

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет
информационных технологий и
электроники

Специальность 10.05.03 –

Специализация –

Кафедра
«Информационная безопасность
систем и технологий»

Информационная безопасность
автоматизированных систем

Защищенные
автоматизированные системы
управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

МЕТОДИКА НАСТРОЙКИ ОПЕРАЦИОННОЙ
СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ
«ASTRA LINUX SPECIAL EDITION» ДЛЯ
ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ,
СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ
ГОСУДАРСТВЕННУЮ ТАЙНУ

Студент

Руководитель

Нормоконтролёр

Рецензент

Работа допущена к защите (протокол заседания кафедры от
10.06.22г. № 9)

Заведующий кафедрой

Работа защищена с отметкой (протокол заседания ГЭК от
23.06.22г. № 5)

Секретарь ГЭК

Иванов М.С.

Сафронкин Д.Н.

Егорова Н.А.

Маркин В.В.

Пенза 2022

Оглавление

Введение	4
1 Анализ возможности использования защищенных операционных систем в автоматизированных системах, предназначенных для обработки информации, составляющей государственную тайну.....	6
1.1 Анализ понятия защищенной операционной системы.....	6
1.2 Анализ возможности применения операционных систем семейства Windows для обработки информации, составляющей государственную тайну ...	7
1.3 Анализ возможности применения операционных систем семейства Linux для обработки информации, составляющей государственную тайну	9
1.4 Анализ актуальных средств защиты информации.....	11
1.5 Выбор и обоснование выбора операционной системы для использования в составе автоматизированной системы, обрабатывающей информацию, содержащую сведения, составляющие государственную тайну .	12
2 Анализ руководящих документов по защите информации, содержащей сведения, составляющие государственную тайну.....	15
3 Разработка модели угроз и действий нарушителя для объекта информатизации	21
3.1 Основные сведения об объекте информатизации.....	21
3.2 Модель угроз безопасности защищаемой информации	22
3.3 Модель нарушителя.....	23
4 Анализ встроенных механизмов безопасности настройки операционной системы специального назначения «Astra Linux Special Edition»	30
5 Разработка методики настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну ...	32
5.1 Разработка требований к методике настройки операционной системы специального назначения «Astra Linux Special Edition»	32
5.2 Разработка методики настройки операционной системы специального назначения «Astra Linux Special Edition»	34

6 Разработка программного обеспечения автоматической настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.....	43
7 Проверка методики настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну ...	49
8 Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	61
Заключение	64
Список используемых источников.....	65

Введение

Актуальность проблемы защиты информации в современном мире связана, в первую очередь, с ценностью информации и развитием технологий. В настоящее время существует большое количество средств защиты информации, в том числе защищенных операционных систем. Но не все средства защиты могут обеспечивать защиту информации, содержащую сведения, составляющие государственную тайну.

Целью настоящего дипломного проекта является разработка методики настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.

Разрабатываемая методика может быть применена для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну, в уже разработанной и разрабатываемой аппаратуре.

Первая глава дипломного проекта посвящена анализу возможности использования защищенных операционных систем в автоматизированных системах, предназначенных для обработки информации, составляющей государственную тайну.

Во второй главе был произведен анализ руководящих документов по защите информации, содержащей сведения, составляющие государственную тайну.

В третьей главе была произведена разработка модели угроз и действий нарушителя для объекта информатизации.

Четвертая глава посвящена анализу встроенных механизмов безопасности настройки операционной системы специального назначения «Astra Linux Special Edition».

В пятой главе дипломного проекта была произведена разработка методики настройки операционной системы специального назначения «Astra

Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.

В шестой главе была произведена разработка скриптов для автоматической настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.

Седьмая глава посвящена проверке методики настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.

В восьмой главе были рассмотрены вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.

1 Анализ возможности использования защищенных операционных систем в автоматизированных системах, предназначенных для обработки информации, составляющей государственную тайну

1.1 Анализ понятия защищенной операционной системы

На данный момент защищенные операционные системы рассматриваются преимущественно в составе автоматизированных систем. Автоматизированная система – это система, состоящая из персонала и совокупности аппаратных средств и программного обеспечения. Именно поэтому в операционной системе должен обеспечиваться комплекс средств защиты информации, основанный на актуальных угрозах безопасности информации рассматриваемых систем. Средства защиты информации — это совокупность организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации [1]. Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [2]. Актуальной же считается такая угроза, которая может быть реализована в системе и представляет опасность для системы.

Для того, чтобы дать полное и точное определение защищенной операционной системы, необходимо ввести следующие определения:

- источник угрозы безопасности информации — субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации [3];

- операционная система считается адекватной актуальным угрозам безопасности информации, если политика безопасности операционной системы постоянно корректируется в соответствии с перечнем актуальных угроз безопасности информации, источников угроз безопасности информации, изменениями в конфигурации операционной системы.

Для обработки информации, составляющей государственную тайну, автоматизированная система должна иметь сертификат соответствия требованиям к средствам защиты информации от несанкционированного доступа в соответствии с направлением применения:

- МО РФ;
- ФСТЭК РФ;
- ФСБ РФ.

Для возможности обработки информации, составляющей государственную тайну, в АС защита информации может обеспечиваться с помощью:

- операционные системы (имеющей сертификат соответствия средств защиты информации от несанкционированного доступа);
- совокупности сертифицированных средств защиты информации от несанкционированного доступа, не входящих в состав операционной системы.

Таким образом, защищенная операционная система — это операционная система, которая:

- реализует заданные требования безопасности;
- адекватна актуальным УБИ;
- имеет сертификат соответствия требованиям к средствам защиты информации от несанкционированного доступа;
- не имеет возможности несанкционированного влияния на её работу извне [4].

1.2 Анализ возможности применения операционных систем семейства Windows для обработки информации, составляющей государственную тайну

Основные достоинства операционных систем семейства Windows:

- стабильность и надежность;
- удобный для пользователя графический интерфейс;

- поддержка подключаемых устройств.

Так, версии Windows NT/2000 были сертифицированы по классу C2 критериев TCSEC [5]. Следовательно, версии операционной системы Windows NT/2000 обеспечивают выполнение требований:

- обязательная идентификация и аутентификация всех пользователей операционной системы;
- обеспечение системного аудита;
- наличие разграничительного контроля доступа;
- защита объектов от повторного использования [6].

Тем не менее, вопрос доверия к разработчику операционных систем становится все более актуальным при выборе защищенных операционных систем. Так, актуальность и простота операционных систем семейства Windows имеет существенный недостаток, заключающийся в возможности сбора данных пользователей производителем. На этих выводах основано «обеспечение информационной безопасности на основе отечественных разработок при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, бизнеса и государства» [7].

Операционные системы Microsoft Windows XP Professional (SP2/SP3) имели действующие сертификаты ФСТЭК России [8] вплоть до 3.12.2016 для SP2 и 3.12.2014 для SP3 для использования в составе автоматизированных систем до класса защищенности 1Г включительно [9].

На момент написания работы сертифицированными ФСТЭК России [8] являются следующие операционные системы семейства Windows:

- Microsoft Windows 10 в редакции Корпоративная (шестого класса защиты. ИТ.ОС.А6.ПЗ, сертификат действителен до 10.02.2026);
- Microsoft Windows Server 2016 (шестого класса защиты. ИТ.ОС.А6.ПЗ, сертификат действителен до 29.08.2023).

При этом, ни одна из сертифицированных операционных систем

семейства Windows не подходит для обработки сведений, составляющих государственную тайну. Для обработки информации, составляющей государственную тайну на автоматизированной системе с операционной системой Microsoft Windows, требуется применение совокупности внешних сертифицированных средств защиты информации от несанкционированного доступа. Автоматизированная система в таком составе должна быть аттестована по требованиям руководящих документов (МО РФ, ФСТЭК РФ или ФСБ РФ) в соответствии с классом и категории обрабатываемой информации и иметь соответствующее Предписание на эксплуатацию.

1.3 Анализ возможности применения операционных систем семейства Linux для обработки информации, составляющей государственную тайну

Основными компонентами, обеспечивающими защиту информации в операционных системах семейства Linux, являются:

- POSIX ACL — разграничение прав доступа к файлам на основе их атрибутов;
- Sudo — выполнение программ от своего и/или чужого имени;
- Chroot — операция, ограничивающая доступ процесса к файловой системе, изменяя её корень в контексте процесса;
- PAM — подключаемые модули аутентификации;
- SELinux — система принудительного контроля доступа, основанная на политиках и контекстах безопасности;
- AppArmor — система упреждающей защиты, основанная на политиках безопасности;
- PolicyKit — средство контроля системных привилегий.

Используемые в операционных системах семейства Linux механизмы защиты позволяют реализовать в операционной системе современные механизмы мандатного и ролевого управления доступом, мандатного контроля

целостности, добиться строгого теоретического обоснования безопасности и верификации полученного решения. Таким образом, сочетание высокой надежности, приемлемых потребительских качеств, открытого исходного кода и возможности доработки механизмов защиты операционных систем семейства Linux позволяет построить на их базе защищенную отечественную операционную систему [4].

На момент написания работы сертифицированными ФСТЭК России [8] являются следующие операционные системы семейства Linux:

- SUSE Linux Enterprise Server for SAP Applications 15 SP3 (шестого класса защиты. ИТ.ОС.А6.ПЗ, сертификат действителен до 17.12.2026);
- Red Hat Enterprise Linux 7 (шестого класса защиты. ИТ.ОС.А6.ПЗ, сертификат действителен до 21.05.2026);
- Red Hat Enterprise Linux 8 (шестого класса защиты. ИТ.ОС.А6.ПЗ, сертификат действителен до 14.05.2026);
- операционная система специального назначения «Astra Linux Special Edition» (второго класса защиты/ ИТ.ОС.А2.ПЗ, сертификат действителен до 27.01.2026);
- SUSE Linux Enterprise Server 12 SP3 (четвертого класса защиты. ИТ.ОС.А4.ПЗ, сертификат действителен до 03.12.2023);
- «Эльбрус» Эльбрус-Д (ТВГИ.00950-01);
- «AlterOS» (А четвертого класса защиты. ИТ.ОС.А4.ПЗ, сертификат действителен до 26.04.2026);
- защищенная мобильная операционная система общего назначения на базе Sailfish Mobile OS RUS (шестого класса защиты. ИТ.ОС.А6.ПЗ, сертификат действителен до 29.01.2029);
- «Альт 8 СП» (четвертого класса защиты. ИТ.ОС.А4.ПЗ, сертификат действителен до 10.08.2023);
- «Заря» (сертификат соответствия МО РФ № 3287).

Пригодными для обработки информации, составляющей государственную тайну, являются отечественные ОС:

- «Эльбрус» Эльбрус-Д (ТВГИ.00950-01);
- операционная система специального назначения (ОСЧН) «Astra Linux Special Edition»;
- «Заря» (сертификат соответствия МО РФ № 3287).

1.4 Анализ актуальных средств защиты информации

Для обеспечения возможности обработки информации, составляющей государственную тайну на автоматизированной системе с операционной системой, не имеющей сертификата соответствия требованиям к средствам защиты информации от несанкционированного доступа, должны быть использованы сторонние сертифицированные средства защиты информации, такие, как:.

- СЗИ Secret Net Studio (сертификат соответствия ФСТЭК России [8] действителен до 16.05.2025);
- программно-аппаратный комплекс «Соболь». Версия 3.0 (сертификат соответствия ФСТЭК России [8] действителен до 07.12.2023);
- программно-аппаратный комплекс «Соболь». Версия 4» (сертификат соответствия ФСТЭК России [8] действителен до 05.12.2023);
- программа инспекционного контроля «ПИК-Эшелон» (сертификаты соответствия Министерства обороны России №3752, 3753, 3754);
- аппаратно-программный модуль доверенной загрузки «Цезарь» (варианты исполнения: ЦАВМ.468266.008, ЦАВМ.468266.008-01, ЦАВМ.468266.008-02, ЦАВМ.468266.008-03) (сертификат соответствия ФСБ России [10] действителен до 31.07.2023, класс защищенности 1Б);
- аппаратно-программный модуль доверенной загрузки «Центурион-Е» ИТБВ.468266.002 (сертификат соответствия ФСБ России [10] действителен

до 20.08.2026, класс защищенности 1Б);

- аппаратно-программный модуль доверенной загрузки «Максим-М1» (сертификат соответствия ФСБ России [10] действителен до 25.12.2022, класс защищенности 1Б);

- программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ» (сертификат соответствия ФСБ России [10] действителен до 30.04.2022, класс защищенности 1Б);

- комплекс программ «Защищенная операционная система «СинтезМ» (сертификат соответствия ФСБ России [10] действителен до 31.10.2022 2 класса защищенности);

- защищенная операционная система «QR ОС» (сертификат соответствия ФСБ России [10] действителен до 20.11.2023, соответствует требованиям ФСБ России к программному обеспечению, используемому в информационных и телекоммуникационных системах специального назначения, и может использоваться для обработки информации, содержащей сведения, составляющие государственную тайну, при условии выполнения требований эксплуатационной документации согласно формуляру РНДК.00390-01 30 01).

1.5 Выбор и обоснование выбора операционной системы для использования в составе автоматизированной системы, обрабатывающей информацию, содержащую сведения, составляющие государственную тайну

На основании предыдущих этапов был сделан вывод о том, что перспективная отечественная защищенная операционная система должна отвечать следующим требованиям:

- соответствие требованиям обеспечения технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи;

- функционирование в компьютерных сетях, как изолированных, так и подключенных к телекоммуникационным сетям, в том числе

ориентированных на обработку информации, отнесенной к государственной тайне, или персональных данных;

- имеет сертификат соответствия требованиям к средствам защиты информации от несанкционированного доступа по направлениям ФСБ, ФСТЭК, МО РФ [4].

Этим требованиям соответствуют операционные системы:

- «Эльбрус» Эльбрус-Д (ТВГИ.00950-01);
- операционная система специального назначения (ОСЧН) «Astra Linux Special Edition»;
- комплекс программ «Защищенная операционная система «СинтезМ»;
- защищенная операционная система «QR ОС»;
- «Заря» (сертификат соответствия МО РФ № 3287).

При этом «Эльбрус» работает лишь на процессорах линейки «Эльбрус», что существенно сужает область применения данной операционной системы на отечественном рынке.

Защищенная операционная система «СинтезМ» является серверной операционной системой, что существенно сужает область применения данной операционной системы на отечественном рынке.

Защищенная операционная система «QR ОС» является собственной разработкой ООО НТП «Криптософт», имеет пакет собственных приложений и не имеет возможности использования сторонних приложений, что существенно сужает область применения данной операционной системы на отечественном рынке.

«Заря» является операционной системой, предназначенной для Министерства обороны РФ. Система сертифицирована Минобороны России, соответствует третьему классу защиты от несанкционированного доступа и второму уровню контроля отсутствия недеklarированных возможностей.

Операционная система специального назначения «Astra Linux Special Edition» имеет сертификат 2 класса защиты ФСТЭК России [8] и класса защиты 1Б ФСБ России [10], потому является наиболее актуальной операционной системой из рассматриваемых. Тем не менее, операционная система не может обеспечивать требуемый уровень защищенности информации без настройки ее компонентов защиты. Для корректной настройки компонентов защиты должна быть разработана универсальная методика настройки операционной системы специального назначения «Astra Linux Special Edition».

2 Анализ руководящих документов по защите информации, содержащей сведения, составляющие государственную тайну

На данном этапе был произведен анализ руководящих документов по защите информации, содержащей сведения, составляющие государственную тайну.

Были выявлены основные понятия:

— государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ;

— носители сведений, составляющих государственную тайну – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов сигналов, технических решений и процессов;

— допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений;

— доступ к сведениям, составляющим государственную тайну – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

— гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и/или в сопроводительной документации на него;

— средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации;

— перечень сведений, составляющих государственную тайну – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством; [11]

— режимные объекты – военные и специальные объекты, воинские части, предприятия, организации, учреждения для функционирования которых установлены дополнительные меры безопасности [12];

— угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [13];

— объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [14];

— контролируемая зона – пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств [15];

— криптографически опасная информация – информация о состояниях криптосредства, знание которой нарушителем позволит ему строить алгоритмы определения ключевой информации (или ее части) или алгоритмы бесключевого чтения [16].

Согласно статье 5 закона РФ от 21.07.1993 №5485-1 «О государственной тайне», государственную тайну составляют:

1) сведения в военной области:

— о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому,

оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

— о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

— о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

— о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

— о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

— о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке.

2) Сведения в области экономики, науки и техники:

— о содержании планов подготовки Российской Федерации и ее

отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

— об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

— о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

— об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

— о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

— о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации).

3) Сведения в области внешней политики и экономики:

— о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;

— о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты:

— о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной, оперативно-розыскной деятельности и деятельности по противодействию терроризму, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

— о силах, средствах, об источниках, о методах, планах и результатах деятельности по обеспечению безопасности лиц, в отношении которых принято решение о применении мер государственной защиты, данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения, а также отдельные сведения об указанных лицах;

— о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

— об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают

перечисленные сведения;

- о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;

- о методах и средствах защиты секретной информации;

- об организации и о фактическом состоянии защиты государственной тайны;

- о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;

- о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;

- о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства;

- о мерах по обеспечению защищенности критически важных объектов и потенциально опасных объектов инфраструктуры Российской Федерации от террористических актов;

- о результатах финансового мониторинга в отношении организаций и физических лиц, полученных в связи с проверкой их возможной причастности к террористической деятельности;

- о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак.

3 Разработка модели угроз и действий нарушителя для объекта информатизации

3.1 Основные сведения об объекте информатизации

Под объектом информатизации будем рассматривать автоматизированную систему, которая:

- состоит из локальной сети не имеющей прямого канала связи с внешней средой;
- расположена в пределах контролируемой зоны;
- имеет в составе персональную электронно вычислительную машину с установленной операционной системой специального назначения «Astra Linux Special Edition».

Рассматриваемая аппаратура должна обеспечивать следующие функции:

- обработку информации содержащую сведения, составляющие государственную тайну:
 - ввод с клавиатуры;
 - ввод/вывод с/на внешние носители;
- работа нескольких пользователей;
- администрирование работы пользователей;
- ведение журнала аудита;
- разграничение прав доступа пользователей.

Основные информационные процессы, происходящие в рассматриваемой аппаратуре:

- ввод информации, содержащей сведения, составляющие государственную тайну;
- вывод информации, содержащей сведения, составляющие государственную тайну;
- изменение информации, содержащей сведения, составляющие государственную тайну;

- создание нового пользователя;
- вход пользователя в систему;
- создание пользователя с правами администратора;
- запись действий пользователей в журнал аудита;
- чтение пользователем с правами администратора записей журнала аудита;
- вывод на носитель пользователем с правами администратора записей журнала аудита;
- обеспечение разграничения доступа к файлам и программам пользователей.

3.2 Модель угроз безопасности защищаемой информации

На основании рассматриваемого объекта информатизации были определены следующие основные угрозы безопасности информации:

- несанкционированное ознакомление с обрабатываемой информацией (включая совокупность сведений, определяющих топологию сети связи);
- несанкционированное ознакомление с передаваемой информацией;
- блокирование санкционированного доступа к информации пользователей;
- удаленное проникновение;
- локальное проникновение;
- отказ в обслуживании.

Основными механизмами атак на объект информатизации являются:

- сбор информации;
 - изучение окружения;
 - идентификация топологии сети;
 - определение роли узла;
- использование легальных каналов доступа к информации;

- использование скрытых каналов доступа к информации;
- создание новых каналов получения информации. [17]

Для успешной реализации угрозы требуется выполнение следующих условий:

- наличие у нарушителя цели атаки;
- наличие у нарушителя соответствующей квалификации, информированности о функционировании изделия и особенностях его эксплуатации, а также о слабостях системы защиты, позволяющих создавать способы атак;
- наличие у нарушителя необходимых технических и программных средств для проведения атаки;
- доступность для нарушителя необходимых каналов для проведения атаки.

3.3 Модель нарушителя

Все возможные потенциальные нарушители могут быть отнесены к следующим категориям:

- нарушитель с низким потенциалом;
- нарушитель со средним потенциалом;
- нарушитель с высоким потенциалом.

Категория нарушителей с низким потенциалом содержит внешних нарушителей, не имеющих доступа в контролируемую зону. К нарушителям данной категории можно отнести следующие группы лиц:

- вооруженные силы и спецслужбы иностранных государств;
- представители террористических и криминальных группировок;
- физические лица, пытающиеся получить доступ к информации.

Категория нарушителей со средним потенциалом содержит нарушителей, имеющих право доступа в контролируемую зону, но не имеющих право эксплуатации и/или обслуживания рассматриваемой аппаратуры.

К нарушителям данной категории можно отнести следующие группы лиц:

- сотрудники, в обязанности которых входит охрана периметра, уборка территории;
- сотрудники других организаций и подразделений, имеющие право постоянного или разового доступа в контролируемую зону.

Категория нарушителей с высоким потенциалом содержит нарушителей, имеющих право доступа в контролируемую зону и имеющих право эксплуатации и/или обслуживания рассматриваемой аппаратуры.

К нарушителям данной категории можно отнести следующие группы лиц:

- пользователи рассматриваемой аппаратуры;
- технический персонал, обеспечивающий обслуживание рассматриваемой аппаратуры.

Нарушители подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны;
- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны.

К внешним нарушителям относятся лица из категории нарушителей с низким потенциалом, а к внутренним нарушителям относятся лица из категорий нарушителей с высоким и средним потенциалами.

Предполагается, что внешний нарушитель обладает высоким уровнем знаний в области программирования, вычислительной техники, схемотехники, проектирования и эксплуатации систем связи и средств защиты информации.

При построении методов и средств атак внешний нарушитель обладает информацией:

- об аппаратных, программных и программно-аппаратных компонентах аппаратуры и алгоритмах её функционирования;
- об информационных потоках и обо всех протоколах информационно-логического взаимодействия, о правилах передачи

информации, регламентируемых этими протоколами, о структуре и форматах передаваемых сообщений;

- о конфигурации аппаратных и программных средств;
- о возможных уязвимостях, недеklarированных возможностях и закладках в программных и аппаратных средствах;
- о правилах эксплуатации аппаратуры и о применяемых организационных мерах защиты.

Внешний нарушитель может применять следующие средства атак:

- агентурные средства и методы получения информации;
- средства воздействия через цепи питания и заземления, выходящие за пределы контролируемой зоны;
- штатные программно-аппаратные средства передачи данных, находящиеся вне контролируемой зоны;
- средства перехвата и обработки информации в каналах распространения побочных сигналов за пределами контролируемой зоны;
- средства приема и обработки информации, поступающей от возможно внедренных специальных электронных закладочных устройств за пределами контролируемой зоны;
- доступные в свободной продаже средства разработки и отладки программного обеспечения;
- средства физического уничтожения пользователей и обслуживающего персонала при эксплуатации аппаратуры в особых условиях.

При осуществлении атак внешний нарушитель обладает возможностями по:

- определению структуры передаваемой за пределами контролируемой зоны информации;
- выделению и использованию всех возможных нарушений правил эксплуатации и отказов в работе оборудования;
- использованию присутствующих недеklarированных программных

и аппаратных возможностей и закладок.

Предполагается, что внутренний нарушитель:

- обладает высоким уровнем знаний в области программирования, вычислительной техники, схемотехники, проектирования и эксплуатации систем связи и средств защиты информации;
- знает схемы организации связи и закономерности формирования потоков информации;
- обладает знаниями о порядке эксплуатации аппаратуры;
- обладает возможностями по несанкционированным действиям с использованием штатных средств.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основными являются организационно-режимные мероприятия, направленные на:

- предотвращение и пресечение несанкционированных действий;
- подбор и расстановку кадров;
- контроль допуска физических лиц в контролируемую зону и к программно-аппаратным средствам;
- контроль за порядком проведения работ.

При осуществлении атак внутренний нарушитель обладает возможностями по осуществлению:

- хищения съемных носителей;
- вскрытия корпуса аппаратуры с целью получения информации;
- подключения к кабельной системе для получения доступа к обрабатываемой информации.

Внутренний нарушитель заинтересован в сокрытии признаков несанкционированного доступа, в связи с чем он не будет предпринимать действий по нарушению целостности технических средств при выполнении несанкционированных действий, а также не будет предпринимать действий,

приводящих к полному или частичному нарушению доступа к обрабатываемой информации.

К тому же, внутренний нарушитель категории 2 не располагает сведениями о текущих настройках аппаратуры.

Были выделены основные каналы атак:

- каналы связи, кабельные системы и коммутационное оборудование за пределами контролируемой зоны;
- каналы связи, кабельные системы и коммутационное оборудование в пределах контролируемой зоны;
- каналы непосредственного физического доступа;
- побочные каналы утечки побочных электромагнитных излучений и наводок, выходящие за пределы контролируемой зоны;
- побочные каналы утечки побочных электромагнитных излучений и наводок, образованные за счет электроакустических преобразований;
- каналы, образованные электронными устройствами негласного получения информации;
- съемные носители информации.

Основными объектами атак нарушителя являются:

- защищаемая информация;
- средства и система защиты информации;
- технические, программные и программно-технические средства, нарушение функционирования которых может привести к реализации угроз безопасности информации или которые могут повлиять на функционирование средств и системы защиты информации.

Целью атак нарушителя является нарушение свойств безопасности информации: конфиденциальности, целостности и доступности.

Было произведено сопоставление категорий нарушителей возможным каналам атак. Результат представлен в таблице 1.

Для удобства отображения каналы атак были пронумерованы:

- каналы связи, кабельные системы и коммутационное оборудование за пределами контролируемой зоны — 1;
- каналы связи, кабельные системы и коммутационное оборудование в пределах контролируемой зоны — 2;
- каналы непосредственного физического доступа — 3;
- побочные каналы утечки побочных электромагнитных излучений и наводок, выходящие за пределы контролируемой зоны — 4;
- побочные каналы утечки побочных электромагнитных излучений и наводок, образованные за счет электроакустических преобразований — 5;
- каналы, образованные электронными устройствами негласного получения информации — 6;
- съемные носители информации — 7.

Таблица 1 — Сопоставление категорий нарушителей возможным каналам атак

№	Категория нарушителя	Каналы атак
1	Категория нарушителей с низким потенциалом	1, 4, 5
2	Категория нарушителей со средним потенциалом	1, 2, 3, 4, 5, 6
3	Категория нарушителей с высоким потенциалом	2, 3, 7

Был произведен анализ способов атак, а также сопоставление категорий нарушителей способам атаки и каналам атак. Результат представлен в таблице 2.

Таблица 2 — Соотношение категорий нарушителей, способов атаки и каналов атаки

№	Категория нарушителя	Способ атаки	Канал атаки
1	Категория нарушителей с низким потенциалом	Перехват за пределами контролируемой зоны информации.	1,4

Продолжение таблицы 2

№	Категория нарушителя	Способ атаки	Канал атаки
2	Категория нарушителей со средним потенциалом	Перехват информации, попавшей в каналы связи.	2,5
3	Категория нарушителей с высоким потенциалом	Атаки, основанные на программных и аппаратных уязвимостях, недеklarированных возможностях программного обеспечения, позволяющих осуществлять: — внедрение вредоносного кода; — несанкционированную модификацию программного кода.	2, 3, 7
4	Категория нарушителей с низким потенциалом	Проникновение в контролируемую зону с целью несанкционированного доступа.	3
5	Категория нарушителей с высоким потенциалом	Целенаправленное искажение обрабатываемой информации.	2, 3, 7
6	Категория нарушителей со средним потенциалом	Визуальный просмотр защищаемой информации на экране монитора.	3

4 Анализ встроенных механизмов безопасности настройки операционной системы специального назначения «Astra Linux Special Edition»

На данном этапе был произведен анализ встроенных механизмов безопасности настройки операционной системы специального назначения «Astra Linux Special Edition», встроенной в рассматриваемую аппаратуру.

Операционная система специального назначения «Astra Linux Special Edition» содержит следующие механизмы защиты:

- аутентификация пользователей с использованием инфраструктуры РАР;
- дискреционное управление доступом процессов к ресурсу поддержкой ACL;
- мандатный контроль целостности процессов к ресурсам;
- мандатное управление доступом процессов к ресурсам;
- изоляция адресных пространств процессов;
- регистрация и аудит событий, реализованные в виде централизованной системы с функцией оповещения администратора безопасности о попытках несанкционированного доступа;
- очистка оперативной памяти и освобождаемых областей данных на запоминающих устройствах;
- регламентный контроль целостности файловой системы;
- создание замкнутой программной среды;
- контроль замкнутой программной среды;
- маркировка документов при выводе их на печать;
- обеспечение надёжного восстановления ОССН после сбоев;
- реализация правил управления доступом к внешним запоминающим устройствам;
- обеспечение доступа к реляционным базам данных;
- обеспечение доступа к информации через сервер гипертекстовой

обработки данных;

- обеспечение обмена сообщениями электронной почты [18].

5 Разработка методики настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.

5.1 Разработка требований к методике настройки операционной системы специального назначения «Astra Linux Special Edition»

Был составлен перечень требований к настройке операционной системы специального назначения «Astra Linux Special Edition».

Требования к парольной политике и политике учетных записей:

- срок действия пароля: 30 дней;
- пароли должны храниться в виде хэшей;
- пароль должен состоять из русских и латинских строчных и прописных букв, а также арабских цифр;
- минимальная длина пароля: 8 символов;
- число дней выдачи предупреждения до смены пароля: 7 дней;
- число дней неактивности учетной записи пользователя до ее блокировки после устаревания пароля: 3 дня;
- ограничить повторное использование пароля: не менее 5 уникальных паролей;
- минимальное количество отличных символов в пароле: 4;
- количество неудачных попыток входа: 3;
- период блокировки учетной записи пользователя: 10 минут.

Требования к политике разграничения доступа:

- отключить доступ к консоли пользователям;
- ограничить доступ к root через su;
- ограничить права на crontab файл;
- ограничить вход суперпользователя в виртуальную консоль;
- ограничить вход суперпользователя через последовательный порт;
- системные исполняемые файлы не должны быть доступны на

запись для всех учётных записей;

- системные разделяемые библиотеки не должны быть доступны на запись для всех учётных записей.

Требования к настройкам ядра:

- настроить загрузчик на загрузку ядра GENERIC, и исключить из меню все другие варианты загрузки, включая режимы восстановления;

- отключить параметры ядра для перенаправлений ICMP по умолчанию;

- отключить параметры ядра для IP Forwarding;

- отключить параметры ядра для принятия Source-Routed пакетов по умолчанию;

- включить параметра ядра для игнорирования ICMP Broadcast Echo запросов;

- включить параметр ядра для использования фильтрации обратного пути у всех интерфейсов;

- отключить механизм SysRq;

- включить параметр ядра для использования TCP syncookies;

- заблокировать исполнение модулей python с расширенным функционалом;

- размер дампа ядра: 0;

- максимальный размер создаваемого файла: 50000000;

- максимальное количество процессов: 1000;

- заблокировать макросы в VLC.

Требования к настройкам операционной системы:

- установить пароль загрузчика;

- отключить все неиспользуемые сервисы;

- установить запрет установки исполняемого бита;

- включить контроль цифровой подписи;

- настроить режим «КИОСК» для обеспечения ограничения прав

пользователей в системе;

- настроить подключение внешних носителей.

5.2 Разработка методики настройки операционной системы специального назначения «Astra Linux Special Edition»

Была произведена разработка методики настройки операционной системы специального назначения «Astra Linux Special Edition».

Методика настройки операционной системы специального назначения «Astra Linux Special Edition» включает в себя следующие разделы:

- 1) установка операционной системы специального назначения «Astra Linux Special Edition»;
- 2) настройка парольной политики операционной системы специального назначения «Astra Linux Special Edition»;
- 3) настройка политики разграничения доступа к файлам и компонентам операционной системы специального назначения «Astra Linux Special Edition»;
- 4) настройка параметров ядра операционной системы специального назначения «Astra Linux Special Edition»;
- 5) настройка параметров операционной системы специального назначения «Astra Linux Special Edition».

Раздел 1. Установка операционной системы специального назначения «Astra Linux Special Edition».

В процессе установки операционной системы специального назначения «Astra Linux Special Edition» должны быть выбраны следующие параметры:

- язык системы — «Russian - Русский»;
- метод разметки диска — «Авто — использовать весь диск». Данный параметр является оптимальным для рассматриваемой аппаратуры, так как в ней присутствует только 1 встроенный физический носитель информации;
- схема разметки — «Отдельный раздел для /home»;

После выставления представленных параметров, а также предпочитаемой комбинации клавиш смены раскладки клавиатуры, имени системы в сети и имени администратора, необходимо произвести проверку правильности разметки носителя и выбрать строку «Закончить разметку и записать изменения на диск».

Затем необходимо произвести выбор устанавливаемых компонентов программного обеспечения. Должны быть установлены следующие компоненты:

- базовые средства;
- рабочий стол Fly;
- средства работы в сети;
- СУБД.

Данные параметры необходимы для корректной работы рассматриваемой аппаратуры. Все остальные параметры в выборе программного обеспечения должны быть отключены.

Затем необходимо произвести выбор среди дополнительных функций устанавливаемой операционной системы установку службы ALD. Она необходима для управления базами данных.

Затем необходимо произвести выбор дополнительных настроек операционной системы. Должны быть установлены следующие параметры:

- включить режим замкнутой программной среды. Данный параметр необходим для включения механизма, обеспечивающего проверку неизменности и подлинности загружаемых исполняемых файлов формата ELF;
- включить очистку разделов страничного обмена. Данный параметр необходим для включения режима очистки памяти разделов подкачки swar;
- включить очистку освобождаемых областей для EXT-разделов. Данный параметр необходим для включения режима очистки блоков файловой системы непосредственно при их освобождении;
- включить блокировку консоли. Данный параметр необходим для

блокировки консоли учетных записей пользователей;

- включить межсетевой экран `ufw`. Данный параметр необходим для включения фильтрации сетевых пакетов;

- отключить возможность трассировки `ptrace`. Данный параметр необходим для отключения возможности трассировки и отладки выполнения программного кода;

- отключить автоматическую настройку сети. Данный параметр необходим для отключения автоматической настройки сетевых интерфейсов.

Раздел 2. Настройка парольной политики операционной системы специального назначения «Astra Linux Special Edition»

Для настройки парольной политики необходимо войти в учетную запись администратора и открыть приложение «Управление политикой безопасности». Оно расположено по пути: Пуск — Панель управления — Политика безопасности.

Затем необходимо выбрать пункт меню «Политики учетных записей», в котором перейти в подпункт «Политика паролей». После этого необходимо указать параметры во вкладках «Сложность» и «Срок действия».

Во вкладке «Сложность» необходимо установить параметры:

- проверка имени пользователя: отключено;
- проверка GECOS: отключено;
- применять для пользователя `root`: отключено;
- минимальная длина пароля: 8;
- минимальное количество строчных букв в новом пароле: 1;
- минимальное количество заглавных букв в новом пароле: 1;
- минимальное количество цифр в новом пароле: 1;
- минимальное количество других символов в новом пароле:

отключено.

Во вкладке «Срок действия» необходимо установить параметры:

- минимальное количество дней между сменами паролей: 0 дней;

- максимальное количество дней между сменами паролей: 30 дней;
- число дней выдачи предупреждения до смены пароля: 7 дней;
- число дней неактивности после устаревания пароля до блокировки учетной записи: 3 дней;
- срок действия учетной записи пользователя: отключено.

Затем необходимо выбрать пункт меню «Политики учетных записей», в котором перейти в подпункт «Блокировка». Затем необходимо выбрать необходимые настройки:

- индивидуальные настройки: отключено;
- не сбрасывать счетчик: отключено;
- не использовать счетчик для пользователя с uid=0: отключено;
- неуспешных попыток: 3;
- период блокировки: 600 секунд;
- период разблокировки: отключено.

Затем необходимо отредактировать файл `common-password`, расположенный по пути «`/etc/pam.d/common-password`».

Для установки минимального количества различных символов необходимо установить параметр «`difok=4`» после «`pam_cracklib.so`» в строке 25.

Для установки проверки повторяемости пароля необходимо отредактировать строку, содержащую параметр «`pam_unix.so`», добавив в нее параметр «`remember=5`» так, чтобы получилась строка «`password - [success=2 default=ignore] pam_unix.so obscure use_authtok tru_first_pass sha512 remember=5`».

Раздел 3. Настройка политики разграничения доступа к файлам и компонентам операционной системы специального назначения «Astra Linux Special Edition»

Для того чтобы разрешить использование `su` только пользователями,

находящимися в группе `sudo`, необходимо в `«/etc/pam.d/su»` добавить строку: `«authrequired pam_wheel.so use_uid»`. Затем создать группу `sudo`, если её не существует, и добавить в нее необходимых пользователей. Добавление группы и пользователей в группу осуществляется через оснастку «Группы» приложения «Управление политикой безопасности».

Загрузчик GRUB должен иметь включённую защиту паролем для предохранения настроек от изменений во время загрузки. Пароль загрузчика устанавливается в процессе установки системы. Для того, чтобы сменить его, необходимо выбрать пароль, а затем сгенерировать хэш от него, выполнив следующую команду: `«grub-crypt --sha-512»`. После этого необходимо заменить в файле `«/etc/grub.d/07_password»` строку хэша на сгенерированную. Строка хэша расположена перед концом файла, обозначаемым параметром «EOF».

Системные файлы `crontab` доступны только демону `cron`, доступному только с привилегиями суперпользователя, и команде `crontab`, которая запускается от имени пользователя `root`. Если непривилегированным пользователям дать права на чтение или модификацию системных `crontab` файлов, это может привести к повышению привилегий локального пользователя. Для того, чтобы ограничить права на `crontab` файл, необходимо выполнить команды: `«sudo chmod 400 /etc/crontab»`, `«sudo chmod -R 770 /var/spool/cron/»`, `«sudo chown -R 0 /var/spool/cron/»`.

Для того, чтобы ограничить вход суперпользователя через виртуальную консоль, необходимо удалить в файле `«/etc/securetty»` строки: `vc/1`, `vc/2`, `vc/3`, `vc/4`, если они существуют.

Для того, чтобы ограничить вход суперпользователя через последовательный порт, необходимо удалить в файле `«/etc/securetty»` строки: `ttyS0`, `ttyS1`, если они существуют.

Для того, чтобы ограничить доступ на запись к системным исполняемым файлам для всех учётных записей, необходимо выполнить команды:

- `sudo chmod 555 /bin;`
- `sudo chmod 555 /usr/bin;`
- `sudo chmod 555 /usr/local/bin;`
- `sudo chmod 555 /sbin;`
- `sudo chmod 555 /usr/sbin;`
- `sudo chmod 555 /usr/local/sbin.`

Для того, чтобы ограничить доступ на запись к системным разделяемым библиотекам для всех учётных записей, необходимо выполнить команды:

- `sudo chmod 555 /lib;`
- `sudo chmod 555 /lib64;`
- `sudo chmod 555 /usr/lib;`
- `sudo chmod 555 /usr/lib64;`
- `sudo chmod 555 /lib/modules.`

Раздел 4. Настройка параметров ядра операционной системы специального назначения «Astra Linux Special Edition»

Для того, чтобы настроить загрузчик на загрузку ядра GENERIC, и исключить из меню все другие варианты загрузки, включая режимы восстановления, необходимо перейти в меню загрузчика GRUB2, расположенному по пути: «Панель управления — Система — Загрузчик GRUB2». Затем необходимо выбрать следующие параметры:

- запись по умолчанию: «AstraLinuxSE GNU/Linux, with Linux 4.15.3-1-generic»;
- автоматически загружать запись по умолчанию после показа меню: Немедленно.

Для того, чтобы отключить параметры ядра для перенаправлений ICMP по умолчанию, необходимо выполнить следующие команды:

```
— sudo sysctl -w
net.ipv4.conf.default.send_redirects=0;
```

```
— sudo sysctl -w
net.ipv4.conf.all.accept_redirects=0.
```

Для того, чтобы отключить параметры ядра для IP Forwarding, необходимо выполнить команду: «sudo sysctl -w net.ipv4.ip_forward=0».

Для того, чтобы отключить параметры ядра для принятия Source-Routed пакетов по умолчанию, необходимо выполнить команду: «sudo sysctl -w net.ipv4.conf.default.accept_source_route=0».

Для того, чтобы включить параметры ядра для игнорирования ICMP Broadcast Echo запросов, необходимо выполнить команду: «sudo sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1».

Для того, чтобы включить параметры ядра для использования фильтрации обратного пути у всех интерфейсов, необходимо выполнить команду: «sudo sysctl -w net.ipv4.conf.all.rp_filter=1».

Для того, чтобы отключить механизм SysRq, необходимо отредактировать файл «/etc/sysctl.conf». Необходимо добавить в него строку «kernel.sysrq = 0».

Для того, чтобы включить параметры ядра для использования TCP syncookies, необходимо выполнить команду: «sudo sysctl -w net.ipv4.tcp_syncookies=0».

Для того, чтобы заблокировать исполнение модулей python с расширенным функционалом, необходимо выполнить команду: «sudo find /usr/lib/python* -type f -name "_ctypes*" -exec sudo dpkg-statoverride --update --add root root 640 '{}' \».

Для того, чтобы заблокировать макросы в VLC, необходимо выполнить

команду: `«sudo find /usr/lib/ -type f -name "liblua_plugin*" -exec sudo dpkg-statoverride --update --add root root 640 '{}' \»`.

Для того, чтобы настроить необходимые параметры ядра, необходимо отредактировать файл `«/etc/security/limits.conf»`, установив следующие параметры:

- `hard fsize 500000000;`
- `hard nproc 1000;`
- `hard core 0.`

Раздел 5. Настройка параметров операционной системы специального назначения «Astra Linux Special Edition»

Для того, чтобы отключить все неиспользуемые сервисы, необходимо вывести их список командой `«apt list --installed»`, после чего просмотреть полученный перечень. Затем необходимо отключить все неиспользуемые сервисы командой `«systemctl disable <наименование сервиса>»`.

Для того, чтобы установить запрет установки исполняемого бита, необходимо перейти в раздел «Настройки безопасности» оснастки «Управление политикой безопасности». В данном разделе необходимо выбрать подраздел «Системные параметры» и включить параметр «Запрет установки бита исполнения».

Для того, чтобы включить контроль целостности файлов и каталогов, необходимо произвести настройки замкнутой программной среды в оснастке «Управление политикой безопасности». Для этого необходимо перейти в раздел «Замкнутая программная среда» и выбрать подраздел «Ключи». Затем необходимо сгенерировать ключ подписи путем выбора каталога «`xattr_keys`» и нажатием на клавишу «Создать новый ключ». Затем необходимо ввести запрашиваемые системой данные. После ввода кода защиты ключа ключ будет

создан и подписан. Затем необходимо перейти в подраздел «Подпись» и выбрать параметр «Подпись в бинарные файлы». Затем необходимо выделить следующие каталоги для подписи: «/etc», «/lib», «/lib64», «/bin», «/sbin», «/boot», «/root», «/opt», «/srv», «/usr». Следом необходимо нажать на кнопку «Подписать», выбрать созданный на предыдущем этапе ключ, ввести код защиты ключа и дождаться завершения подписывания каталогов.

Для настройки режима «КИОСК» необходимо перейти в оснастку «Системный киоск», расположенную во вкладке «Безопасность» панели управления. Затем необходимо создать во вкладке «Профили пользователей» профили для всех необходимых пользователей, настроив для каждого пользователя доступ ко всем директориям в соответствии с потребностями. Для этого нужно нажать на клавишу «Добавить», ввести имя пользователя, нажать на клавишу «Вставить файл». Затем необходимо выбрать все необходимые файлы настройки и включить режим «КИОСК», нажав на кнопку «Включить режим киоска» в контекстном меню «Правка».

Для настройки подключаемых носителей необходимо перейти во вкладку «Оборудование» панели управления и открыть оснастку «Обработка подключения устройств». Затем необходимо отключить все действия, кроме действия «Открыть в менеджере файлов». Затем необходимо перейти в раздел «Настройки безопасности» оснастки «Управление политикой безопасности». В данном разделе необходимо выбрать подраздел «Устройства и правила» и выбрать вкладку «Устройства». Затем необходимо нажать кнопку «Добавить» и подключить устройство к системе. После этого необходимо выбрать устройство и нажать кнопку «Да». Затем необходимо ввести наименование правила, выбрать необходимого пользователя и/или группу пользователя, назначить права доступа для них и остальных пользователей. Затем необходимо выбрать в разделе «Свойства» ключ типа «ID_SERIAL».

6 Разработка программного обеспечения автоматической настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.

На данном этапе была произведена разработка программного обеспечения автоматической настройки операционной системы специального назначения «Astra Linux Special Edition», встроенной в рассматриваемую аппаратуру, для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну, в соответствии с составленной ранее методикой настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.

Разработанные скрипты производят автоматическую настройку операционной системы специального назначения «Astra Linux Special Edition» в соответствии с пунктами методики, кроме:

- контроля целостности;
- настройки режима «КИОСК»;
- настройки блокировки пользователей.

Данные параметры необходимо настраивать в ручную.

Скрипты были разделены на файлы «main.sh», «auth.sed», «grub.sed». Файлы с расширением «.sed» необходимы для упрощения настройки параметров. Для запуска скриптов необходимо перейти в папку расположения скриптов и выполнить команду «sudo ./main.sh».

Содержимое файла main.sh:

```
#!/bin/bash
```

```
echo "Этап №1"
```

```
echo "Создание пользователя"
```

```
adduser --disabled-password -gecos GECOS astrauser
echo "Настройка параметров аутентификации"
sed -i -f ./auth.sed /etc/pam.d/common-password
rm ./auth.sed

echo "Этап №2"

echo "Смена пароля grub"
param1=`echo -e 'Qkimfmif\nQkimfmif' | grub-mkpasswd-
pbkdf2 | grep grub | awk '{ print $5 }'`
param2="sed -i s/grub.pbkdf2.sha512\(.*\)/$param1/
/etc/grub.d/07_password"
$param2 #> /etc/grub.d/07_password
echo "Ограничить права на crontab"
chmod 400 /etc/crontab
chmod -R 770 /var/spool/cron/
chown -R 0 /var/spool/cron/
echo "Ограничить доступ к root"
echo "auth required pam_wheel.so use_uid" >>
/etc/pam.d/su
echo "Ограничить доступ на запись к системным исполняемым
файлам и библиотекам"
chmod 555 /bin;
chmod 555 /usr/bin;
chmod 555 /usr/local/bin;
chmod 555 /sbin;
chmod 555 /usr/sbin;
chmod 555 /usr/local/sbin
chmod 555 /lib;
```

```
chmod 555 /lib64;  
chmod 555 /usr/lib;  
chmod 555 /usr/lib64;  
chmod 555 /lib/modules.
```

```
echo "Этап №3"  
echo "Настройка grub"  
sed -i -f ./grub.sed /etc/default/grub  
update-grub  
rm ./grub.sed
```

```
echo "Настройка параметров ядра"  
echo "net.ipv4.conf.default.send_redirects=0" >>  
/etc/sysctl.conf  
echo "net.ipv4.conf.all.accept_redirects=0" >>  
/etc/sysctl.conf  
echo "net.ipv4.conf.all.send_redirects=0" >>  
/etc/sysctl.conf  
echo "net.ipv4.ip_forward=0" >> /etc/sysctl.conf  
echo "net.ipv4.conf.default.accept_source_route=0" >>  
/etc/sysctl.conf  
echo "net.ipv4.conf.default.secure_redirects=0" >>  
/etc/sysctl.conf  
echo "net.ipv4.icmp_echo_ignore_broadcasts=1" >>  
/etc/sysctl.conf  
echo "net.ipv4.conf.all.rp_filter=1" >> /etc/sysctl.conf  
echo "kernel.sysrq=0" >> /etc/sysctl.conf  
echo "net.ipv4.tcp_syncookies=256" >> /etc/sysctl.conf  
sysctl -w net.ipv4.conf.default.send_redirects=0
```

```

sysctl -w net.ipv4.conf.all.accept_redirects=0
sysctl -w net.ipv4.conf.all.send_redirects=0
sysctl -w net.ipv4.ip_forward=0
sysctl -w net.ipv4.conf.default.accept_source_route=0
sysctl -w net.ipv4.conf.default.secure_redirects=0
sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
sysctl -w net.ipv4.conf.all.rp_filter=1
sysctl -w kernel.sysrq=0
sysctl -w net.ipv4.tcp_syncookies=256
find /usr/lib/ -type f -name "liblua_plugin*" -exec sudo
dpkg-statoverride --update --add root root 640 '{}' \
find /usr/lib/python* -type f -name "_ctype*" -exec sudo
dpkg-statoverride --update --add root root 640 '{}' \
echo "* hard fsize 50000000" >> /etc/security/limits.conf
echo "* hard nproc 1000" >> /etc/security/limits.conf
echo "* hard core 0" >> /etc/security/limits.conf

echo "Этап №4"

echo "Отключить сервисы"
echo "Отключить службу acpi-support"
systemctl disable acpi-support
echo "Отключить службу acpid"
systemctl disable acpid
echo "Отключить службу alsa-utils"
systemctl disable alsa-utils
echo "Отключить службу anacron"
systemctl disable anacron
echo "Отключить службу avahi-daemon"

```

```
systemctl disable avahi-daemon
echo "Отключить службу bootlogs"
systemctl disable bootlogs
echo "Отключить службу cron"
systemctl disable cron
echo "Отключить службу cups"
systemctl disable cups
echo "Отключить службу exim4"
systemctl disable exim4
echo "Отключить службу hwclock.sh"
systemctl disable hwclock.sh
echo "Отключить службу keyboard-setup"
systemctl disable keyboard-setup
echo "Отключить службу kmod"
systemctl disable kmod
echo "Отключить службу motd"
systemctl disable motd
echo "Отключить службу ntp"
systemctl disable ntp
echo "Отключить службу openvpn"
systemctl disable openvpn
echo "Отключить службу parlogd"
systemctl disable parlogd
echo "Отключить службу plymouth"
systemctl disable plymouth
echo "Отключить службу plymouth-log"
systemctl disable plymouth-log
echo "Отключить службу procsps"
systemctl disable procsps
```

```

echo "Отключить службу rmnologin"
systemctl disable rmnologin
echo "Отключить службу sendsigs"
systemctl disable sendsigs
echo "Настройка монтирования носителей"
systemctl enable media-cdrom0.mount
systemctl enable media-cdrom0.automount
echo "Установить запрет установки исполняемого бита"
astra-nochmodx-lock enable
echo 1 > /parsecfs/nochmodx
echo 1 > /etc/parsec/nochmodx
astra-interpreters-lock enable
astra-ptrace-lock enable

```

Содержимое файла auth.sed:

```

#!/bin/sed -rf
s/\(remember\)=[0-9]\{1,2\}//
s/\(success\)=[0-9]\{1,2\}\(.*\) \(pam_unix.so\) \
(.*\) /\1=2\2\3\4                                remember=5/
s/\(difok\)=[0-9]\{1,2\} /\1=4/ 1 i \

```

Содержимое файла grub.sed:

```

#!/bin/sed -rf
s/\(GRUB_HIDDEN_TIMEOUT\)=[0-9]\{1,2\}//
s/\#GRUB_DISABLE_RECOVERY="true"/GRUB_DISABLE_RECOVERY="t
rue"/1 i\
s/\(GRUB_TIMEOUT\)=[0-9]\{1,2\} /\1=0
\GRUB_HIDDEN_TIMEOUT=0/g

```

7 Проверка методики настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.

На данном этапе была произведена проверка методики настройки операционной системы специального назначения «Astra Linux Special Edition», встроенной в рассматриваемую аппаратуру, для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.

Было произведено выполнение всех указанных в методике пунктов.

Результат проверки установки операционной системы специального назначения «Astra Linux Special Edition» представлен на рисунках 1-7.

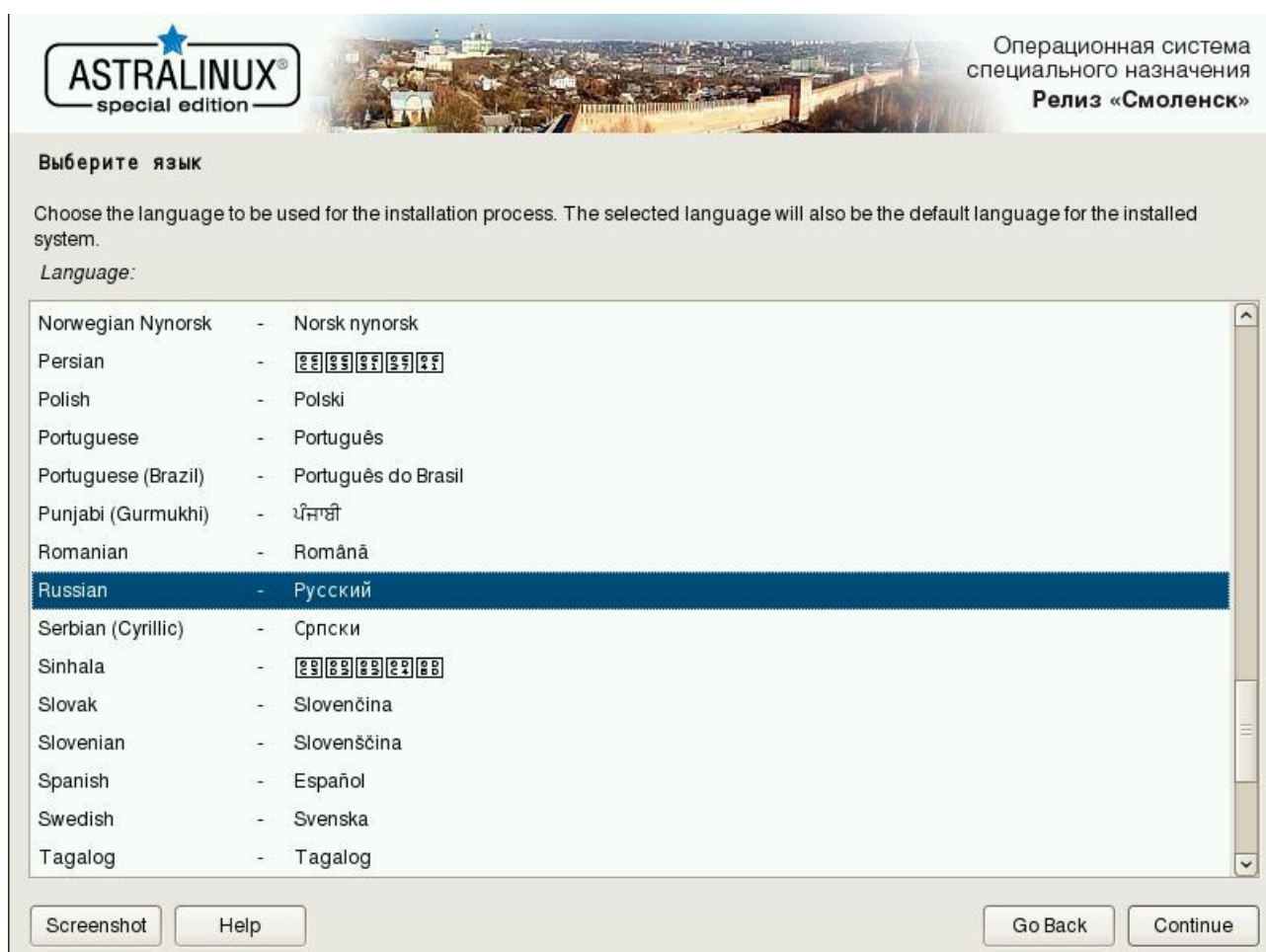


Рисунок 1 — Выбор языка системы

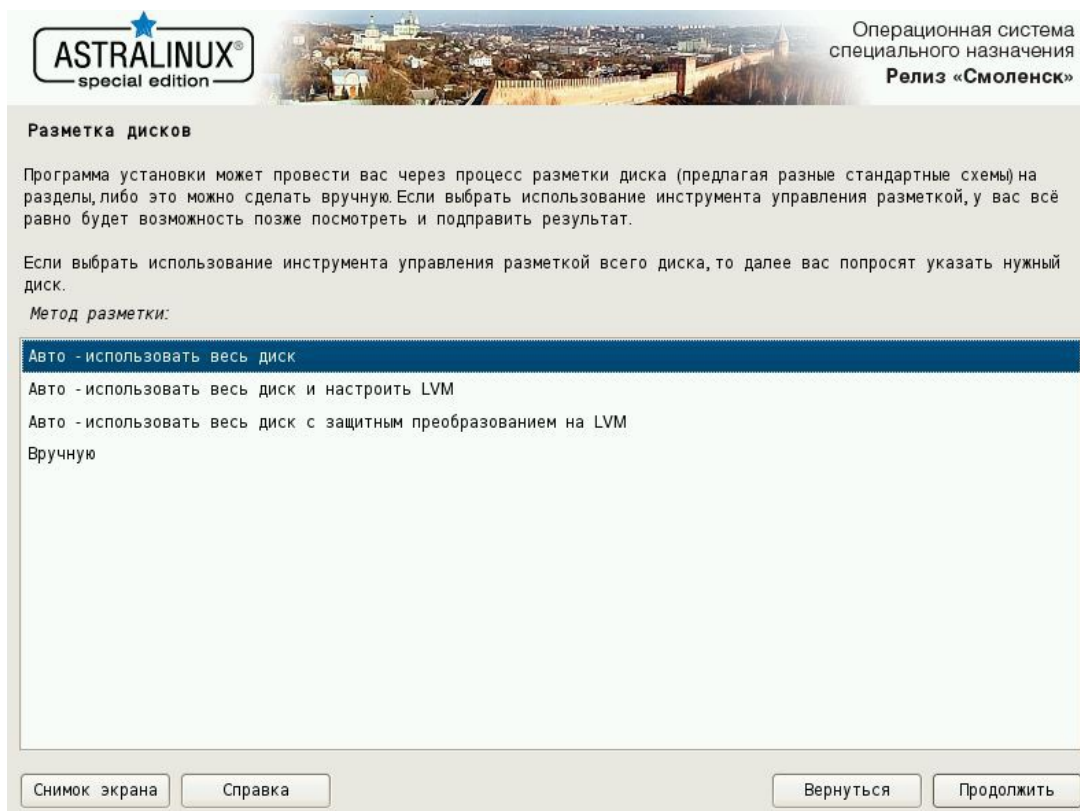


Рисунок 2 — Выбор метода разметки диска

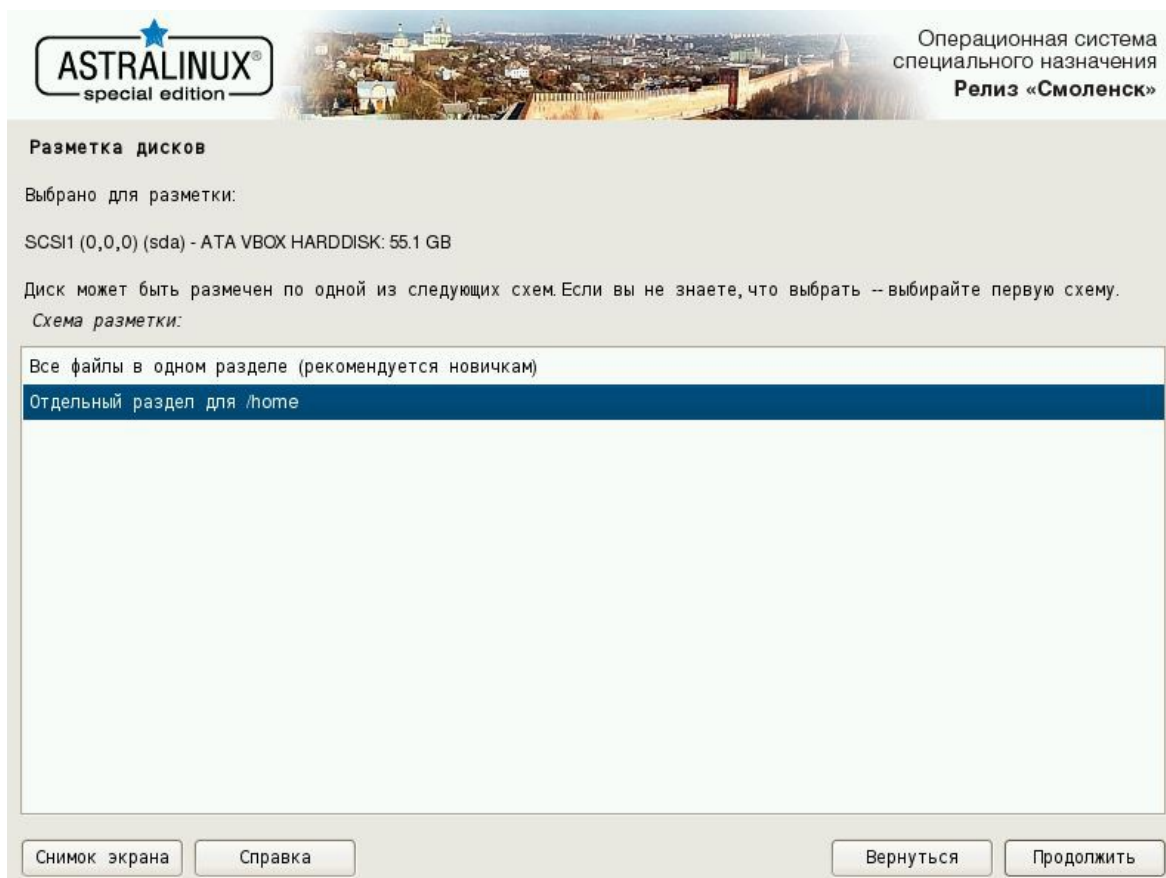


Рисунок 3 — Выбор схемы разметки

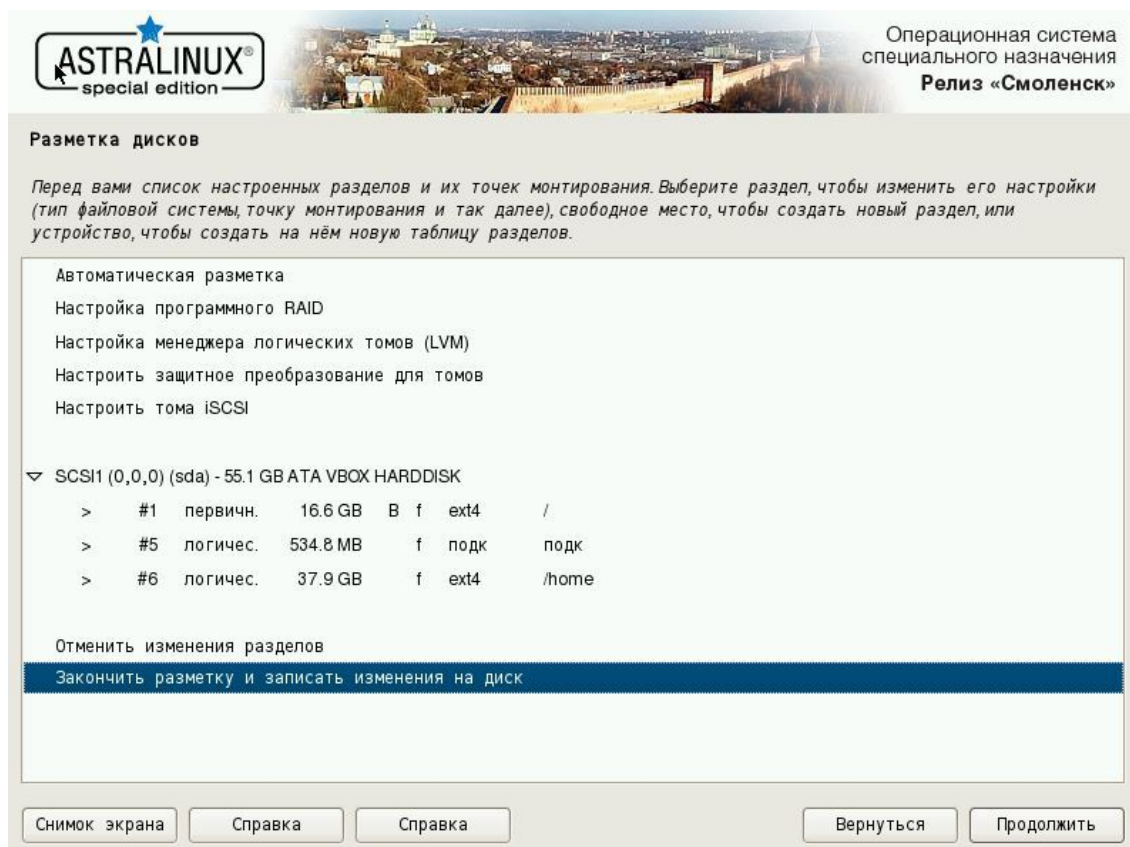


Рисунок 4 — Завершение разметки

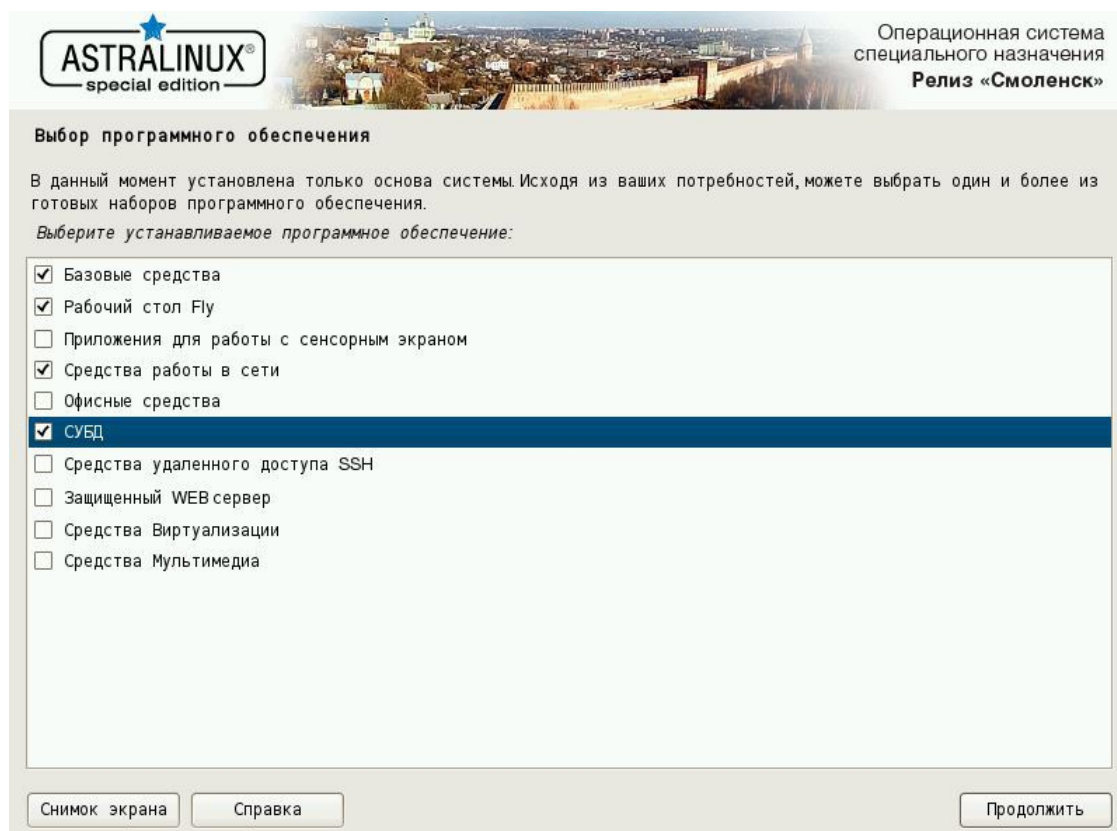


Рисунок 5 — Выбор программного обеспечения

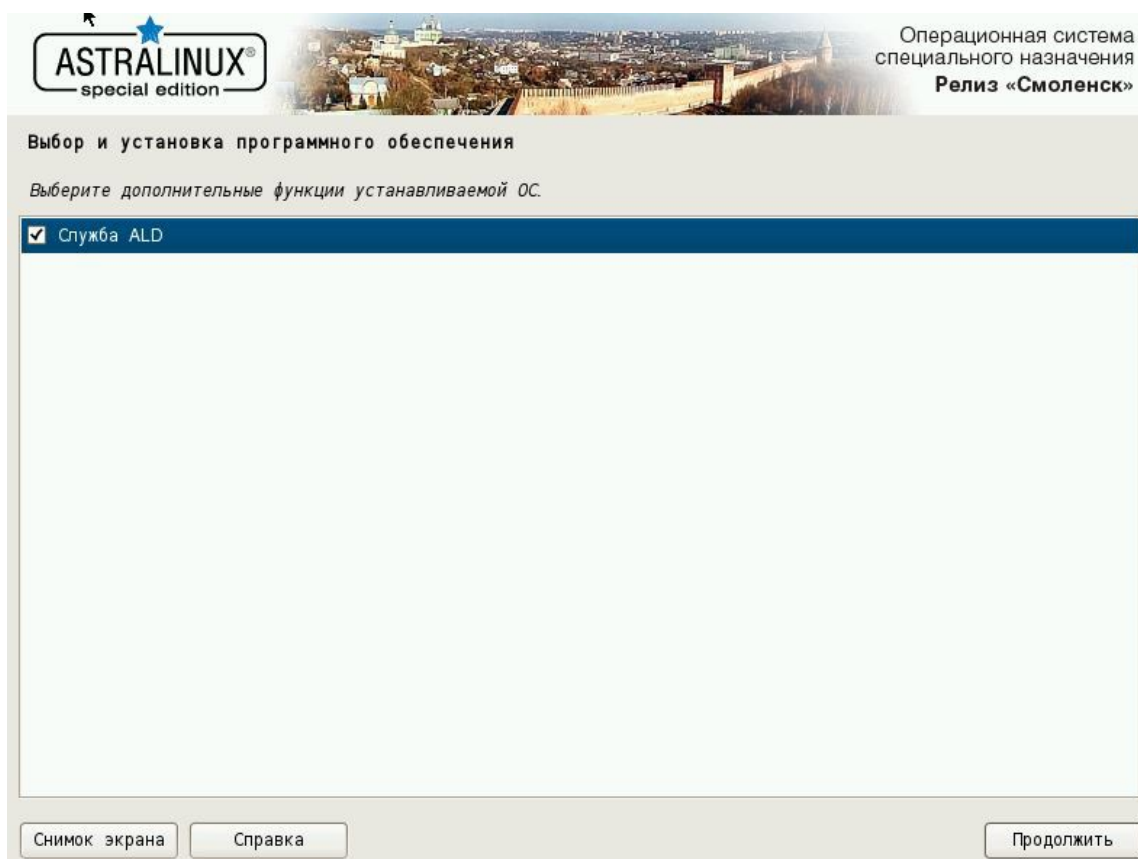


Рисунок 6 — Выбор дополнительных функций программного обеспечения

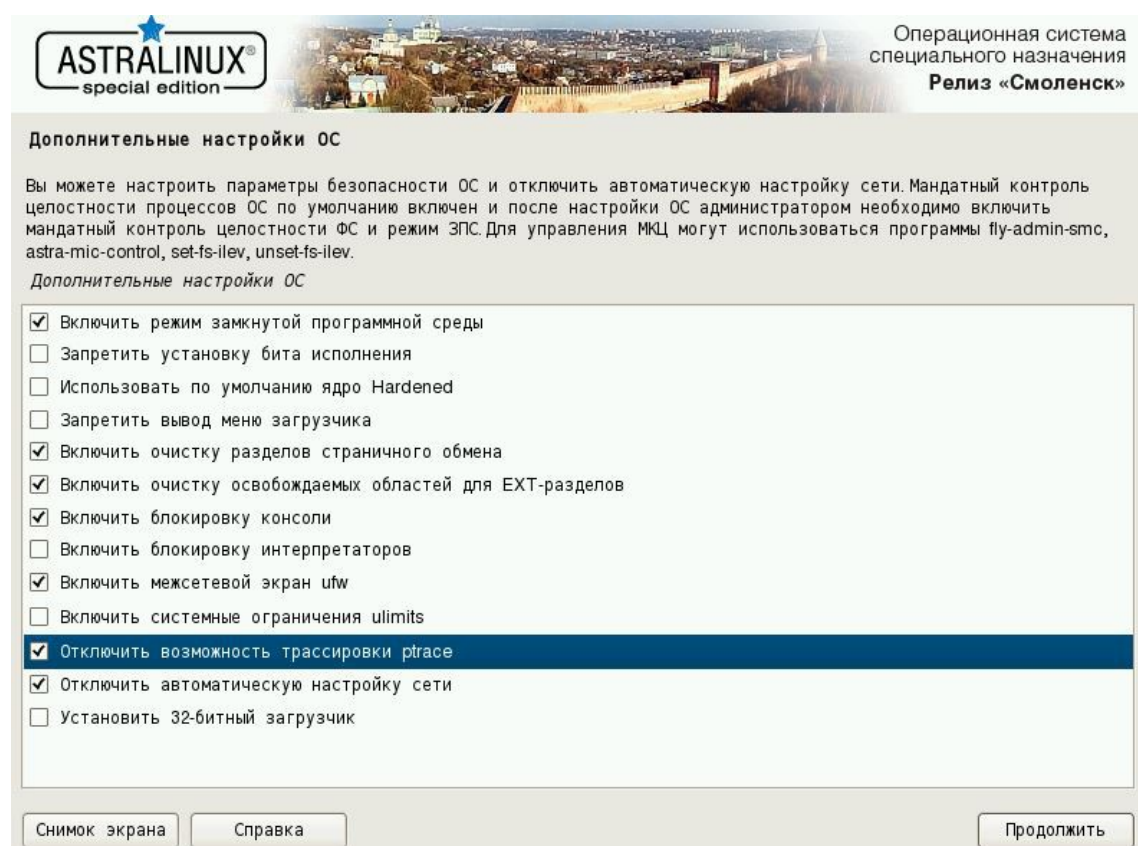


Рисунок 7 — Выбор настроек системы

Затем была произведена настройка парольной политики операционной системы специального назначения «Astra Linux Special Edition». Результат настройки представлен на рисунках 8-11.

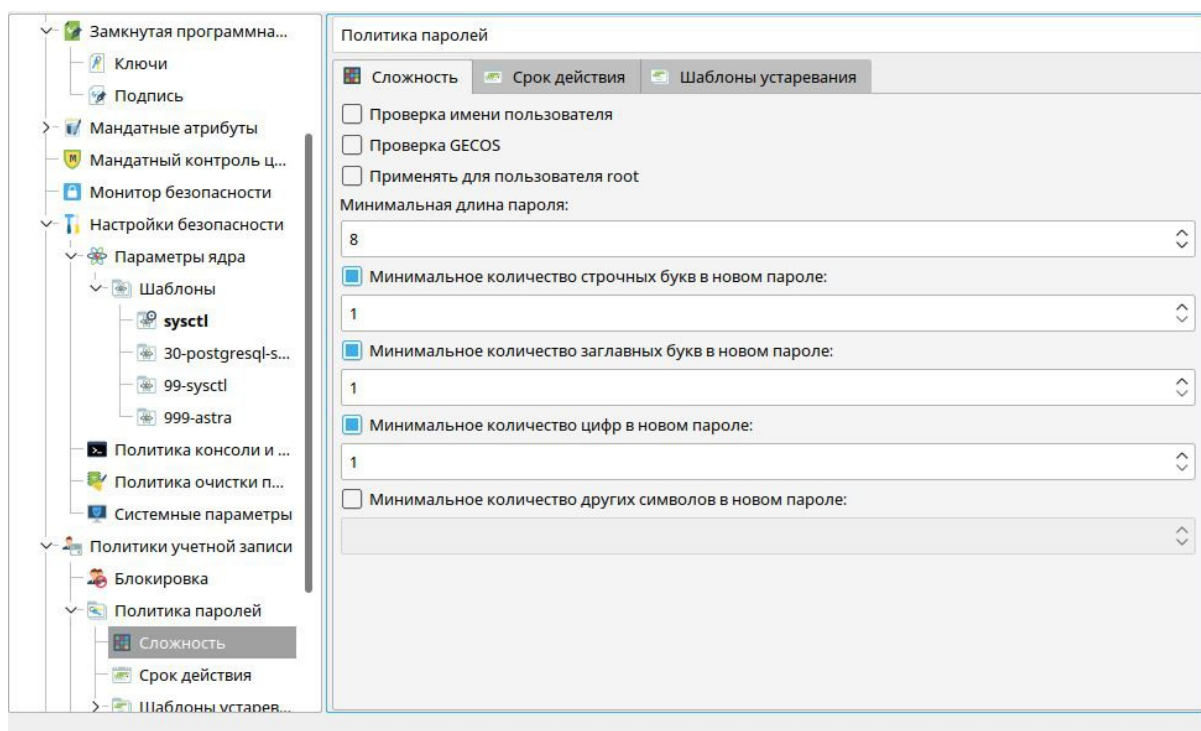


Рисунок 8 — Настройка сложности паролей

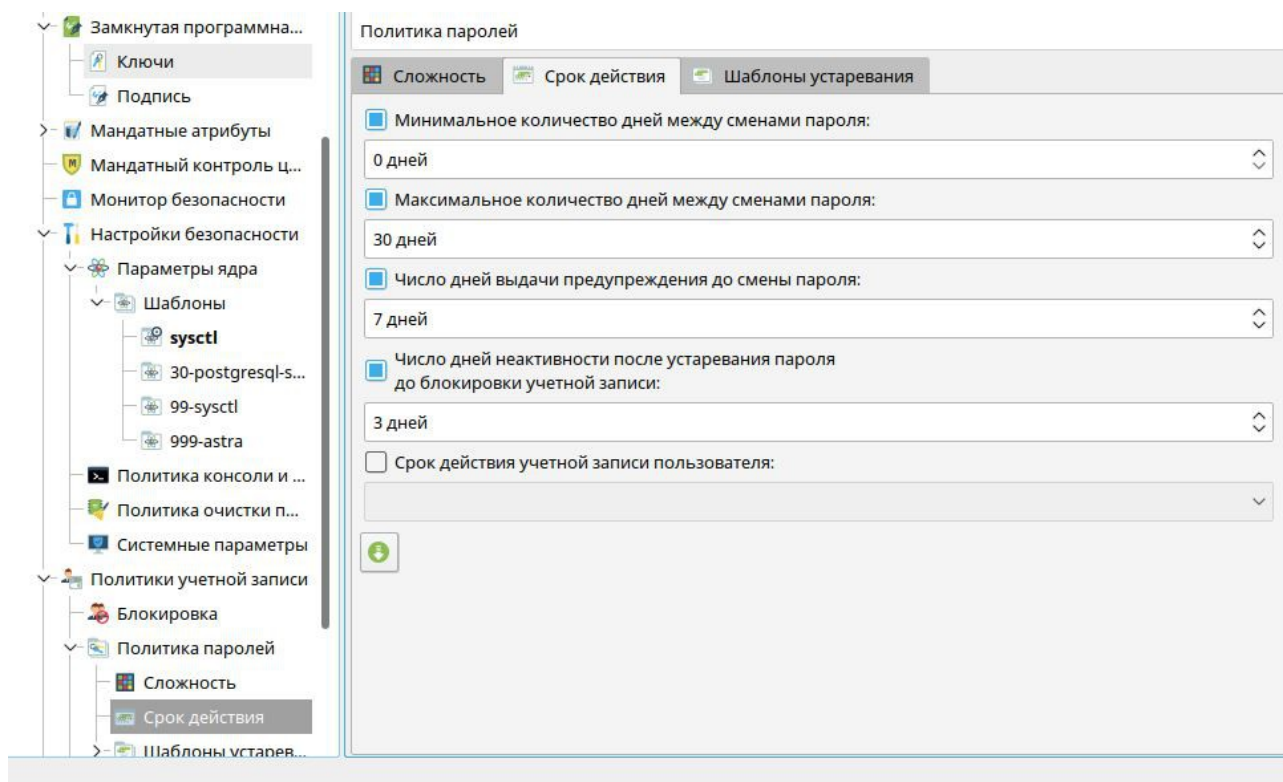


Рисунок 9 — Настройка срока действия паролей

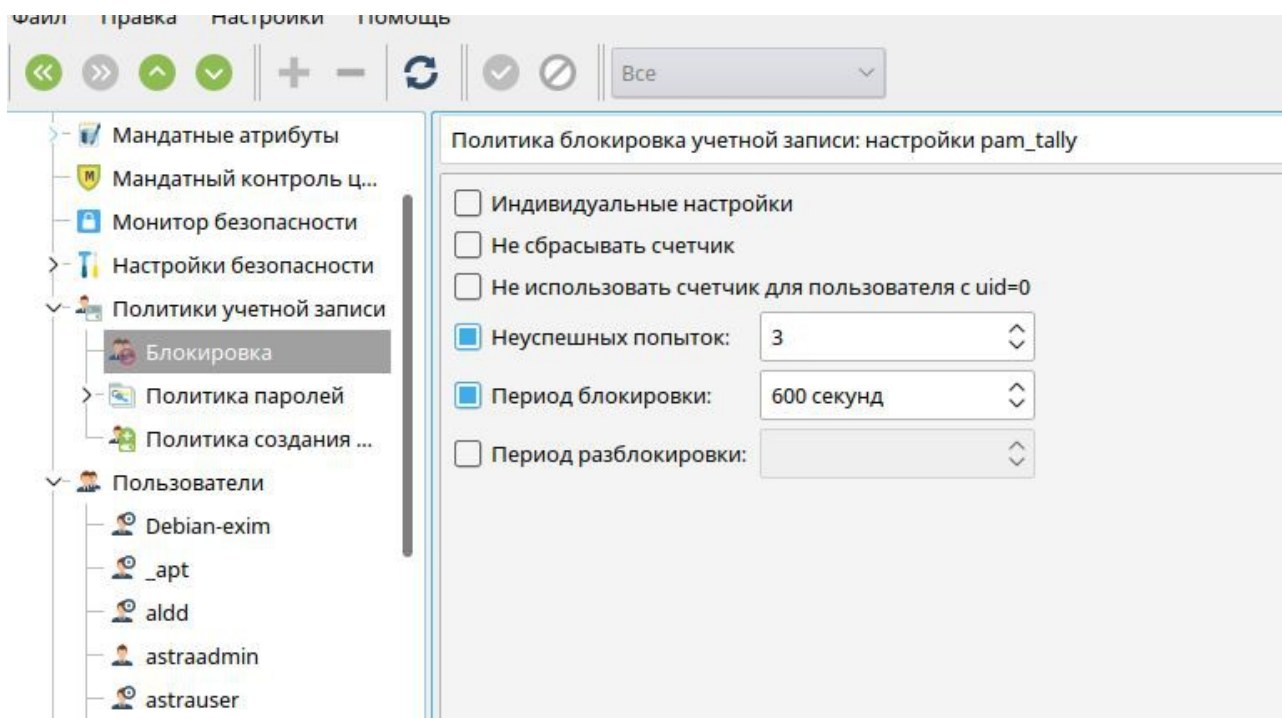


Рисунок 10 — Настройка блокировок учетных записей

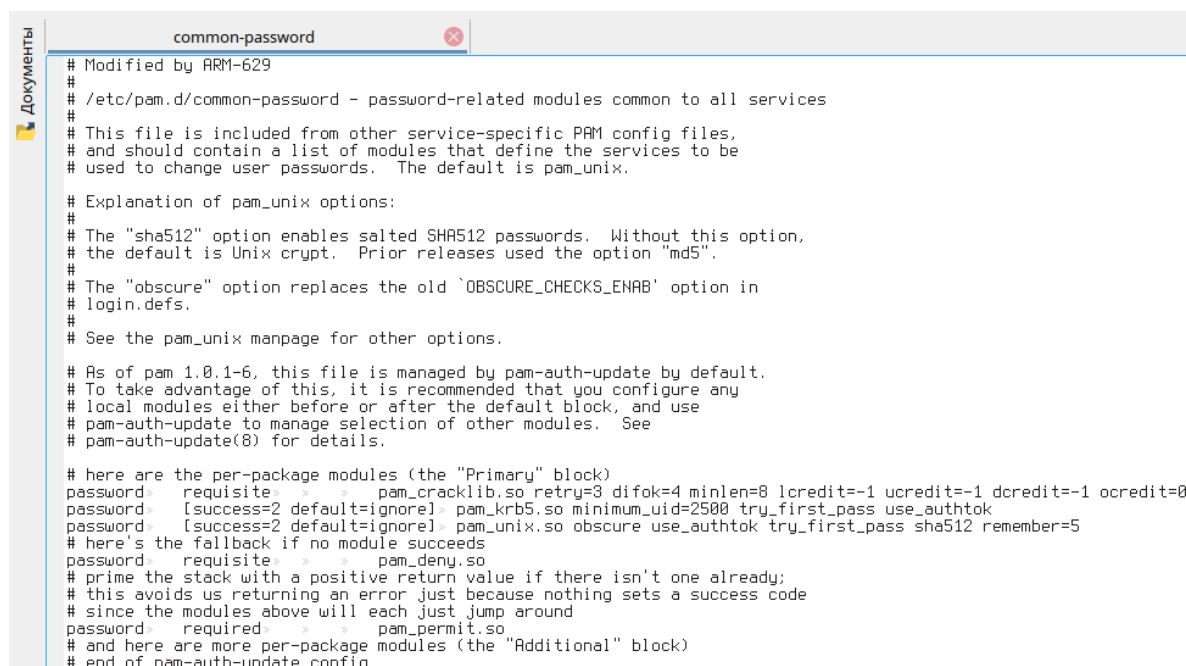


Рисунок 11 — Содержимое файла «common-password»

Пример ошибок смены пароля представлен на рисунках 12-15.

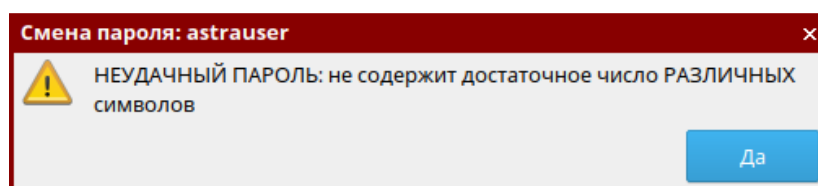


Рисунок 12 — Ошибка минимального количества отличных символов

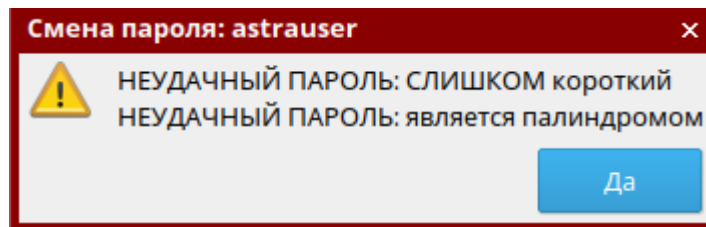


Рисунок 13 — Ошибка длины пароля

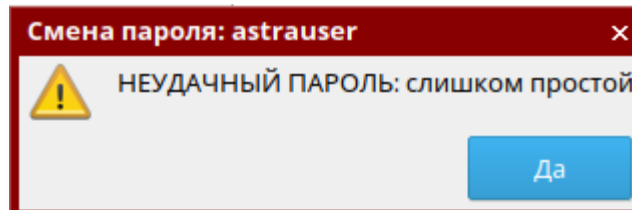


Рисунок 14 — Ошибка сложности пароля

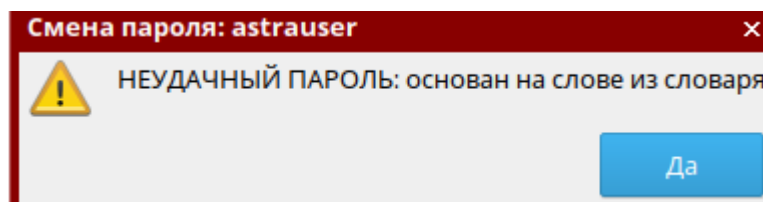


Рисунок 15 — Ошибка повторяемости пароля

В результате настройки политики разграничения доступа к файлам и компонентам операционной системы специального назначения «Astra Linux Special Edition» было выявлено, что пользователь без прав суперпользователя не имеет доступа к ограниченным файлам. Пример ошибки доступа представлен на рисунке 16.

```
astraadmin@astra:~/Desktop/Scripts$ /etc/crontab  
bash: /etc/crontab: Отказано в доступе
```

Рисунок 16 — Ошибка доступа к crontab

Результат настройки параметров ядра операционной системы специального назначения «Astra Linux Special Edition» представлен на рисунке 17.

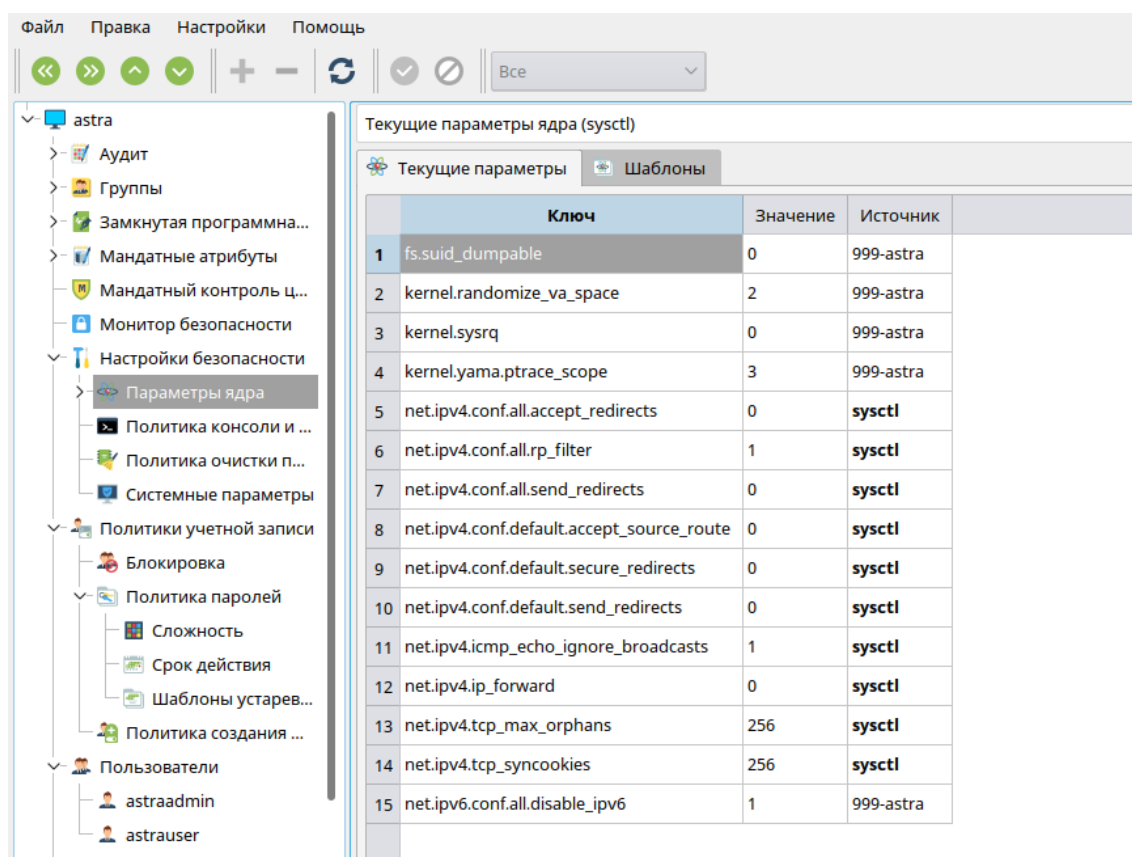


Рисунок 17 — Результат настройки параметров ядра

Результат настройки параметров операционной системы специального назначения «Astra Linux Special Edition» представлен на рисунках 18-28.

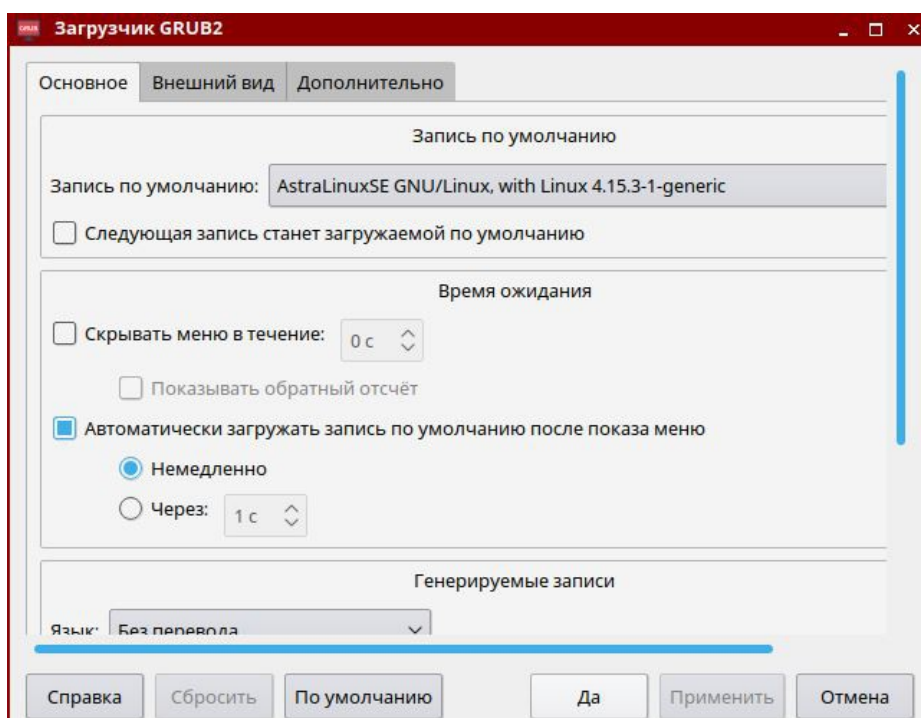


Рисунок 18 — Результат настройки загрузчика GRUB

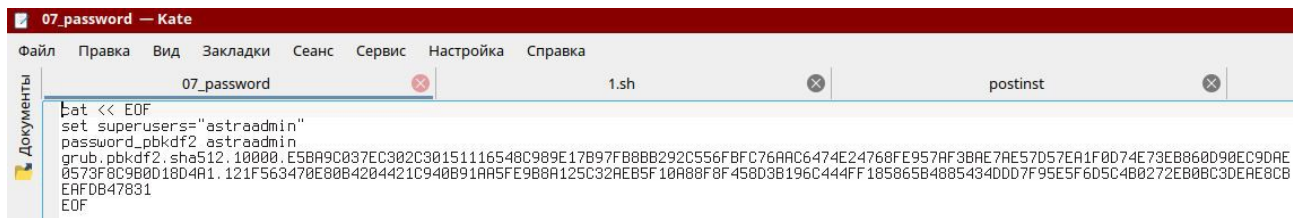


Рисунок 19 — Результат настройки пароля загрузчика GRUB

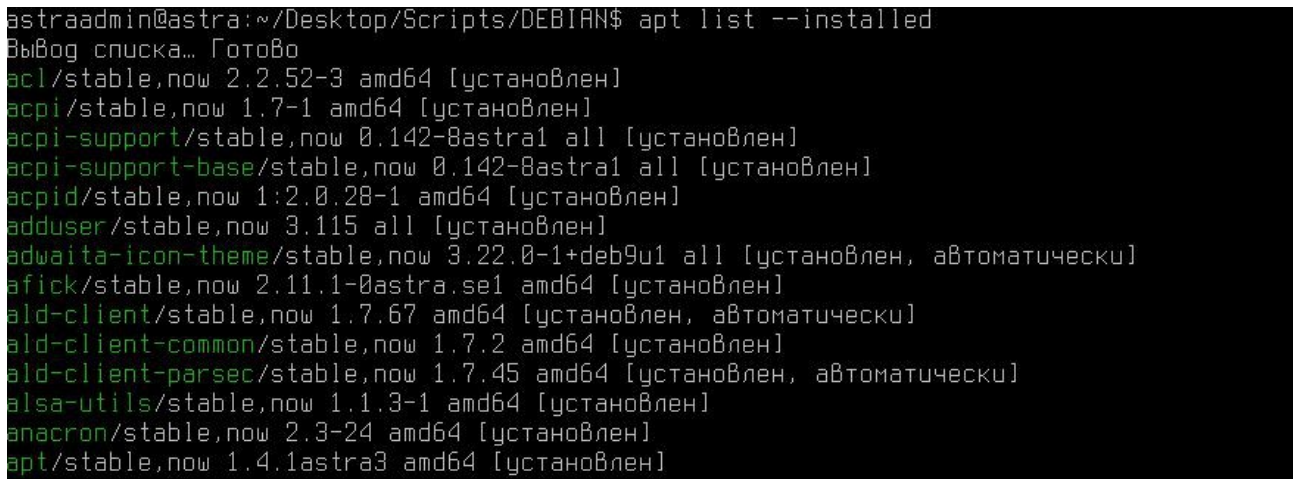


Рисунок 20 — Результат отключения сервисов

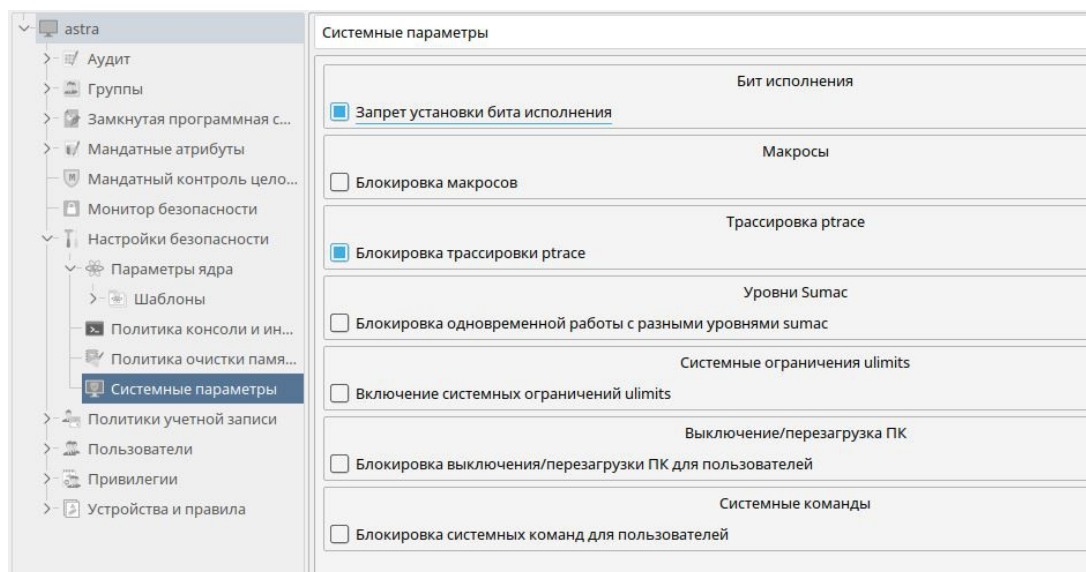


Рисунок 21 — Результат настройки запрета бита исполнения

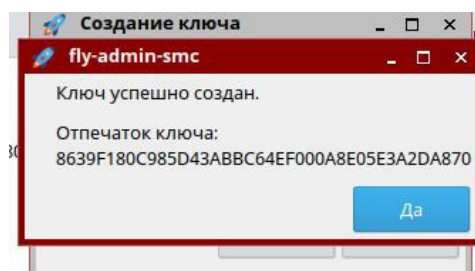


Рисунок 22 — Создание ключа подписи

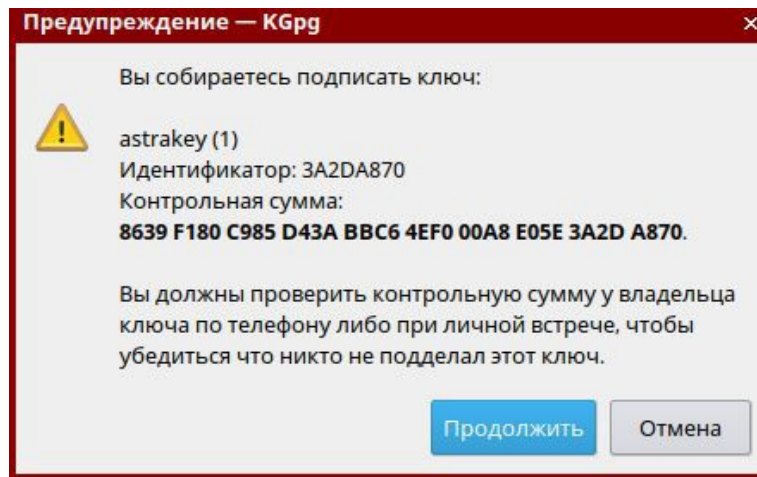


Рисунок 23 — Подписывание ключа

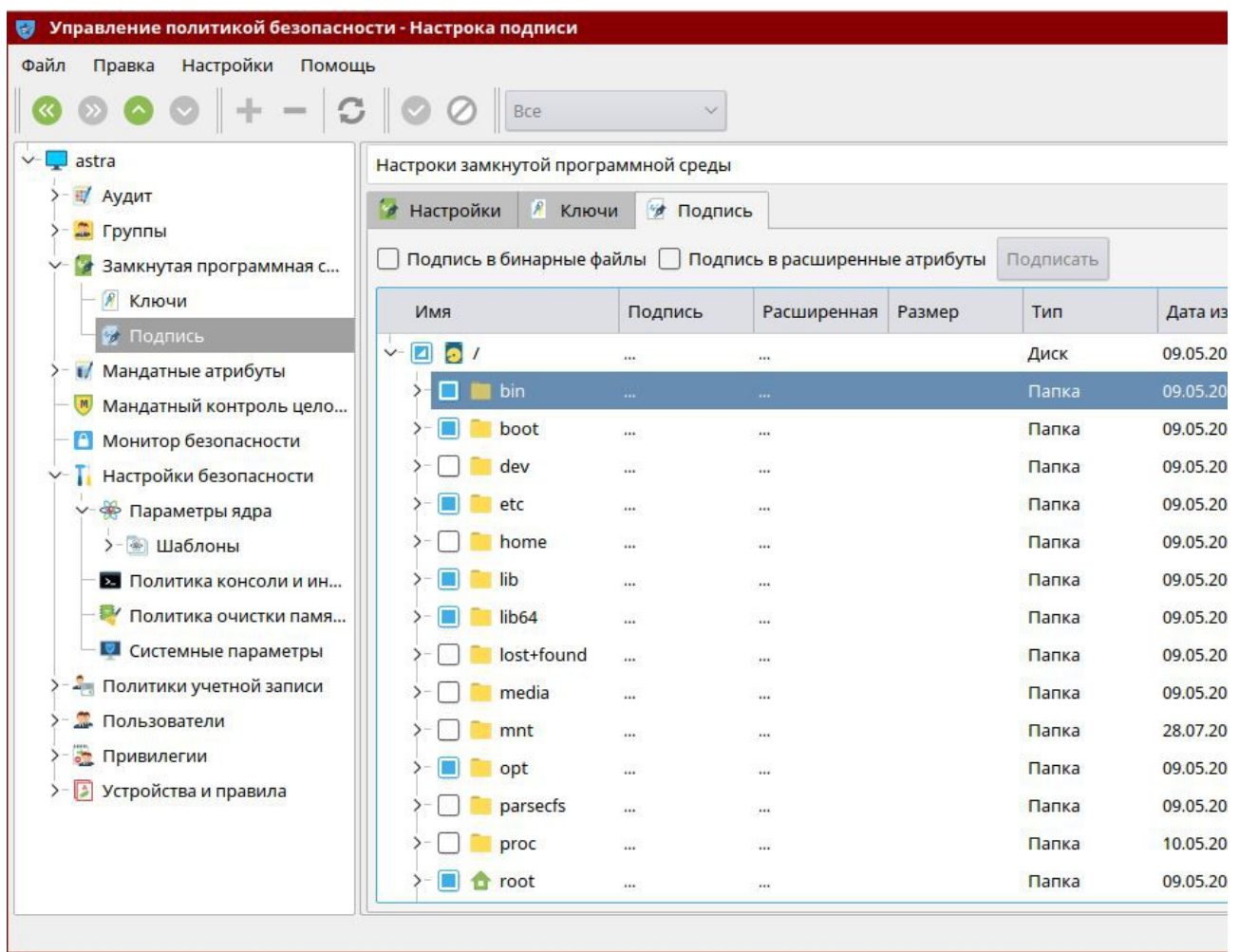


Рисунок 24 — Выбор подписываемых каталогов

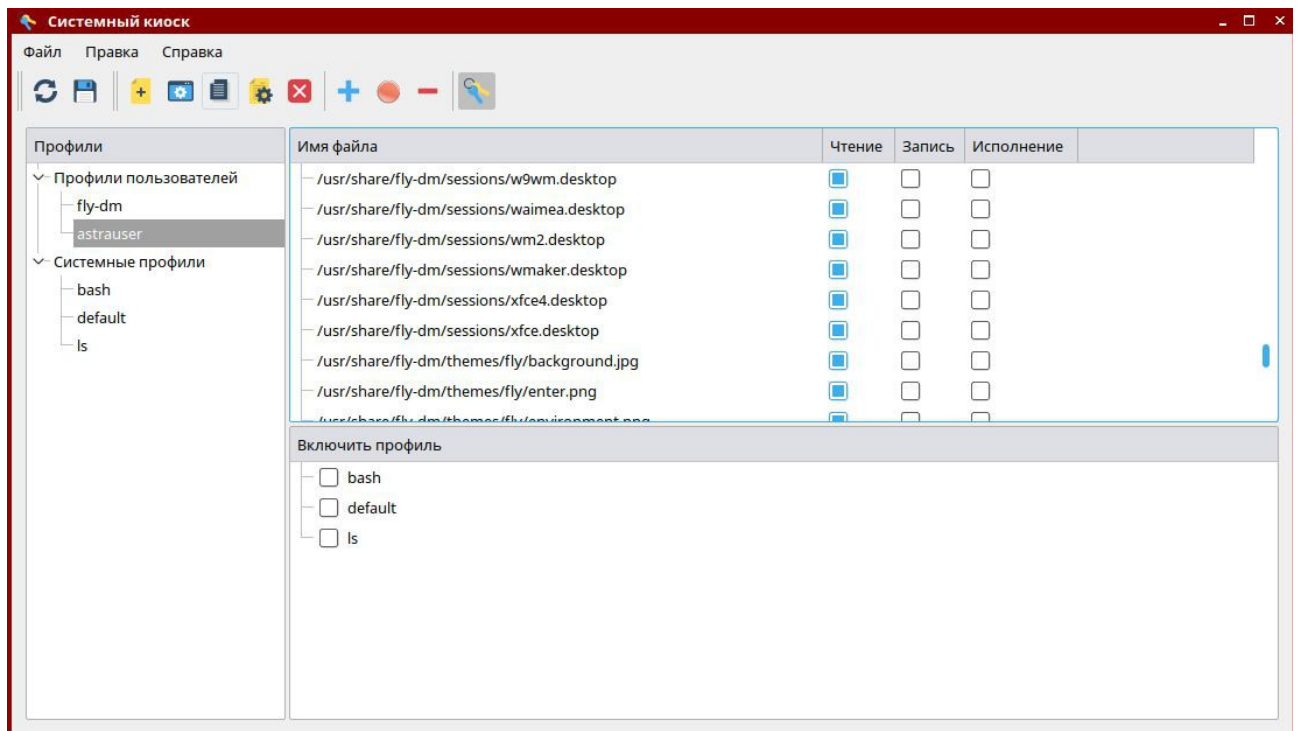


Рисунок 25 — Настройка режима «КИОСК»

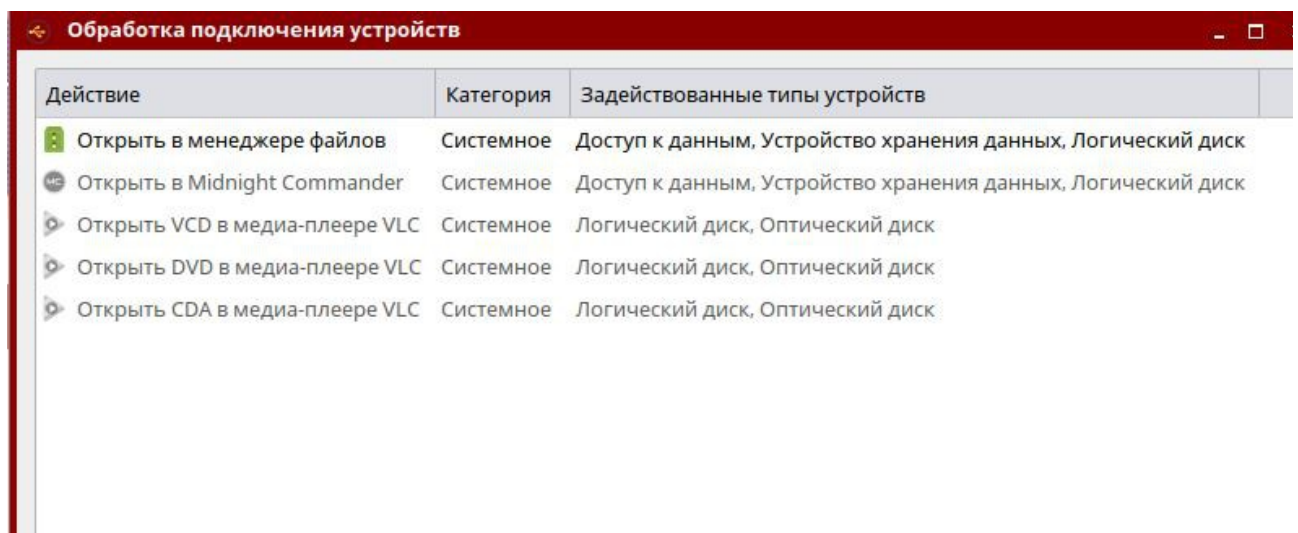


Рисунок 26 — Настройка обработки подключения устройств

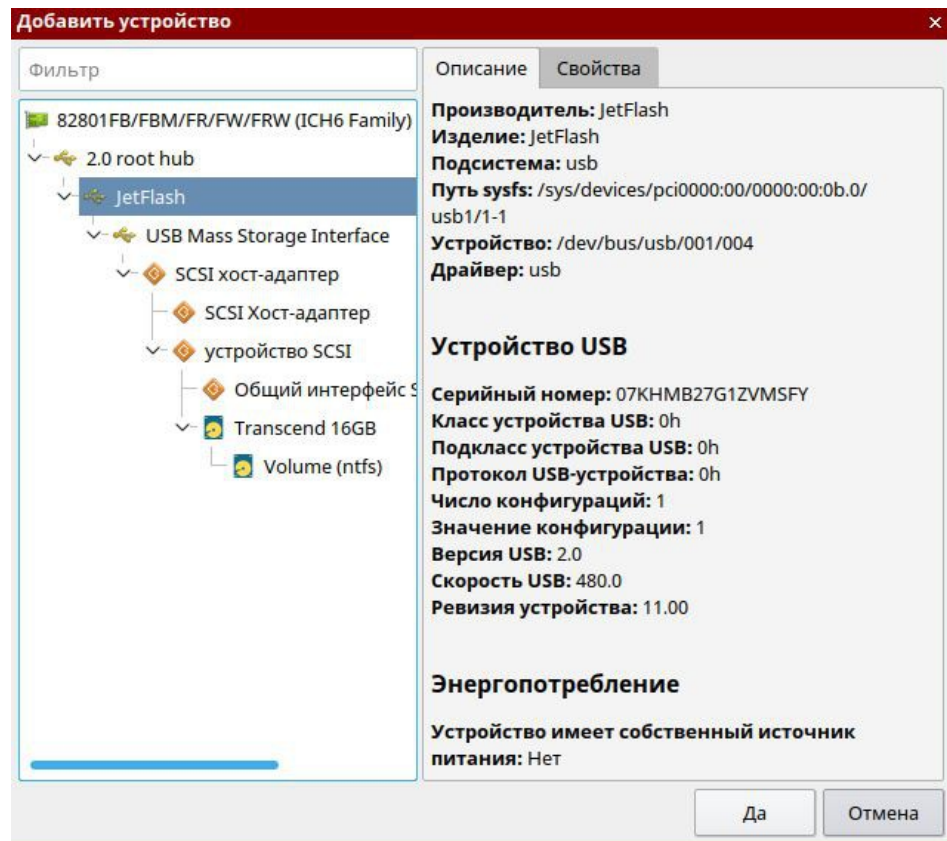


Рисунок 27 — Подключение USB

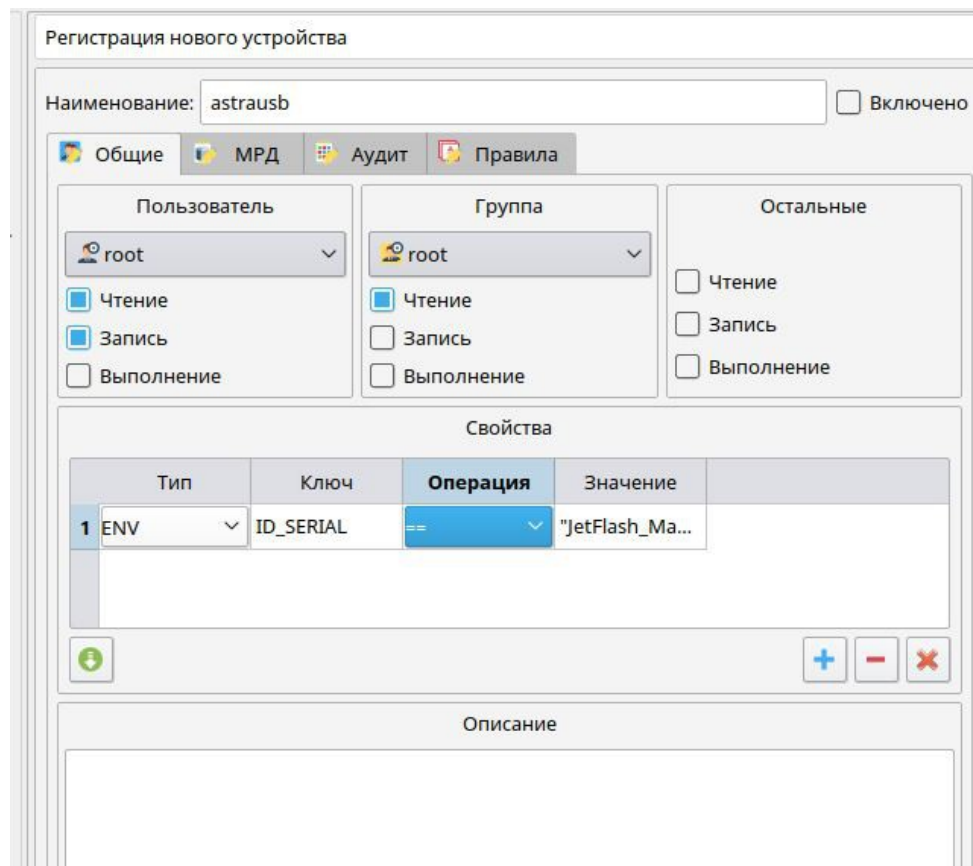


Рисунок 28 — Настройка USB

8 Вредные психофизиологические факторы, влияющие на психоэмоциональное состояние специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.

В соответствии с ГОСТ 12.0.003-2015 опасные и вредные производственные факторы, обладающие свойствами психофизиологического воздействия на организм человека, подразделяют:

- на физические перегрузки, связанные с тяжестью трудового процесса;
- нервно-психические перегрузки, связанные с напряженностью трудового процесса.

Физические перегрузки подразделяют на:

- статические;
- динамические нагрузки..

Статические перегрузки связаны с рабочей позой. Динамические же нагрузки могут быть связаны с массой поднимаемого и перемещаемого вручную груза, а также повторением стереотипных рабочих движений.

Физические перегрузки организма, связанные с тяжестью трудового процесса, в целях оценки условий труда, разработки и принятия мероприятий по их улучшению характеризуются такими показателями, как:

- масса поднимаемого и перемещаемого груза вручную;
- физическая динамическая нагрузка;
- статическая нагрузка;
- стереотипные рабочие движения;
- рабочая поза;
- наклоны корпуса тела работника;
- перемещение в пространстве.

Нервно-психические перегрузки подразделяют на:

- перенапряжение анализаторов и умственное перенапряжение, в том числе вызванное информационной нагрузкой;
- монотонность труда, вызывающая монотонию;
- эмоциональные перегрузки.

Нервно-психические перегрузки организм, связанные с напряженностью трудового процесса, в целях оценки условий труда, разработки и принятия мероприятий по их улучшению характеризуются такими показателями, как:

- длительность сосредоточенного наблюдения;
- активное наблюдение за ходом производственного процесса;
- число производственных объектов одновременного наблюдения;
- плотность сигналов (световых, звуковых) и сообщений в единицу времени;
- нагрузка на слуховой анализатор;
- нагрузка на голосовой аппарат;
- работа с оптическими приборами.

С каждой из перечисленных нагрузок специалист по информационной безопасности может столкнуться в ходе своей работы.

Для снижения воздействия вредных психофизиологических факторов, влияющих на психоэмоциональное состояние специалиста по защите информации, необходимо выполнять физические упражнения, направленные на:

- сокращение периода вработывания в умственную деятельность, выполняя упражнения меньшей интенсивности;
- снижение эмоциональных перегрузок путем периодического отдыха от трудовой деятельности;
- мышечное расслабление путем выполнения периодических разминочных упражнений;

— снижение нагрузки на зрение путем использования специализированных очков, снижающих нагрузку на зрение при работе с экранами, а также выполнения гимнастики для глаз.

Заключение

В результате выполнения дипломного проекта была произведена разработка методики настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.

Для ее разработки был произведен анализ руководящих документов по защите информации и механизмов защиты операционной системы специального назначения «Astra Linux Special Edition».

В ходе дипломного проектирования была произведена разработка модели угроз и действий нарушителя.

На основании полученных данных была произведена разработка методики настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.

Для автоматизации настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну была произведена разработка скриптов автоматической настройки части компонентов разработанной методики.

Для подтверждения работоспособности методики была произведена проверка настройки операционной системы специального назначения «Astra Linux Special Edition» для обеспечения защиты информации, содержащей сведения, составляющие государственную тайну.

Все поставленные задачи на дипломное проектирование были выполнены в полном объеме.

Список используемых источников

- 1 ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. [Электронный ресурс] URL: <https://docs.cntd.ru/document/1200108858> (дата обращения 05.02.2022).
- 2 Методический документ. Методика оценки угроз безопасности информации. — ФСТЭК России, — 2021. [Электронный ресурс] URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhdenn-fstek-rossii-5-fevralya-2021> (дата обращения 05.02.2022).
- 3 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. — ФСТЭК России, — 2008. [Электронный ресурс] URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114spetsialnye-normativnye-dokumenty/379bazovaya-model-ugroz-bezopasnosti-perso-nalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii2008god> (дата обращения 05.02.2022).
- 4 Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие для вузов / П.В. Буренин, П.Н. Девянин, Е.В. Лебеденко, В.Г. Проскурин, А.Н. Цибуля; Под редакцией доктора техн. наук П.Н. Девянина, — 3-е издание, стереотипное — М.: Горячая линия — Телеком, 2019 — 363 с.: ил. (дата обращения 05.02.2022).
- 5 Department of defense trusted computer system evaluation criteria / Department of defense standard, — USA, — 1985. (дата обращения 06.02.2022).
- 6 Методические указания к лабораторным работам: Модель безопасности ОС Windows / Сост. Лясин Д.Н., Саньков С.Г.; Волгоград. гос. техн. ун-т. — Волгоград, 2011, — 24 с. (дата обращения 06.02.2022).
- 7 Паспорт национального проекта «Национальная программа

«Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7)[Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_328854/ (дата обращения 06.02.2022).

8 Государственный реестр сертифицированных средств защиты информации. [Электронный ресурс] URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00> (дата обращения 06.02.2022).

9 Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации. — Руководящий документ, — Гостехкомиссия России, — 1992. [Электронный ресурс] URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-> (дата обращения 06.02.2022).

10 Общие сведения по сертификации. [Электронный ресурс] URL: <http://clsz.fsb.ru/clsz/certification.htm> (дата обращения 06.02.2022).

11 Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» [Электронный ресурс] URL: <http://www.fsb.ru/fsb/npd/more.htm%21id%3D10343056%40fsbNpa.html> (дата обращения 10.04.2022).

12 Указ Президента РФ от 24.01.1998 N 61 «О перечне сведений, отнесенных к государственной тайне» [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_17631/de05c3e5586ac7ac5c8f62e2c129ed105bbc2422/ (дата обращения 10.04.2022).

13 ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. [Электронный ресурс] URL: <https://docs.cntd.ru/document/1200058320> (дата обращения 10.04.2022).

14 ГОСТ Р 51275-2006 Защита информации. Объект информатизации.

Факторы, воздействующие на информацию. Общие положения. [Электронный ресурс] URL: <https://docs.cntd.ru/document/1200057516> (дата обращения 10.04.2022).

15 ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования. [Электронный ресурс] URL: <https://cyberleninka.ru/article/n/osnovnye-ugrozy-bezopasnosti-operatsionnyh-sistem> (дата обращения 10.04.2022).

16 Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. — ФСБ РФ. — 2008 г. N 149/54-144 [Электронный ресурс] URL: <https://docs.cntd.ru/document/420220524> (дата обращения 10.04.2022).

17 Скрыпников А. В. Основные угрозы безопасности операционных систем / А. В. Скрыпников, Е. В. Чернышова, А. В. Василенко. — Текст : непосредственный // Евразийский Союз Ученых. — 2015. — № 3. — С. 43-46. [Электронный ресурс] URL: <https://docs.cntd.ru/document/1200065692> (дата обращения 10.04.2022).

18 Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие для вузов / П.В. Буренин, П.Н. Девянин, Е.В. Лебеденко, В.Г. Проскурин, А.Н. Цибуля; Под редакцией доктора техн. наук П.Н. Девянина, — 3-е издание, стереотипное — М.: Горячая линия — Телеком, 2019 — 363 с.: ил. (дата обращения 01.05.2022).

19 ГОСТ 12.0.003-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Опасные и вредные производственные факторы. Классификация. [Электронный ресурс] URL: <https://docs.cntd.ru/document/1200136071> (дата обращения 8.05.2022).