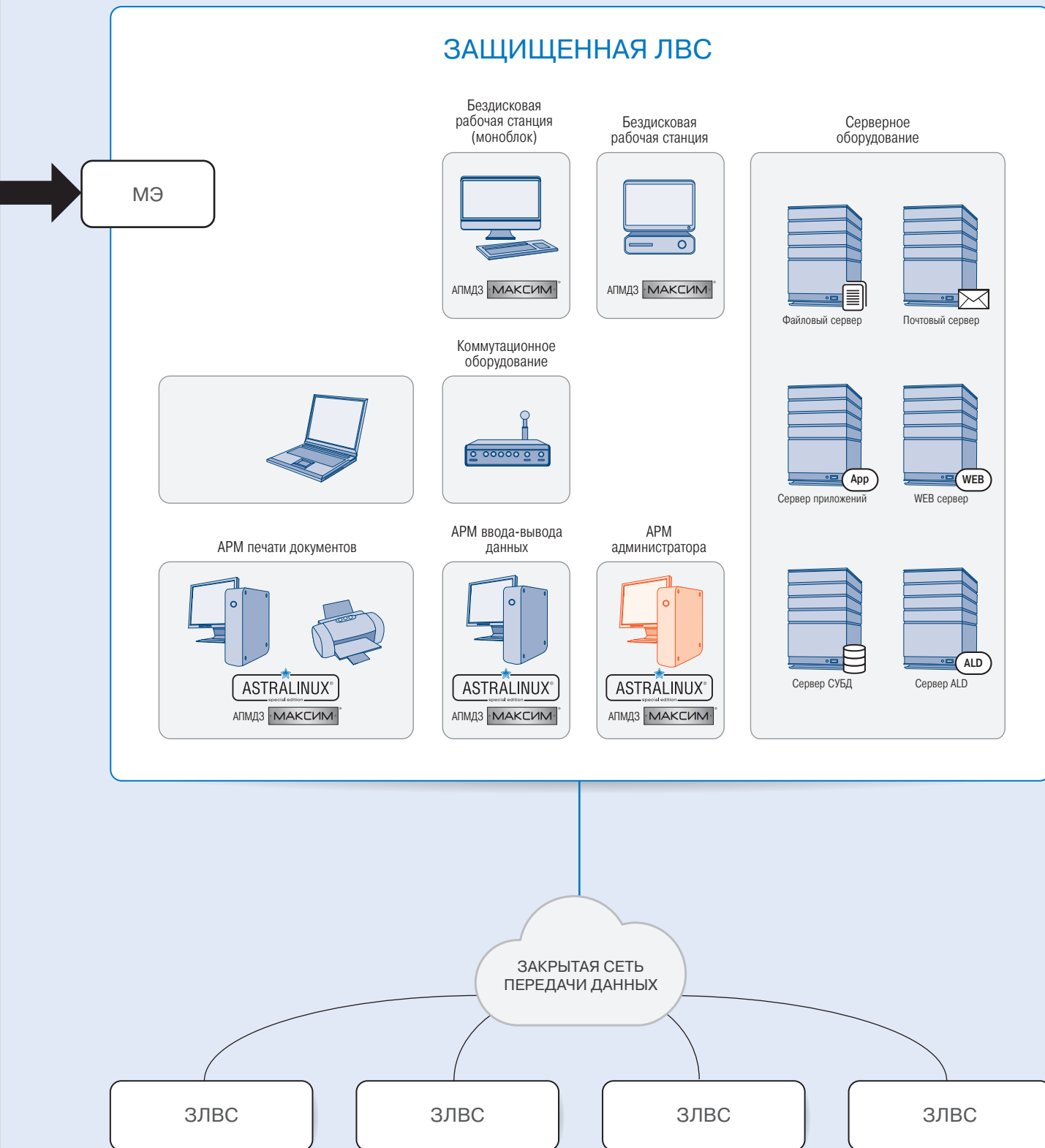
\* ЗЛВС – защищенная локальная вычислительная сеть

\*\* МЭ – межсетевой экран

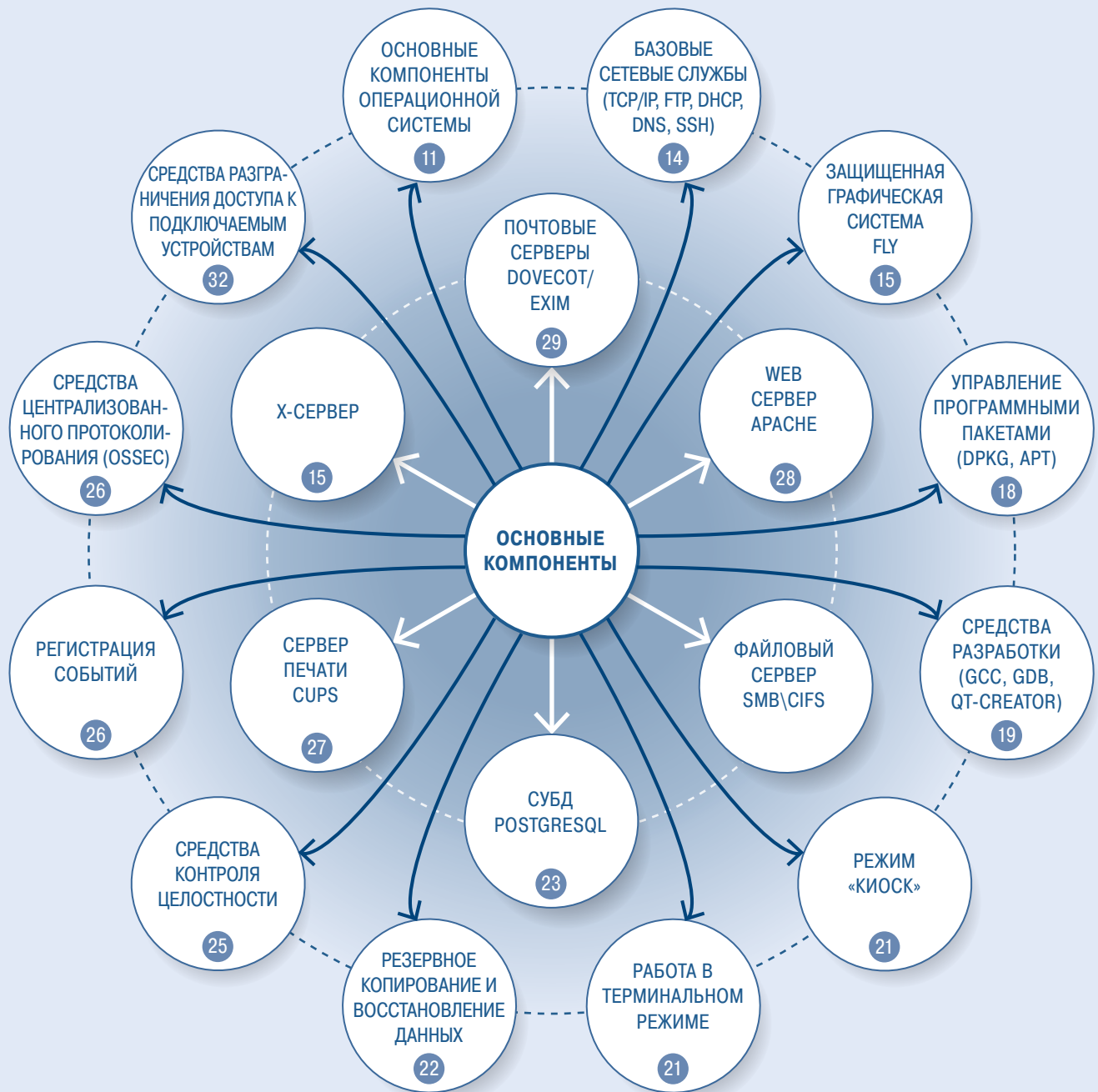


РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

СЕКТОР ОБРАБОТКИ СВЕДЕНИЙ, СОДЕРЖАЩИХ  
ГОСУДАРСТВЕННУЮ ТАЙНУ



## ОСНОВНЫЕ КОМПОНЕНТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ

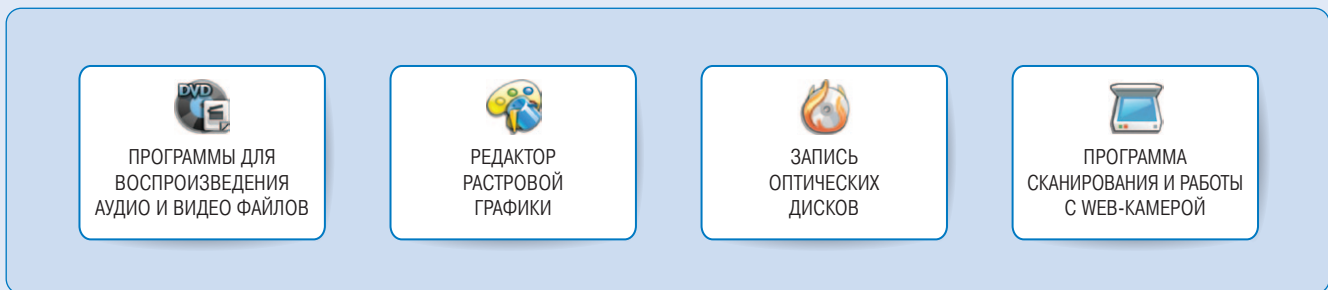


## ОСНОВНЫЕ КОМПОНЕНТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ

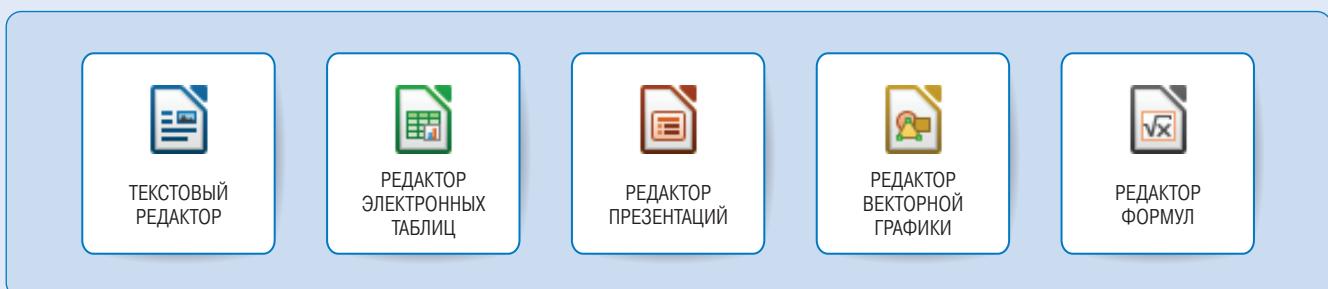
### ЗАЩИЩЕННЫЙ ПРОГРАММНЫЙ КОМПЛЕКС ОРГАНИЗАЦИИ ЕДИНОГО ПРОСТРАНСТВА ПОЛЬЗОВАТЕЛЕЙ И РЕСУРСОВ ЛВС (ДОМЕН ALD)



### РАБОТА С МУЛЬТИМЕДИА И ИЗОБРАЖЕНИЯМИ



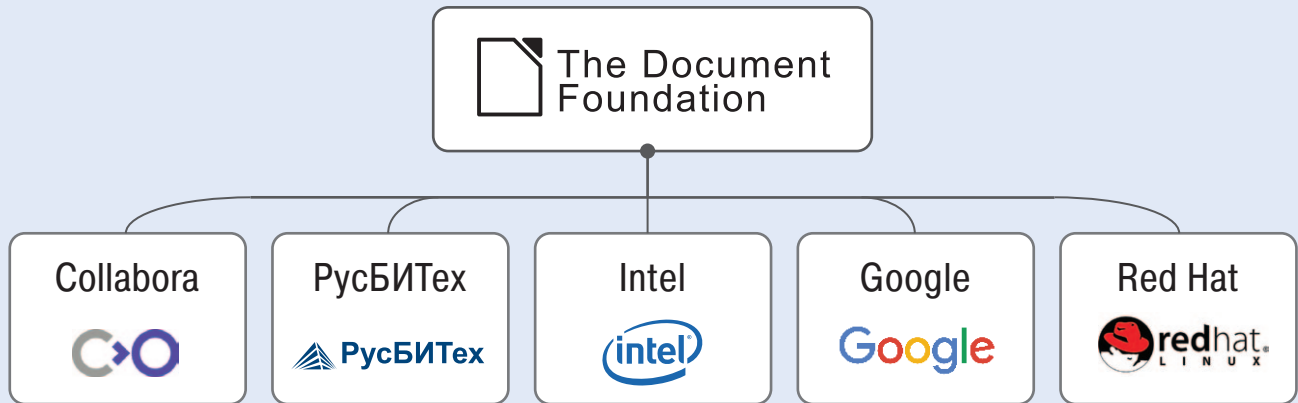
### РАБОТА С ДОКУМЕНТАМИ (LIBREOFFICE)





## СРЕДСТВА РАБОТЫ С ДОКУМЕНТАМИ

### КЛЮЧЕВЫЕ ЧЛЕНЫ КОНСУЛЬТАЦИОННОГО СОВЕТА «THE DOCUMENT FOUNDATION»



### ОФИСНЫЕ ПРИЛОЖЕНИЯ LIBREOFFICE



<p><b>Текстовый редактор WRITER</b></p>		<p><b>Форматы:</b> .odt .docx (2007-2013) .doc (97/XP/2000/2003) .rtf .txt</p>	
<p><b>Табличный редактор CALC</b></p>		<p><b>Форматы:</b> .ods .xlsx (2007-2013) .xls (97/XP/2000/2003) .dbf .csv</p>	
<p><b>Векторный редактор DRAW</b></p>		<p><b>Форматы:</b> .odg .vsd (Visio) .jpg, gif, png, bmp .tif, tiff .eps</p>	
<p><b>Редактор презентаций IMPRESS</b></p>		<p><b>Форматы:</b> .odp .pptx (2007-2013) .ppt (97/XP/2000/2003) .pps</p>	

## 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.

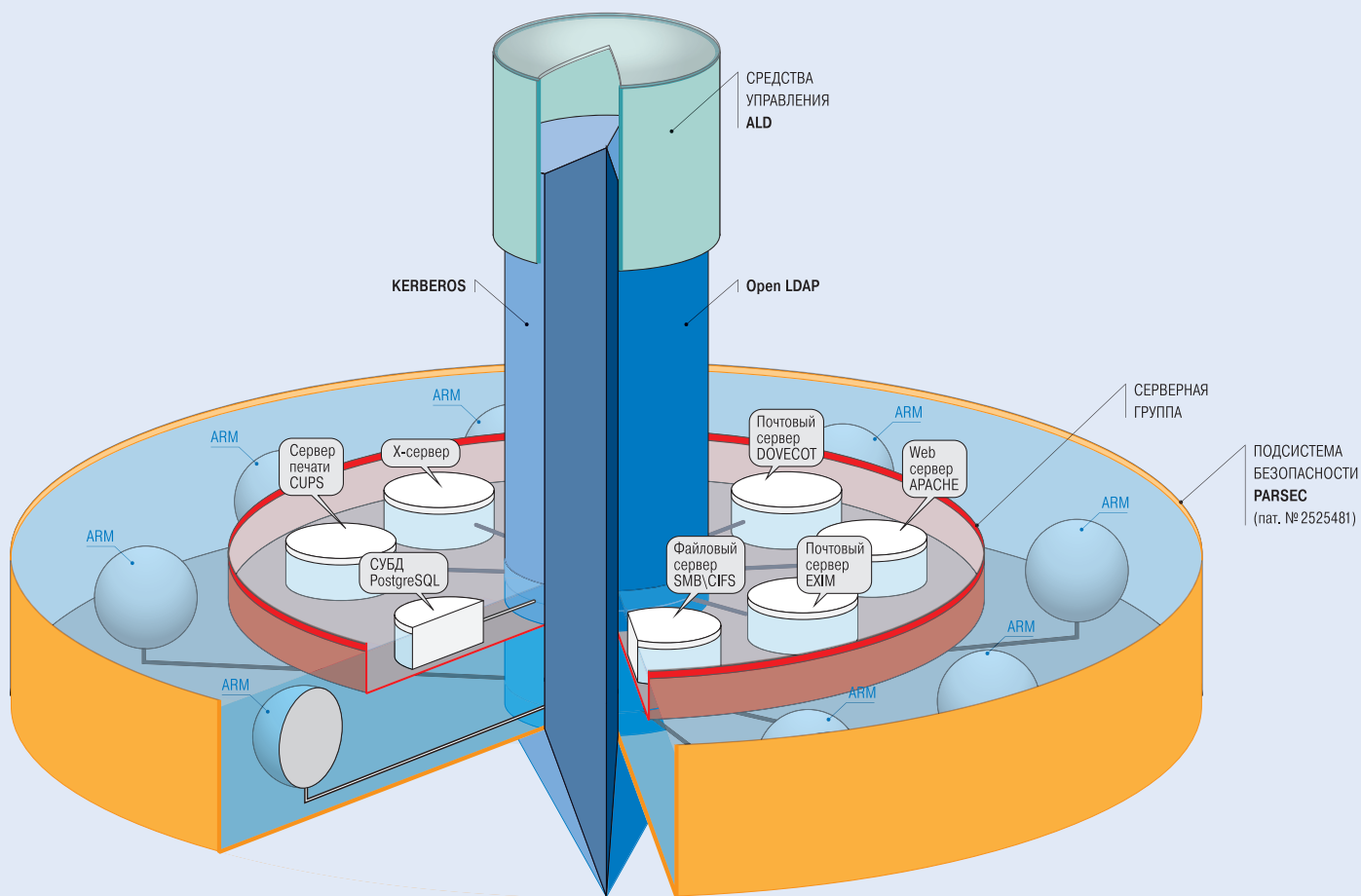


СХЕМА ОРГАНИЗАЦИИ ДОМЕНА ALD

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

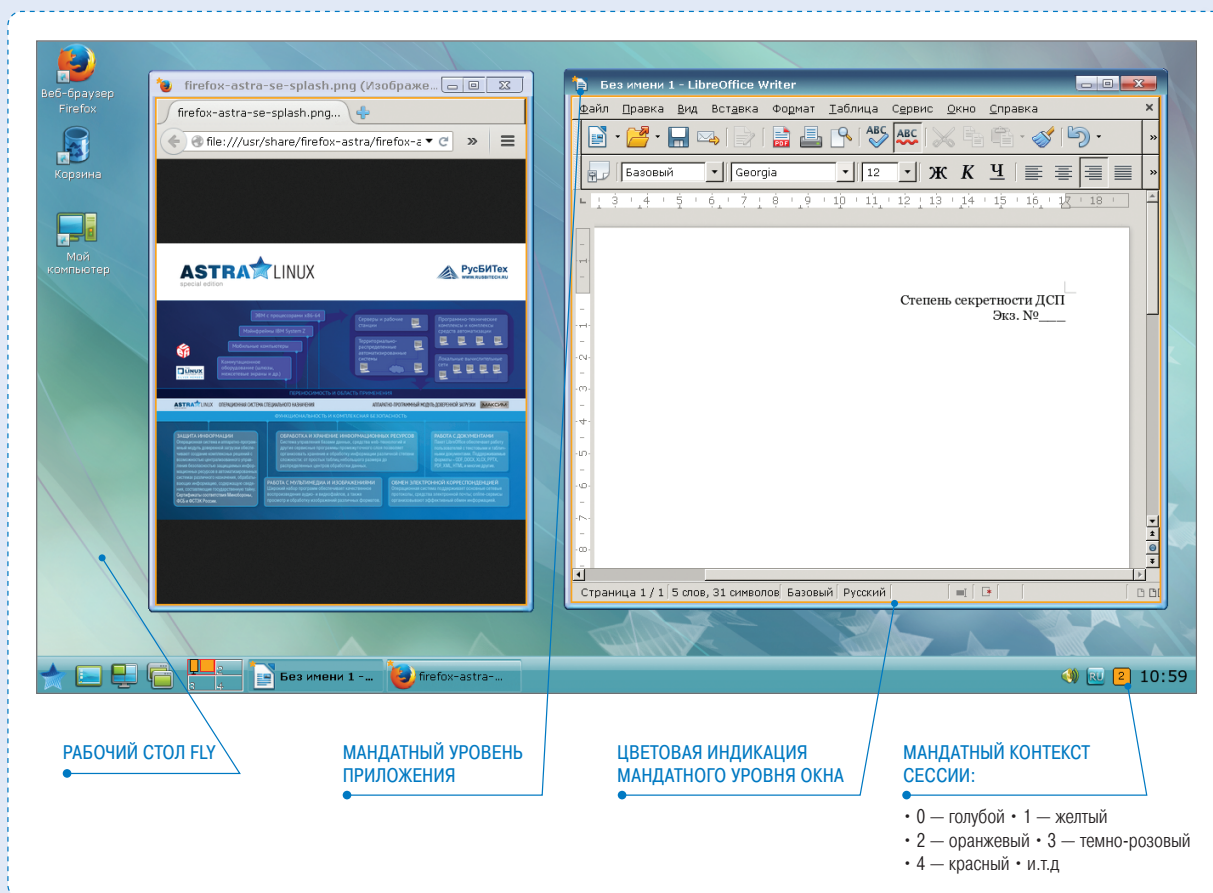
**Сетевая защищенная файловая система**

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.

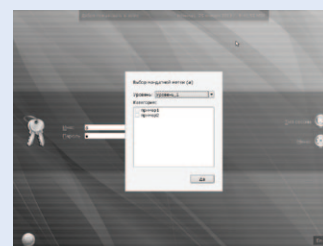
В состав защищенной графической системы ОС СН входит рабочий стол пользователя FLY, интегрированный с внедренными в X-сервер механизмами защиты информации и обеспечивающий отображение мандатного контекста сессии:



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

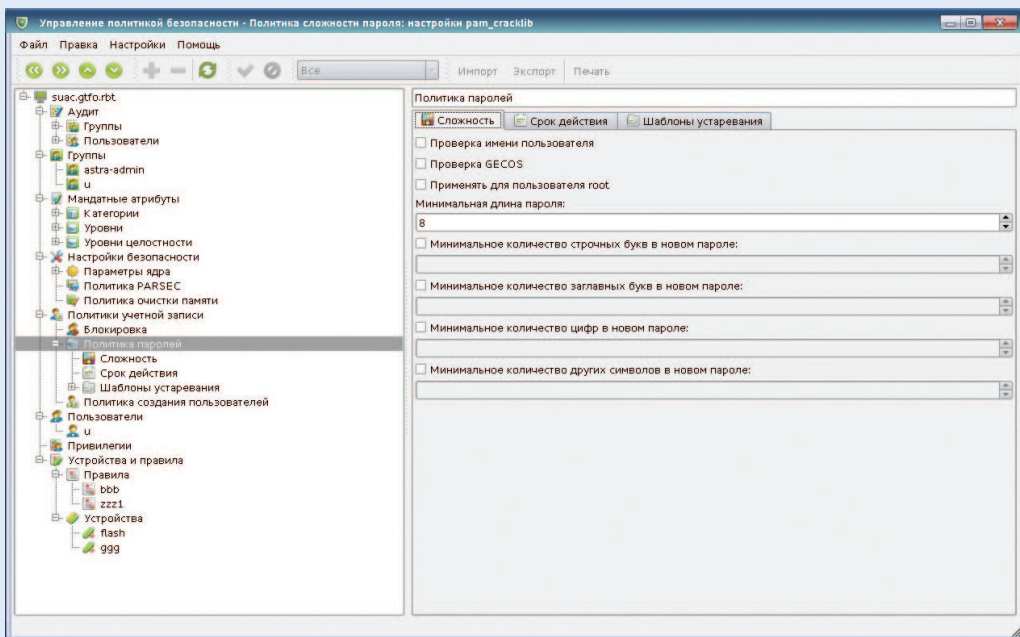
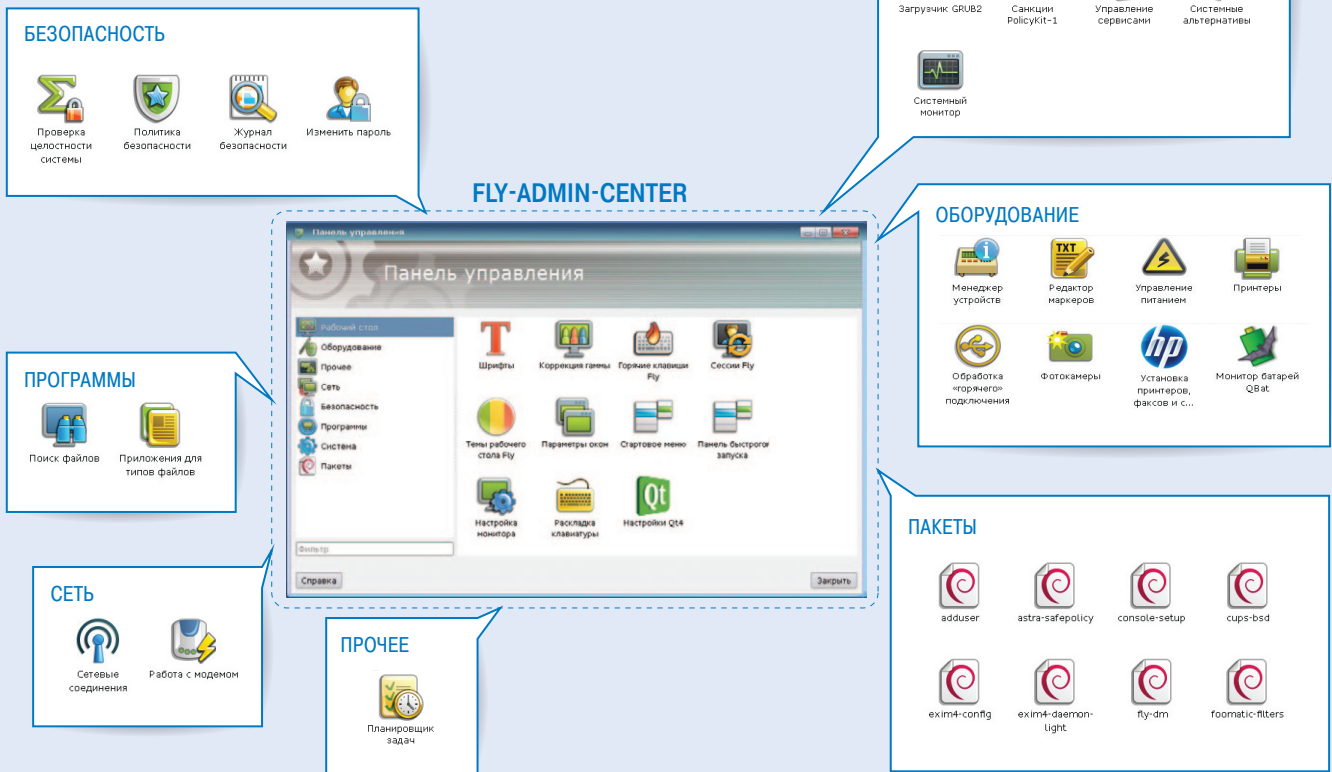
При графическом входе в систему пользователь выбирает в специальном диалоге уровень и категорию конфиденциальности. После этого вся его графическая сессия будет выполняться в режиме выбранной совокупности уровня секретности и/или категории. Одновременно пользователем может быть выполнено несколько входов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



## ЗАЩИЩЕННАЯ ГРАФИЧЕСКАЯ СИСТЕМА FLY

### ОСНОВНЫЕ ГРАФИЧЕСКИЕ УТИЛИТЫ ДЛЯ АДМИНИСТРИРОВАНИЯ СИСТЕМЫ

Централизованный доступ к графическим утилитам настройки и администрирования системы





## 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

**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

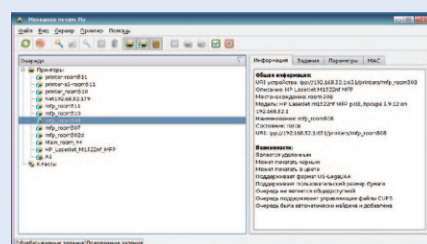
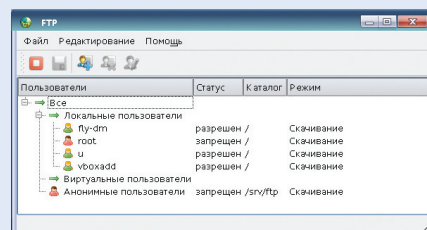
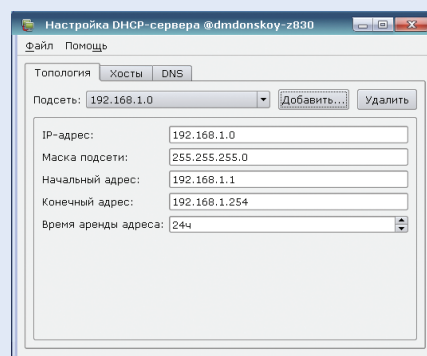
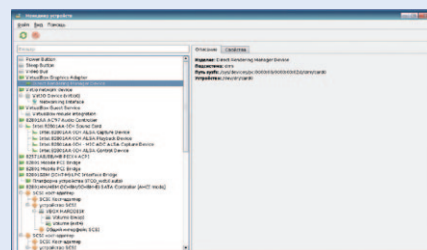
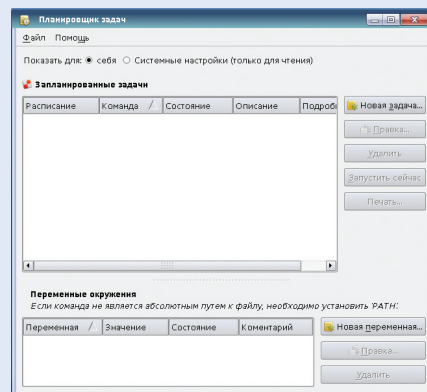
**fly-admin-theme** — утилита настройки тем рабочего стола и режимов переключения рабочий стол/планшет

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

**fly-admin-samba** — утилита управления общими папками Samba

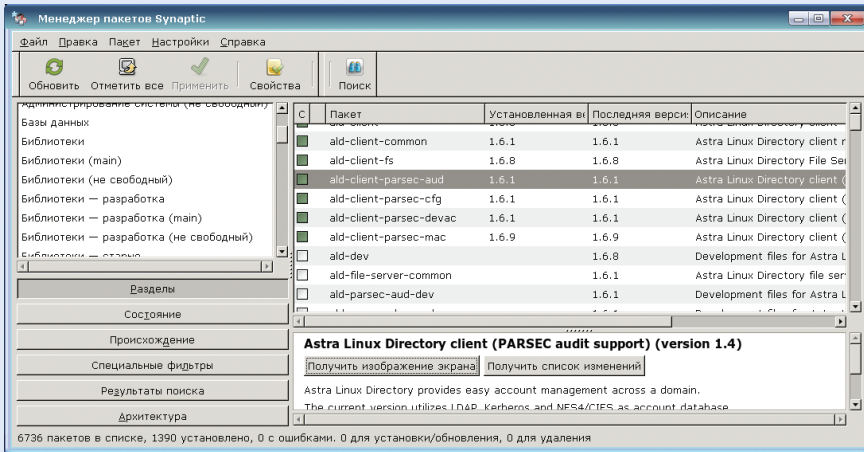
**fly-admin-marker** — редактор маркировки страниц, выводимых на печать

**fly-admin-service** — Консоль управления сервисами. Позволяет рассматривать статус и конфигурацию служб, осуществлять их запуск и остановку, а также осуществлять автоматизированную настройку служб в соответствии с «Руководством администратора»

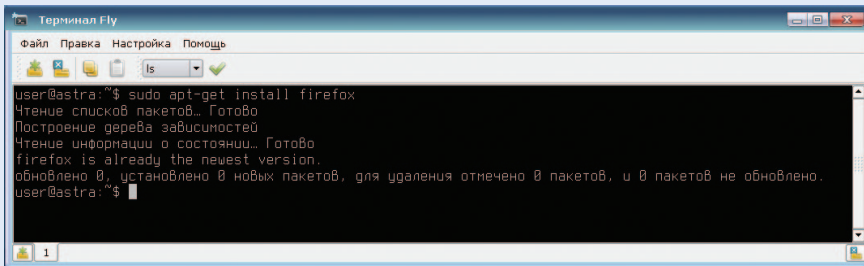


## УПРАВЛЕНИЕ ПРОГРАММНЫМИ ПАКЕТАМИ

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`.

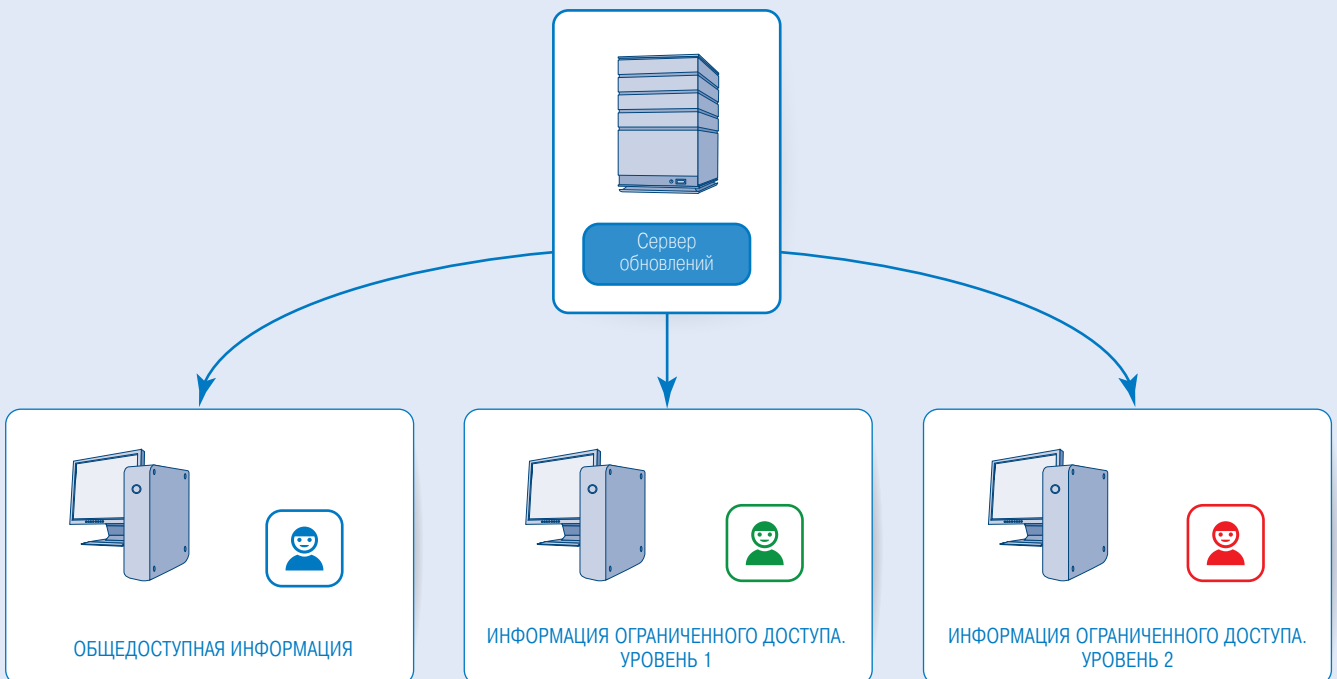


По умолчанию обычный пользователь не имеет права использовать эти инструменты. Для всех операций с пакетами необходимы права администратора.



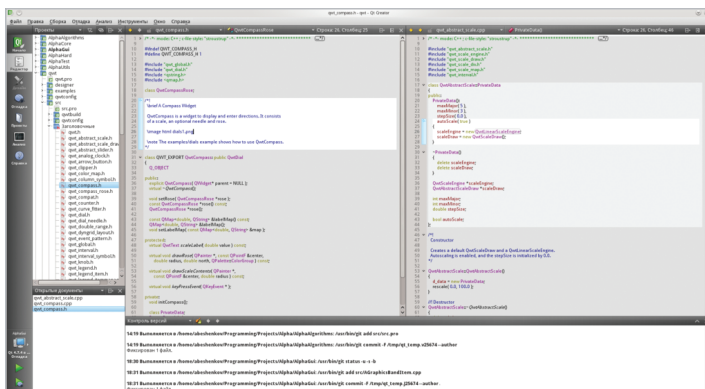
Мониторинг системы в процессе установки и ведение журнала установки позволяют корректно удалить приложение, ставшее ненужным.

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

```

emx@venice:~$ gcc --version
gcc (GCC) 4.1.2 20060928 (prerelease) (Ubuntu 4.1.1-13ubuntu5)
Copyright (C) 2006 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is no
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

emx@venice:~$ gcc -v
Using built-in specs.
Target: i486-linux-gnu
Configured with: ../src/configure -v --enable-languages=c,c++,fortran,objc,obj
-c++,treelang --prefix=/usr --enable-shared --with-system-llib --libexecdir=/u
sr/lib --without-included-gettext --enable-threads=posix --enable-nls --progra
m-suffix=.4.1 --enable_cxa_atexit --enable-clocale=gnu --enable-libstdc++de
bug --enable-mpfr --enable-checking=release i486-linux-gnu
Thread model: posix
gcc version 4.1.2 20060928 (prerelease) (Ubuntu 4.1.1-13ubuntu5)
emx@venice:~$
    
```

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

```

GNU gdb 6.8.21
Copyright 2002 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB. Type "show warranty" for details.
This GDB was configured as "i486-pc-mingw32".
GDB help
List of classes of commands:
Aliases -- Aliases of other commands
breakpoints -- Making program stop at certain points
data -- Examining data
files -- Specifying and examining files
internals -- Maintenance commands
obscure -- Obscure features
running -- Running the program
stack -- Examining the stack
status -- Status inquiries
support -- Support facilities
tracpoints -- Tracing of program execution without stopping the program
user-defined -- User-defined commands
Type "help" followed by a class name for a list of commands in that class.
    
```

**ASTRALINUX**  
special edition

Операционная система специального назначения

**Версии ядра, libc, GCC, QT**  
вы можете посмотреть на официальном сайте [www.astralinux.ru](http://www.astralinux.ru) в разделе «Основные компоненты операционной системы специального назначения»

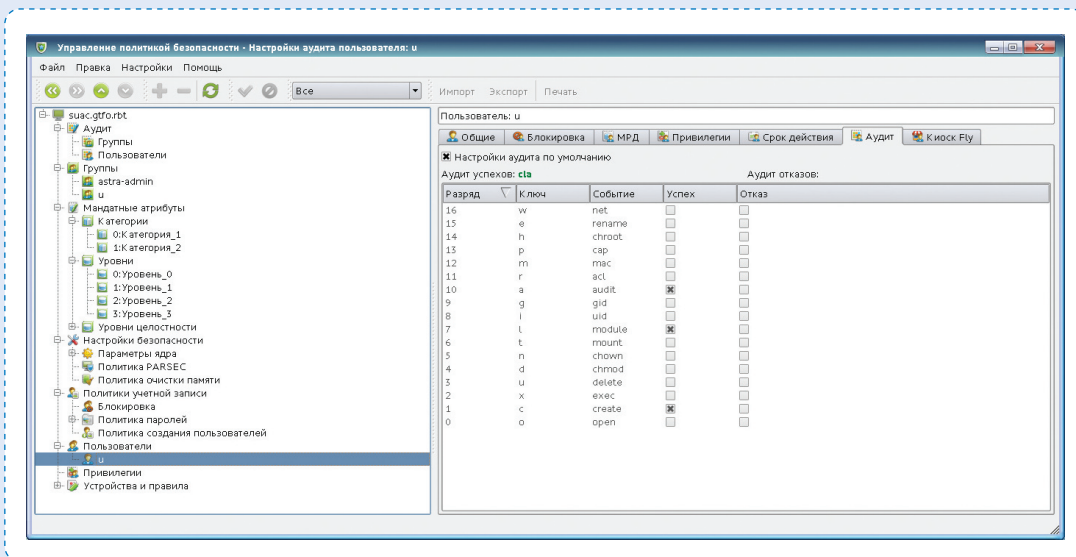
**ЗАГОЛОВОЧНЫЕ  
ФАЙЛЫ**

**БИБЛИОТЕКИ**

**УТИЛИТЫ**

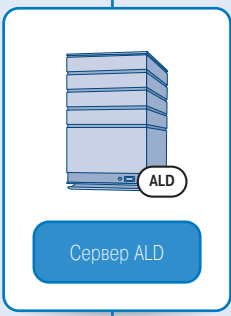
# АУДИТ И ЖУРНАЛИРОВАНИЕ СОБЫТИЙ

## НАСТРОЙКА ПАРАМЕТРОВ АУДИТА

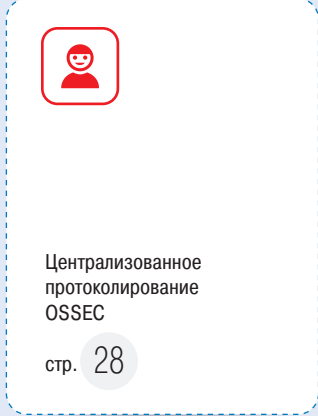
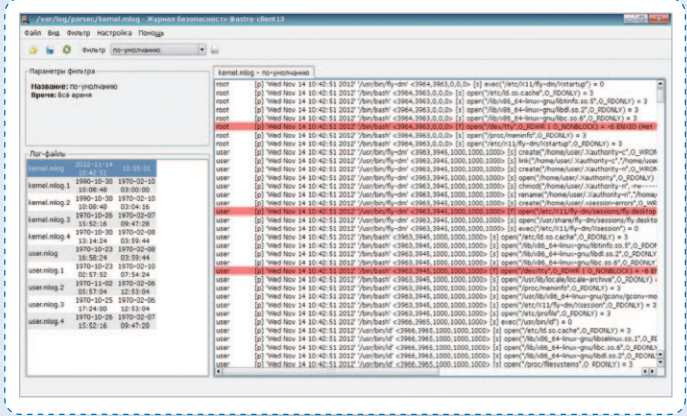
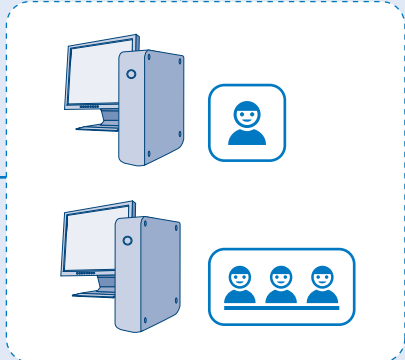


Настройки аудита

Применение настроек аудита



Протоколирование событий



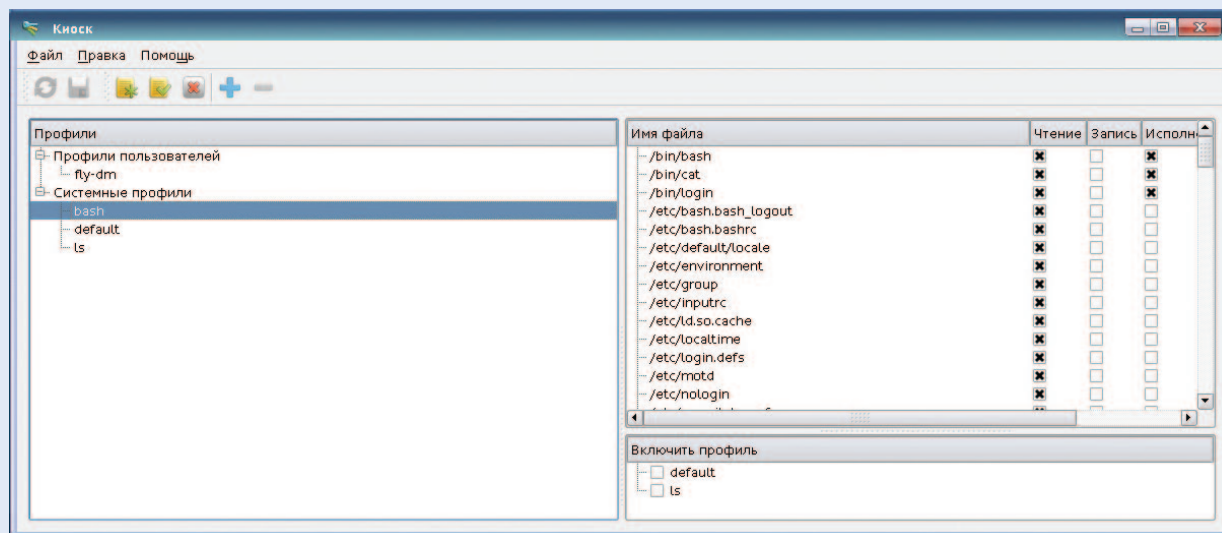
Централизованное протоколирование OSSEC  
стр. 28

СОСТАВ И ОСНОВНЫЕ КОМПОНЕНТЫ

## РЕЖИМ «КИОСК»

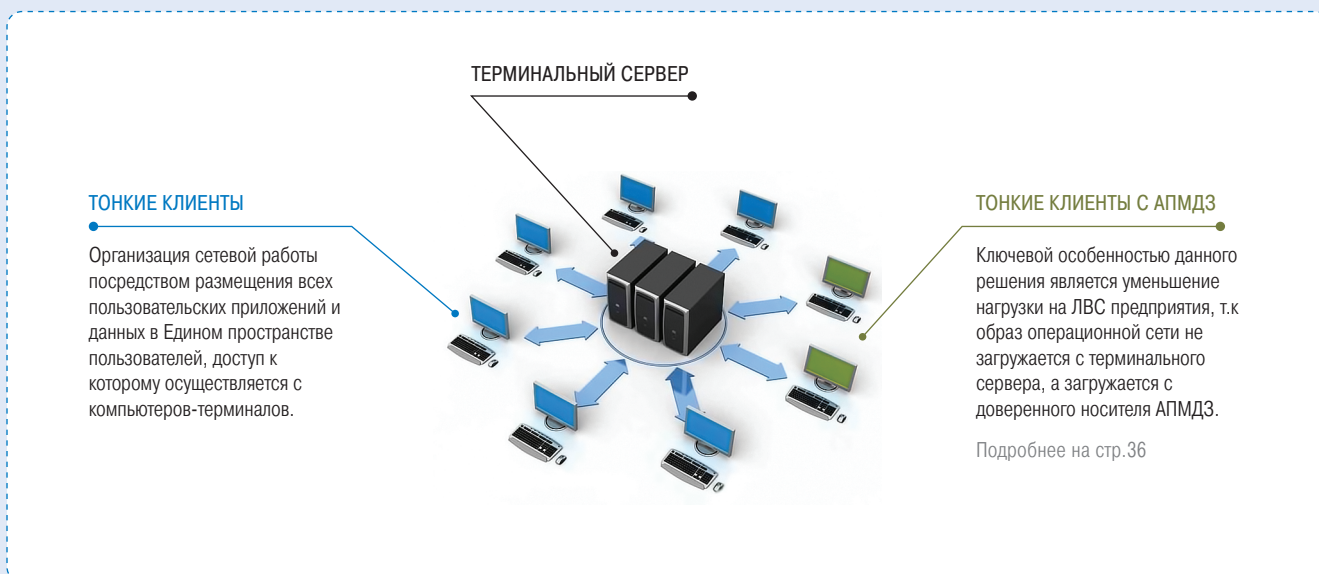
### РЕЖИМ «КИОСК»

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

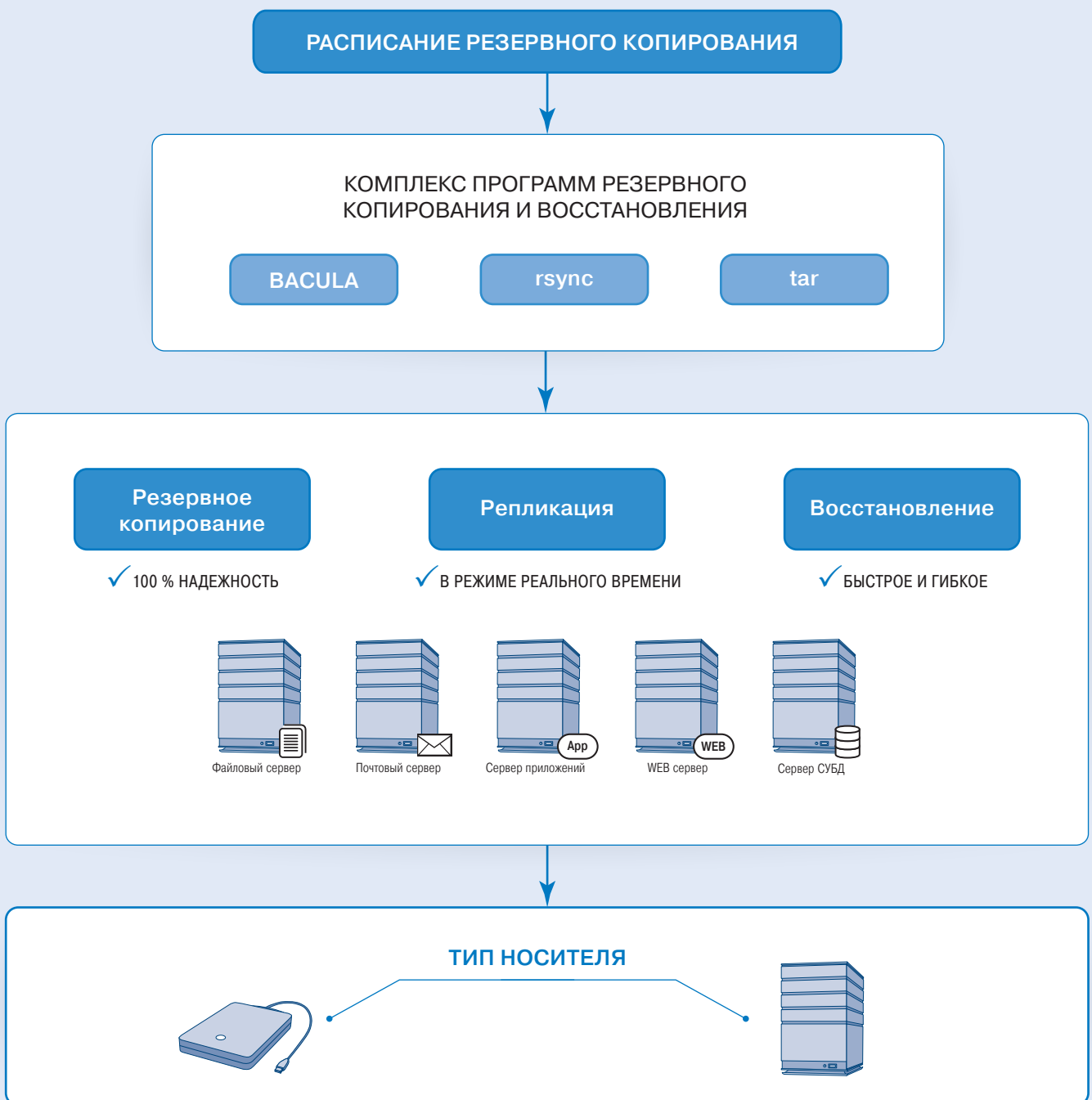




## РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

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.

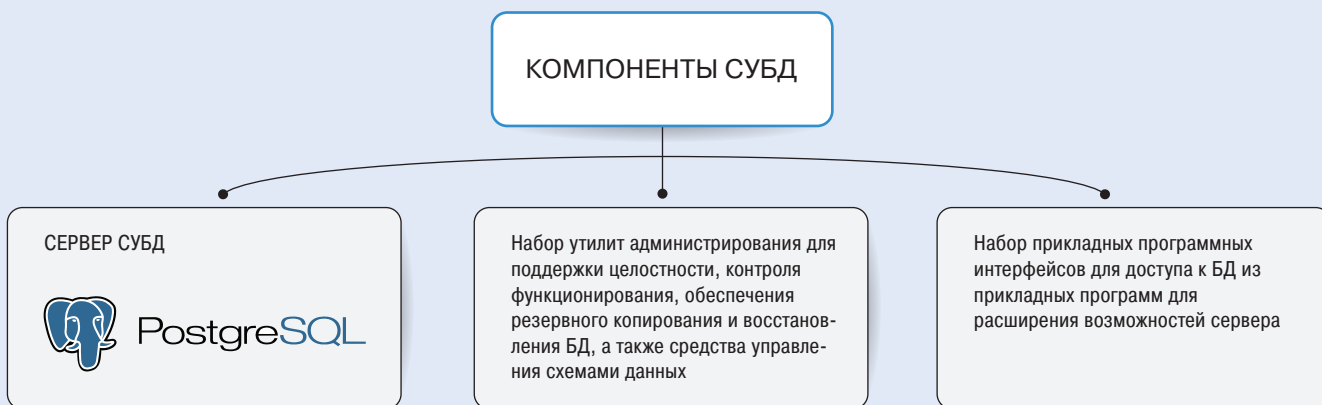


## ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

### НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

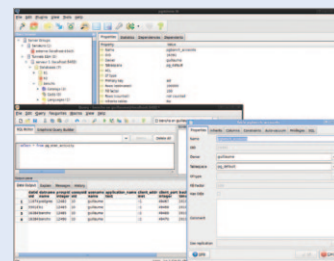
Защищенная система управления базами данных из состава операционной системы специального назначения «Astra Linux Special Edition» с интегрированными средствами защиты информации (далее – СУБД) предназначена для создания информационных и управляющих систем для работы как с конфиденциальной информацией, 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 недеklarированных 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 Direcorv, что позволяет обеспечить доступ к серверам СУБД через сетевые сервисы (например, WEB-сервер) на основе единой политики безопасности информации с использованием сквозной аутентификации.

## 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	Perl, Python, Ruby, Tcl, C/C++, PL/pgSQL, Java
Поддержка интерфейсов средств разработки	ODBC, Perl, Python, Ruby, C, C++, PHP, Lisp, Scheme, Qt, Java (JDBC)
Обеспечение отказоустойчивости	Резервное копирование и восстановление. Асинхронная и синхронная репликация данных ( в том числе и двунаправленная).
Средства администрирования	Утилиты командной строки администрирования. Графическая утилита разработки БД и управления доступом.
Механизмы аутентификации	- парольная, LDAP, RADIUS; - PAM (Pluggable Authentication Modules); - Ident, Peer; - Kerberos, SSPI, GSSAPI; - сертификаты.

## КОНТРОЛЬ ЦЕЛОСТНОСТИ

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

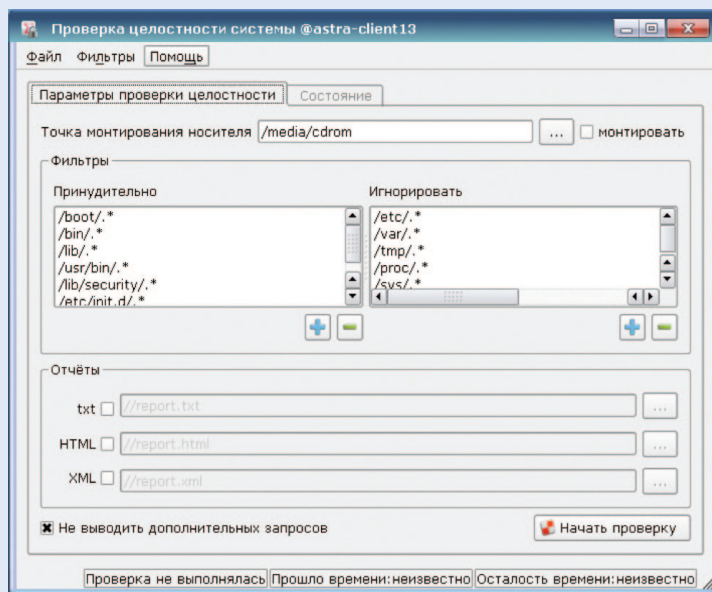
В ОС СН реализован многоуровневый контроль целостности программного обеспечения:

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 реализованы функции хэширования (одностороннего криптографического преобразования) в соответствии с ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит и ГОСТ Р 34.11-2012 с длиной хэш-кода 512 бит. 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.

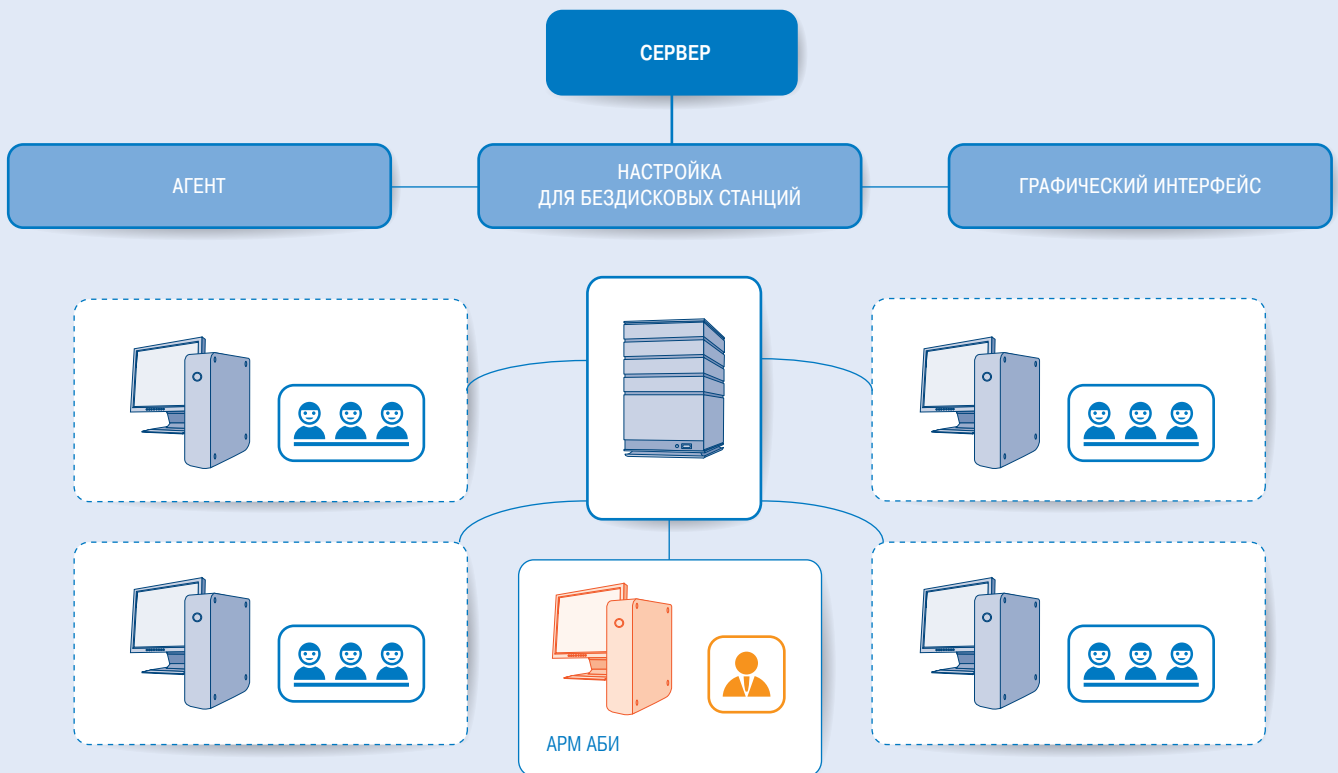
В ОС СН реализован механизм, обеспечивающий проверку неизменности и подлинности загружаемых исполняемых файлов в формате ELF (Executable and Linkable Format). Проверка производится на основе контрольных сумм, вычисляемых в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит, и ЭЦП, реализованной в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, которые внедрены в исполняемые файлы формата ELF в процессе сборки ОС.

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

## 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:



13 ч. 14 мин. 05 сек. - РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ - Mozilla Firefox @ arm1

arm1/osssec/prog/UnitList.php

События безопасности информации по состоянию на 13 ч. 14 мин. 01 сек.

Из 2 устройств: 1 - включено 1 - выключено 0 - нет данных Распределение событий по устройствам: 2 - ТРЕВОГА 2 - ВНИМАНИЕ 2 - Сообщения 0 - нет данных

Полученные события		менее 10 минут назад	от 10 до 30 минут назад	от 30 минут до 1 часа назад	более 1 часа назад
№ п/п	Устройство	Уровень	Время, дата	Событие (Код)	Источники
1	arm1	5	13:46:23 03.10.2014	Ошибка аутентификации пользователя в домене. (120020)	/var/remote_logs/127.0.0.1/all.log
2	arm1	5	13:45:39 03.10.2014	Ошибка аутентификации пользователя в домене. (120020)	/var/remote_logs/127.0.0.1/all.log
3	dc	3	13:43:04 03.10.2014	Завершение сеанса. (120030)	/var/remote_logs/192.168.32.170/all.log
4	dc	3	13:42:42 03.10.2014	Успешная аутентификация пользователя в домене. (120010)	/var/remote_logs/192.168.32.170/all.log
5	dc	3	12:51:23 03.10.2014	Успешная аутентификация пользователя в домене. (120010)	/var/remote_logs/192.168.32.170/all.log
6	dc	12	12:47:50 03.10.2014	Завершение удаленного (ssh) сеанса root. (120331)	/var/remote_logs/192.168.32.170/all.log
7	dc	3	12:39:04 03.10.2014	Успешная аутентификация пользователя в домене. (120010)	/var/remote_logs/192.168.32.170/all.log
8	arm1	3	12:27:42 03.10.2014	Успешная аутентификация пользователя в домене. (120010)	/var/remote_logs/127.0.0.1/all.log
9	arm1	3	12:26:50 03.10.2014	Успешная аутентификация пользователя в домене. (120010)	/var/remote_logs/127.0.0.1/all.log
10	arm1	3	12:26:34 03.10.2014	Завершение сеанса. (120030)	/var/remote_logs/127.0.0.1/all.log
11	arm1	3	12:22:22 03.10.2014	Успешная аутентификация пользователя в домене. (120010)	/var/remote_logs/127.0.0.1/all.log
12	dc	3	12:20:04 03.10.2014	Успешная аутентификация пользователя в домене. (120010)	/var/remote_logs/192.168.32.170/all.log
13	arm1	3	11:57:44 03.10.2014	Успешная аутентификация пользователя в домене. (120010)	/var/remote_logs/127.0.0.1/all.log
14	arm1	4	11:57:36 03.10.2014	Excessive number of events (above normal). (11)	/var/remote_logs/127.0.0.1/all.log
15	arm1	3	11:57:34 03.10.2014	Завершение сеанса. (120030)	/var/remote_logs/127.0.0.1/all.log
16	arm1	3	11:56:18 03.10.2014	Успешная аутентификация пользователя в домене. (120010)	/var/remote_logs/192.168.32.170/all.log

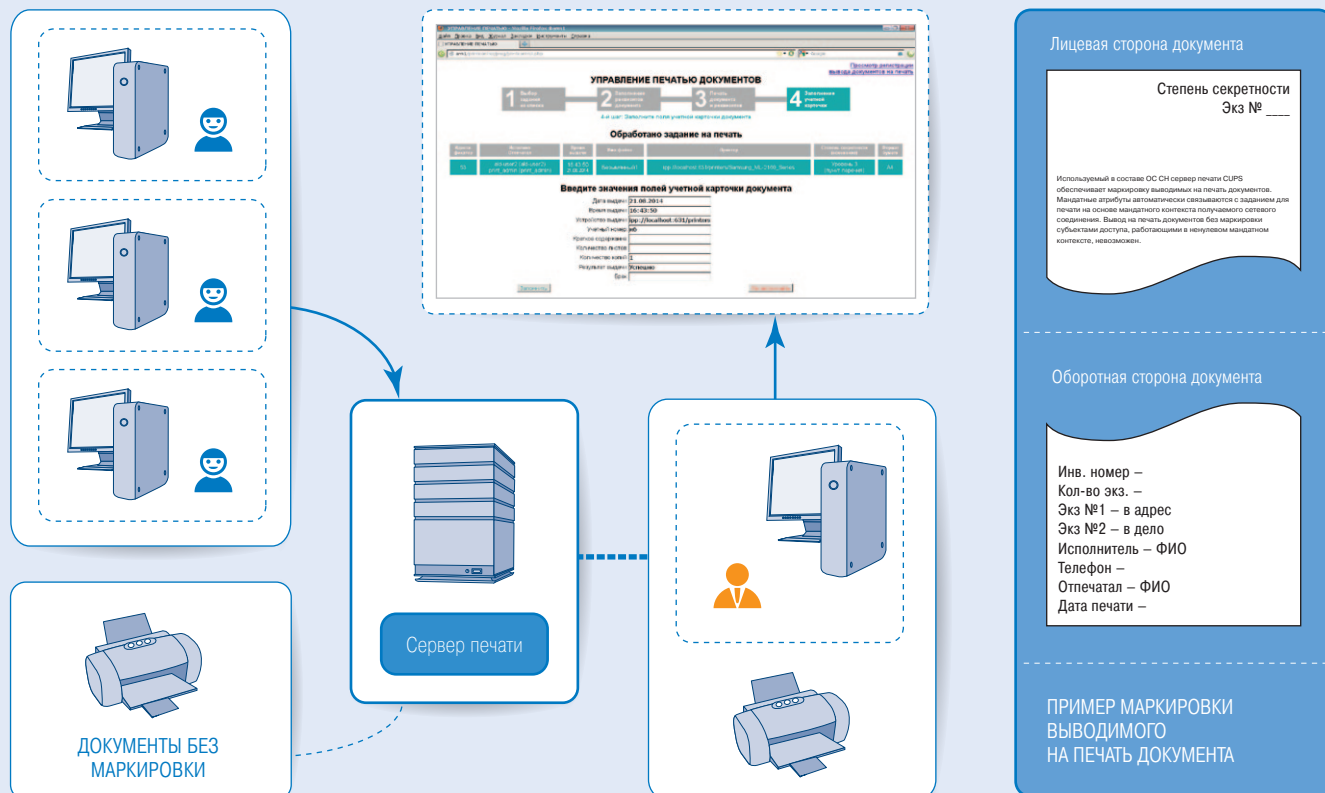
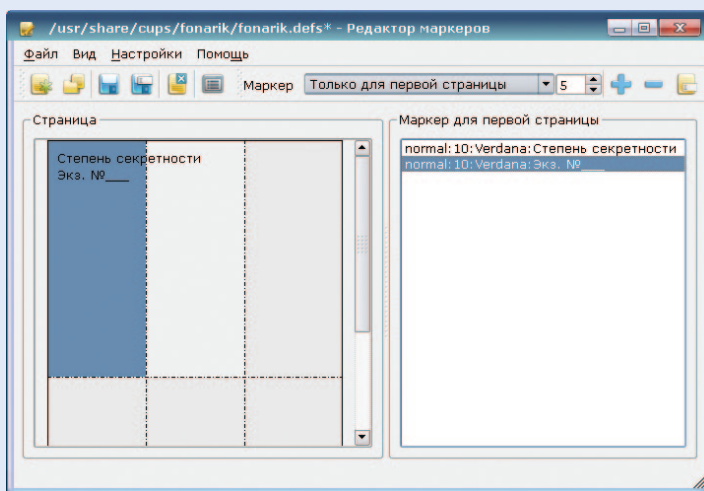


## ПЕЧАТЬ И МАРКИРОВКА ДОКУМЕНТОВ

### 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.

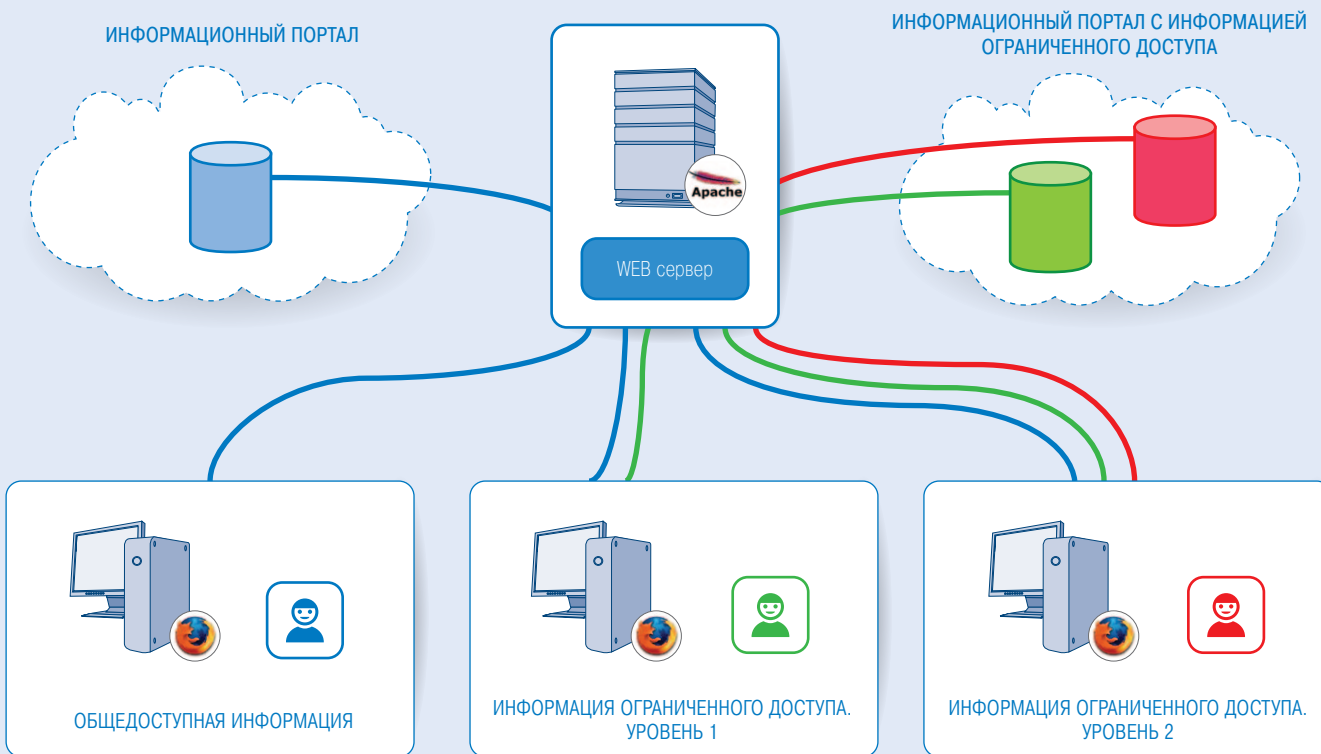
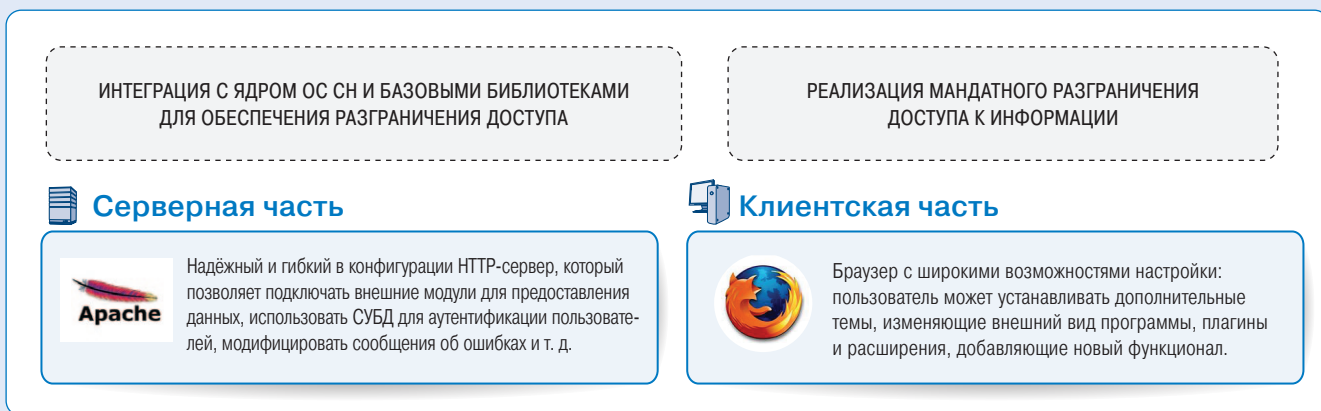


## ГИПЕРТЕКСТОВАЯ ОБРАБОТКА ДАННЫХ

### 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.

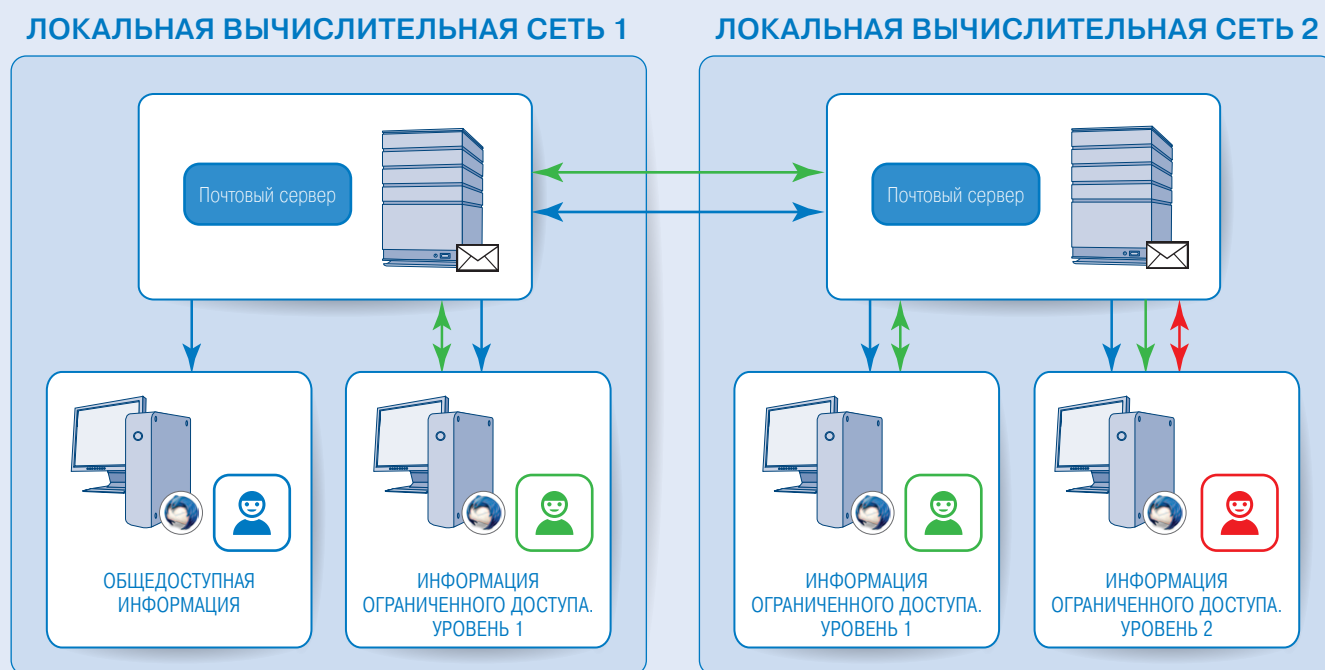
При обслуживании запросов пользователей web-сервер переключается в соответствующий мандатный контекст безопасности пользователя. Доступ к защищаемой информации разграничивается средствами расширенной подсистемы безопасности PARSEC.



## 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:



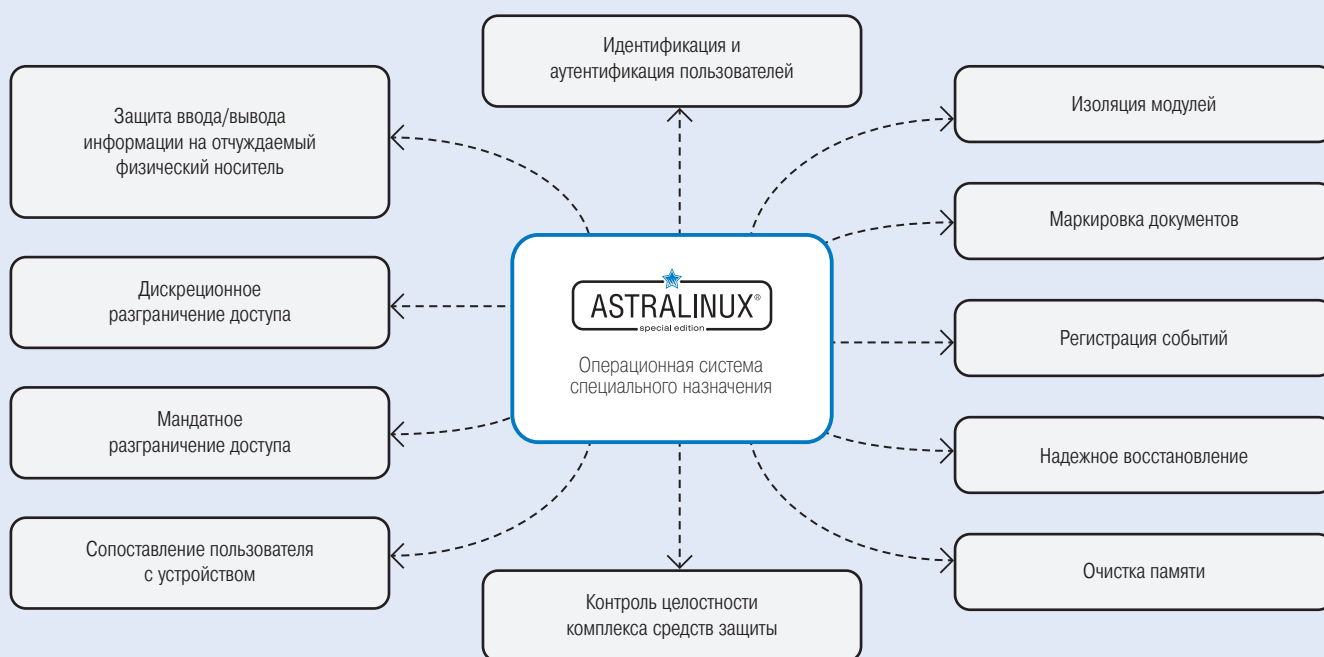
Защищенный комплекс электронной почты обеспечивает идентификацию и аутентификацию доменных пользователей.

## 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.

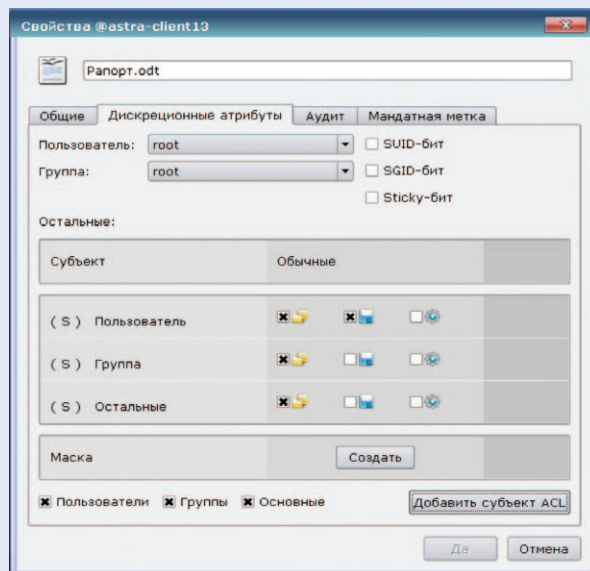
## РЕАЛИЗОВАННЫЕ ФУНКЦИИ СЗИ ОТ НСД

### 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.

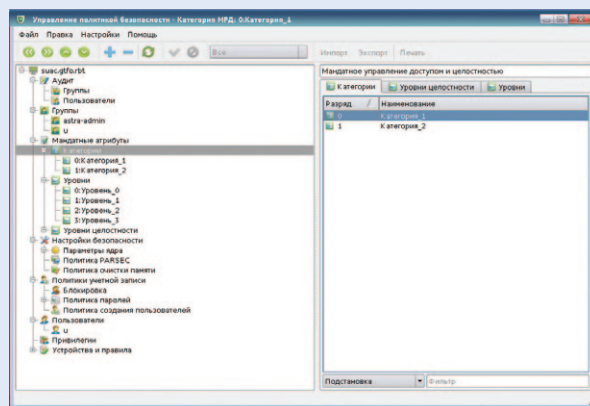


### МАНДАТНОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА

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

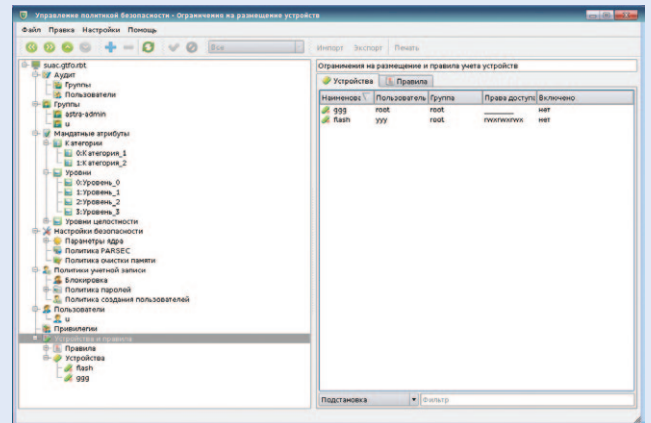
### СРЕДСТВА РАЗГРАНИЧЕНИЯ ДОСТУПА К ВНЕШНИМ УСТРОЙСТВАМ

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

	0	1	2	3
0	ЧЗМ	М	М	М
1	ЧМ	ЧЗМ	М	М
2	ЧМ	ЧМ	ЧЗМ	М
3	ЧМ	ЧМ	ЧМ	ЧЗМ

Мандатный уровень документа

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

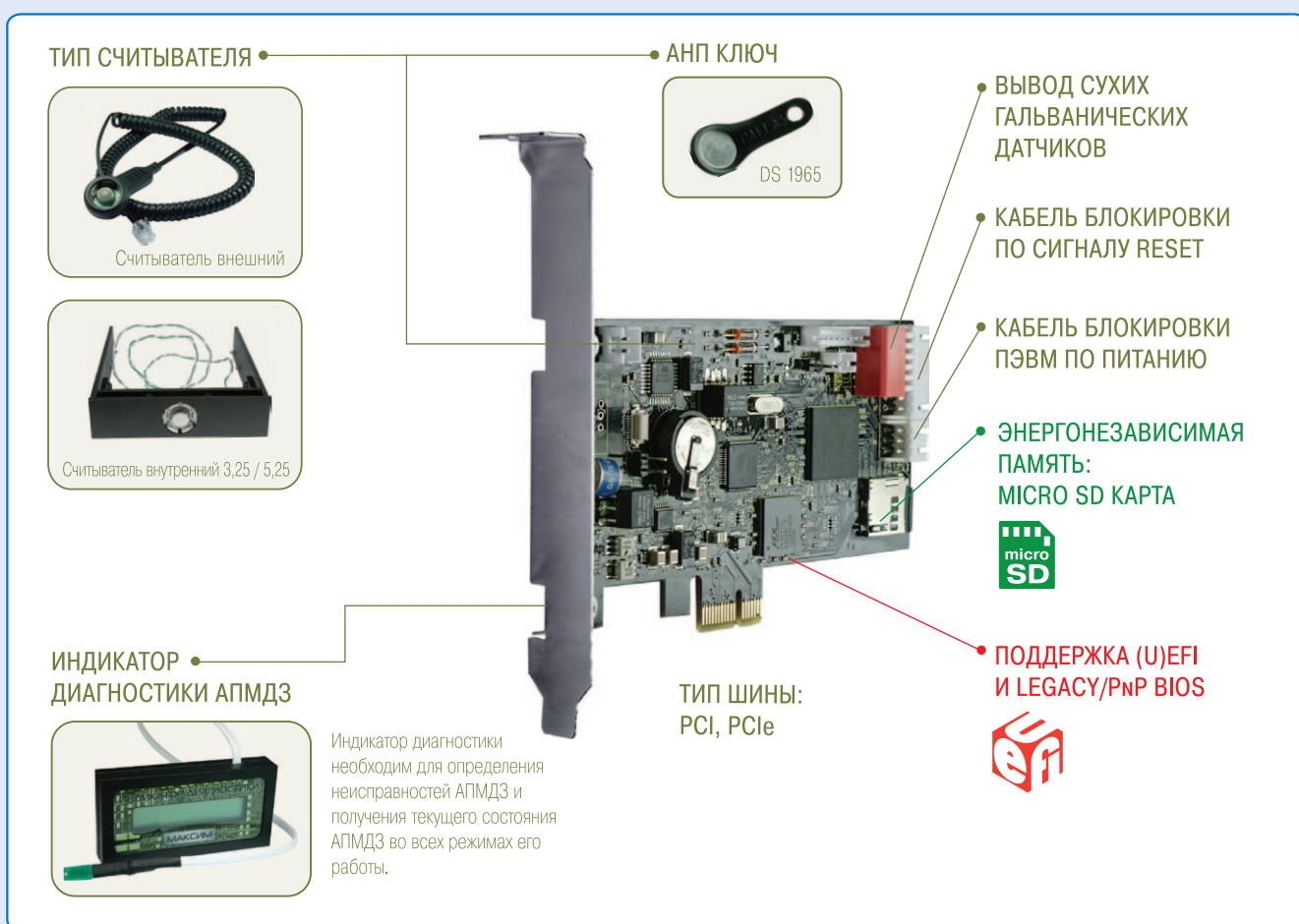
Набор изменений PaX предотвращает выполнение произвольного кода на основе контроля доступа к сегментам памяти следующих типов: «чтение», «запись», «исполнение» – или их комбинации. Комбинация «запись» и «исполнение» запрещена.

## 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»



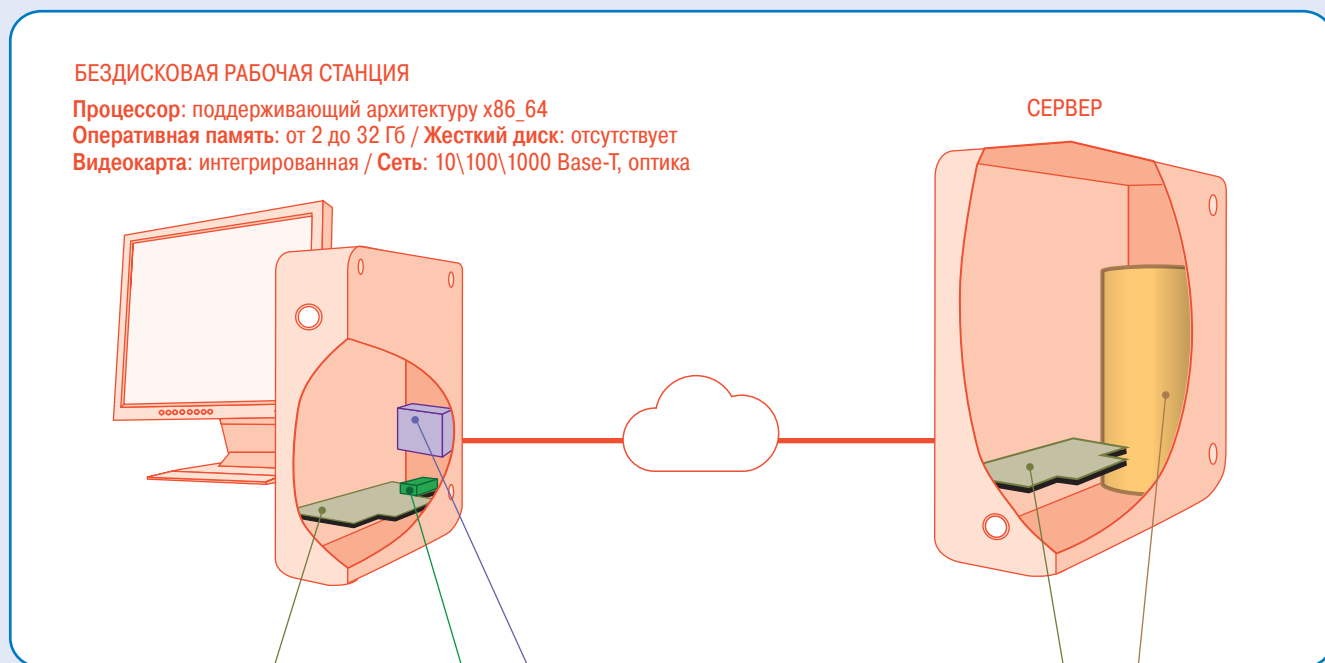
### ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- ✓ 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

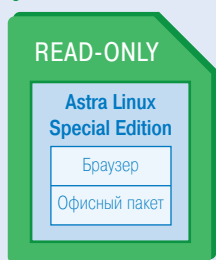
Унифицированное решение предназначено для создания защищенных автоматизированных систем, обрабатывающих информацию до грифа «совершенно секретно» включительно.

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



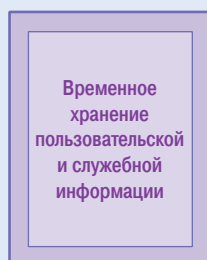
АПМДЗ «МАКСИМ-М1»  
(М-643М1)  
Сертифицированное средство защиты информации от несанкционированного доступа

READ-ONLY  
ФЛЭШ-НАКОПИТЕЛЬ



Энергонезависимая память – microSD карта

ОПЕРАТИВНАЯ ПАМЯТЬ



АПМДЗ «МАКСИМ-М1»  
(М-643М1)  
Сертифицированное средство защиты информации от несанкционированного доступа

ДИСКОВЫЙ RAID-МАССИВ



## 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.

## АПМДЗ «МАКСИМ-А1»

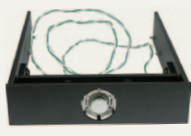
Аппаратно-программный модуль доверенной загрузки «Максим-А1» (изделие М-643А1) предназначен для обеспечения защиты от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну со степенью секретности не выше «совершенно секретно», обрабатываемой на автоматизированных рабочих местах (АРМ), путем реализации надежного контроля доступа пользователей к техническим средствам АРМ и выполнения загрузки доверенной операционной системы (ОС).

АПМДЗ разрабатывается в соответствии с требованиями ФСБ России к аппаратно-программным модулям доверенной загрузки ЭВМ **по классу А1 (многопользовательский режим с удаленным управлением)**.

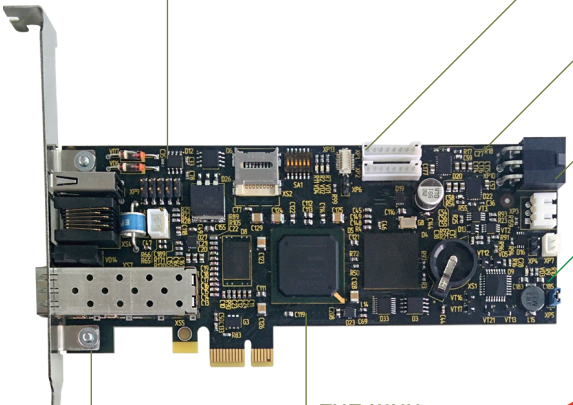
**ТИП СЧИТЫВАТЕЛЯ**




Считыватель внешний



Считыватель внутренний 3,5 / 5,25




- ВЫВОД СУХИХ ГАЛЬВАНИЧЕСКИХ ДАТЧИКОВ
- КАБЕЛЬ БЛОКИРОВКИ ПО СИГНАЛУ RESET
- КАБЕЛЬ БЛОКИРОВКИ ПЭВМ ПО ПИТАНИЮ
- ЭНЕРГОНЕЗАВИСИМАЯ ПАМЯТЬ: MICRO SD КАРТА














micro SD

• ТИП ШИНЫ: PCIe, 1X



ПОДДЕРЖКА (UEFI И LEGACY/PNP BIOS)

**ТИПЫ ПРИМЕНЯЕМЫХ ИНПИ**

<b>iButton</b>		<b>Рутокен</b>			
DS-1995	DS-1996	Рутокен S	Рутокен ЭЦП	Рутокен Lite	Рутокен Lite SC
					
<b>ESMART</b>		<b>JaCarta PKI</b>		<b>ACOS</b>	
ESMART Token ГОСТ	Смарт-карты ESMART	USB-токены и смарт-карты		ACOS3	ACOS5
					

Смарт-карты и USB-токены на базе ИС типа M1K51SC72D с ОС Trust





## АПМДЗ «МАКСИМ-А1»

### ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ПРЕИМУЩЕСТВА

- ✓ выполнение функций администрирования в локальном и удаленном режимах (через защищенный канал на базе ЛВС) с возможностью работы в централизованном (до 256 АРМ в группе) и децентрализованном режимах администрирования;
- ✓ реализация функций доверенного сетевого адаптера на скоростях 10/100/1000 Мбит/с с возможностью ограничения доступа пользователей к ЛВС на базе интерфейса SFP для подключения модулей доступа к среде передачи данных, обеспечивающих возможность работы АПМДЗ в ЛВС как на основе витой пары (RJ-45), так и с оптическими линиями передачи данных со скоростями 1000 Мбит/с (1000 Base-X);
- ✓ полная интеграция со средствами защиты информации операционной системы «Astra Linux Special Edition»;
- ✓ обязательная взаимная аутентификация АПМДЗ в режиме удаленного управления и настраиваемая дополнительная двухфакторная аутентификация администратора до начала сеанса удаленного управления;
- ✓ возможность выполнения задач удаленного управления АПМДЗ как из интерфейса АПМДЗ, так и из операционной системы;
- ✓ возможность мониторинга наличия сетевого подключения к ЛВС с настраиваемой реакцией на событие пропадания связи с ЛВС;
- ✓ реализация функций устройства для одностороннего ввода данных с носителей типа USB MSC с интерфейсом USB 2.0 с возможностью разграничения администратором доступа пользователей к подключаемым носителям;
- ✓ возможность подключения четырех внешних датчиков с выходами типа «сухой контакт»;
- ✓ обеспечение защиты от внешних воздействий, направленных на вывод АПМДЗ из строя;
- ✓ поддержка спецификаций BIOS EFI версии не ниже 1.10 или UEFI версии не ниже 2.1 и Plug and Play BIOS Specification Version 1.0A;
- ✓ возможность подключения дополнительного питания платы АПМДЗ.

#### Поддерживает операционные системы:

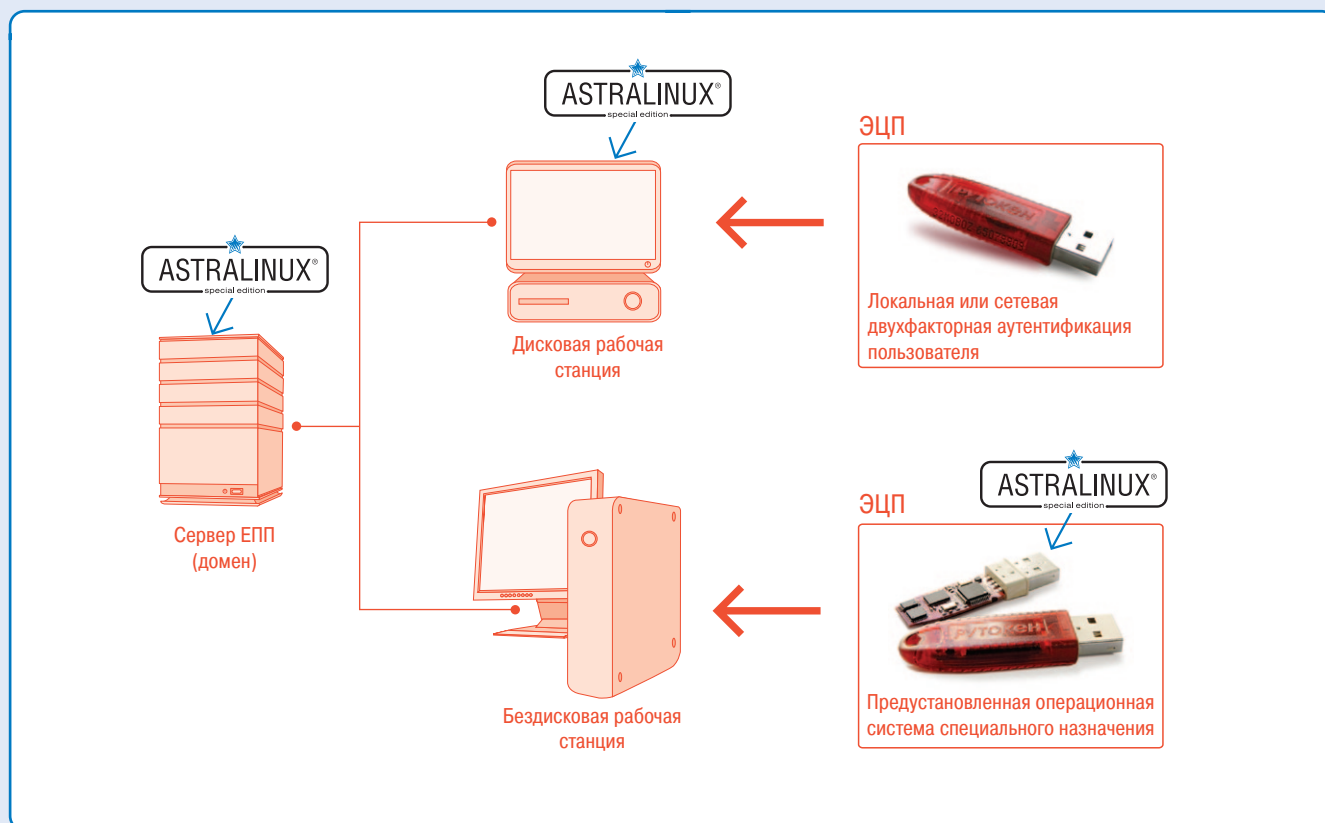
<p>ASTRA LINUX SPECIAL EDITION релизы 1.4 и 1.5</p> 	<p>LINUX Ядро 2.6.x, 3.x или 4.x, Qt версии 4.8.x</p> 	<p>WINDOWS Windows 7 (x86/x64), Windows Server 2008 R2 (x86/x64), Windows 8 (x86/x64), Windows Server 2012 (x86/x64), Windows 8.1 (x86/x64), Windows Server 2012 R2 (x86/x64), Windows 10 (x86/x64), Windows Server 2016 (x86/x64)</p> 
---	---	--

### АПМДЗ «МАКСИМ-А1» ОБЕСПЕЧИВАЕТ:

- ✓ идентификацию/аутентификацию пользователей в начале сеанса работы;
- ✓ КЦ программной среды ЭВМ и файлов пользователей в начале сеанса работы;
- ✓ блокировку попыток загрузки ОС со съемных носителей информации и из ЛВС;
- ✓ регистрацию событий в процессе работы АПМДЗ;
- ✓ локальный и удаленный контроль состояния и администрирование (только для администратора);
- ✓ хранение ПО и данных пользователей в ЭНП АПМДЗ;
- ✓ прием/передачу информации по ЛВС

## 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 АО «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»**

- Установка 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. Электrozаводская, д. 24

**Многоканальный телефон:** +7(495) 223-23-92 (доб. 342)

**Бесплатный звонок из любого региона России:** 8-800-100-05-02 (доб. 342)

## ВИРТУАЛИЗАЦИЯ И УПРАВЛЕНИЕ

### НАЗНАЧЕНИЕ

Программный комплекс «Виртуализация и управление» (далее по тексту — ПК «ВИУ») предназначен для создания защищенной виртуальной среды, обеспечивающей функционирование виртуальных машин и управление ими в операционной системе специального назначения «Astra Linux Special Edition» РУСБ.10015-07 (далее по тексту – ОС СН) в условиях дискреционного и мандатного разграничения доступа.

### ОБЛАСТЬ ПРИМЕНЕНИЯ

Автоматизированные системы в защищенном исполнении, обрабатывающие информацию ограниченного доступа, в том числе содержащую сведения составляющие государственную тайну со степенью секретности до «совершенно секретно» включительно.

### РЕШАЕМЫЕ ЗАДАЧИ

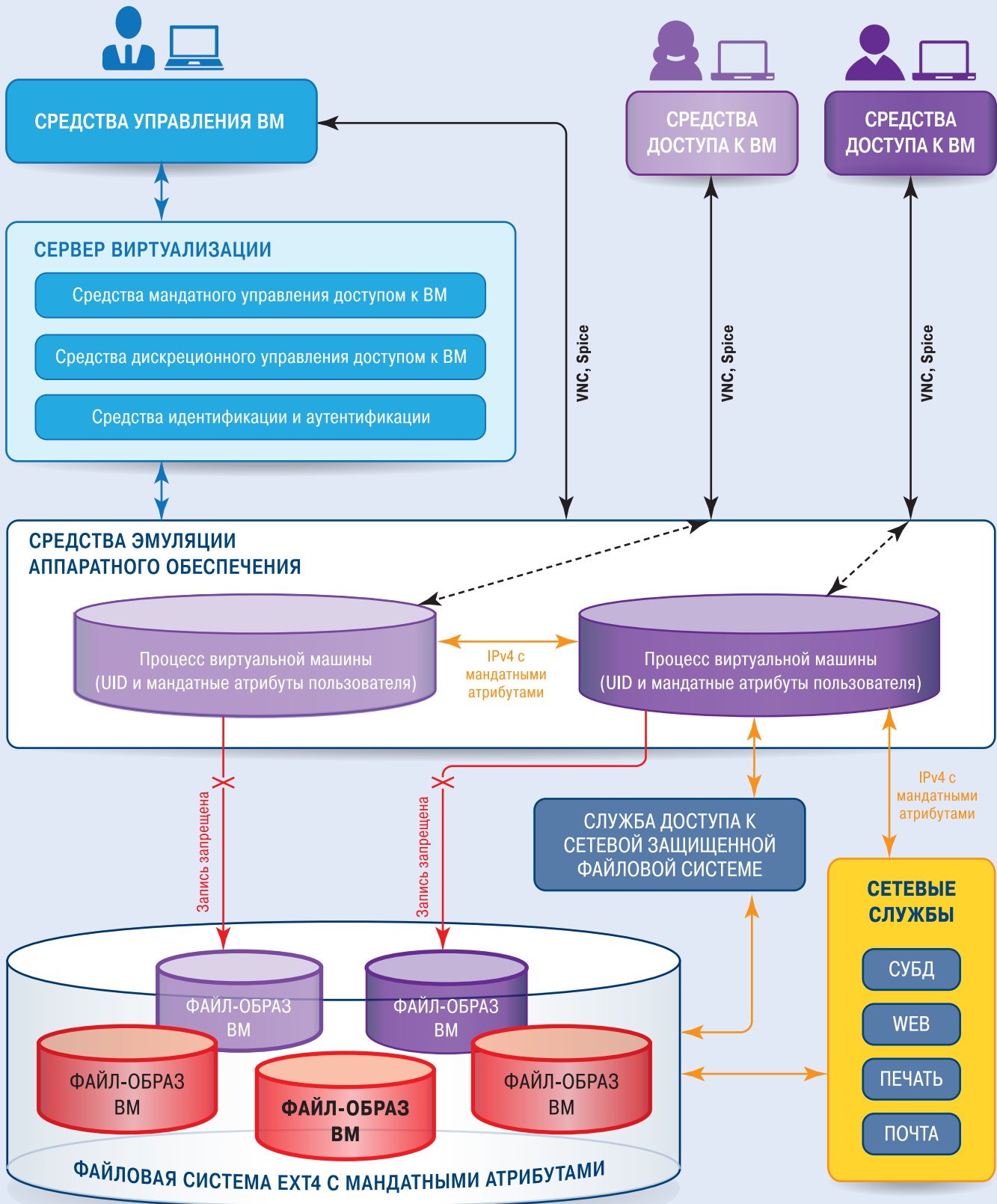
- ✓ обеспечение создания тонких (терминальных) клиентов с использованием технологии VDI;
- ✓ использование аппаратных возможностей архитектуры x86-64 по виртуализации процессоров на основе модуля KVM из состава ОС СН и средств эмуляции аппаратного обеспечения QEMU;
- ✓ идентификация и аутентификация пользователя до предоставления доступа к функциям виртуализации и управления ПК «ВИУ»;
- ✓ создание виртуальных машин с помощью графической и консольных утилит;
- ✓ запуск виртуальной машины в виде отдельного процесса ОС СН, который функционирует от имени учетной записи пользователя с его мандатными атрибутами безопасности;
- ✓ предоставление пользователям удаленного доступа к виртуальным машинам в соответствии с дискреционными и мандатными правилами разграничения доступа;
- ✓ управление конфигурацией виртуальных машин с помощью графической и консольных утилит;
- ✓ взаимодействие между виртуальными машинами по протоколам стека IPv4 в условиях мандатного разграничения доступа;
- ✓ взаимодействие между процессами пользователей и виртуальными машинами по протоколам стека IPv4 в условиях мандатного разграничения доступа;
- ✓ маршрутизация сетевых пакетов виртуальных машин;
- ✓ возможность защиты файлов-образов виртуальных машин от модификации в процессе функционирования виртуальных машин.

### СОСТАВ

Серверная часть	Клиентская часть
<ul style="list-style-type: none"> <li>✓ Средства эмуляции аппаратного обеспечения</li> <li>✓ Сервер виртуализации</li> <li>✓ Служба доступа к сетевой защищенной файловой системе</li> </ul>	<ul style="list-style-type: none"> <li>✓ Консольный интерфейс управления виртуальными машинами</li> <li>✓ Графический интерфейс управления виртуальными машинами</li> <li>✓ Графический интерфейс для удаленного доступа (VDI) пользователей к виртуальным машинам по протоколам VNC и Spice</li> </ul>

## ВИРТУАЛИЗАЦИЯ И УПРАВЛЕНИЕ

### СХЕМА ФУНКЦИОНИРОВАНИЯ





## 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

АО «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



**Галактика ERP**  
Enterprise Resource Planning

Корпорация «Галактика», г. Москва

### Средства контроля защищенности



ЗАО НПО «Эшелон», г. Москва



ООО «Центр Специальной Системотехники», г. Москва



ООО «СЛ Девелопмент», г. Новосибирск

### Системы управления базами данных



ЗАО НПП «РЕЛЭКС», г. Воронеж



SAP Hana, ООО «САП СНГ»



Компания «TMaxSoft», СУБД Tiberio



ООО «Постгрес Профессиональный», г. Москва

### Системы документооборота



ООО «Арта», г. Санкт-Петербург



ООО «Телеформ ИС», г. Москва

### Информационно-справочные системы



ЗАО «Кодекс», г. Санкт-Петербург



ЗАО «КонсультантПлюс», г. Москва

### (УЭК) Универсальные электронные карты



Группа компаний «ISBC», г. Зеленоград



«Группа компаний «Микрон», г. Зеленоград

### Средства аутентификации



Компания «Аладдин Р.Д.», г. Москва



ЗАО «Актив-софт», г. Москва

### Средства антивирусной защиты



ЗАО «Лаборатория Касперского», г. Москва



ООО «Доктор Веб», г. Москва

### Гео-информационные системы



ОАО «НИИАА», г. Москва



ЗАО КБ «Панорама», г. Москва

### DLP-системы



ООО «СёрчИнформ», г. Москва

### Обучающие программы



Консалтинговая группа «ТЕРМИКА», г. Москва

### Средства криптографической защиты



ОАО «ИнфоТекС», г. Москва



ООО «КРИПТО-ПРО», г. Москва



ООО «ЛИССИ-Крипто», г. Юбилейный

### Технология миграции



АО «НПК Пеленгатор», г. Санкт-Петербург

### Системы IP-телефонии и видео-конференцсвязи



MIND, г. Москва



Компания «TooLabs», г. Тула



ПАО «Информационные телекоммуникационные технологии», г. Санкт-Петербург

**БОЛЕЕ 80 ОТЕЧЕСТВЕННЫХ КОМПАНИЙ-ПАРТНЕРОВ**

## 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](mailto: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](mailto:support@rusbitech.ru)  
<http://www.astra-linux.ru>









Научно-производственное объединение  
**РусБИТех**  
Акционерное общество

**ВАШ НАДЕЖНЫЙ  
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](mailto:mail@rusbitech.ru) / Сайт: [www.rusbitech.pф](http://www.rusbitech.pф)