УДК 004.056

В.А. Шипунова
Московский институт электроники и математики имени А.Н. Тихонова НИУ ВШЭ

РЕКОМЕНДАЦИИ ПО НАСТРОЙКЕ ОПЕРАЦИОННЫХ СИСТЕМ ДЛЯ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ПРИКАЗА ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ № 17 С УЧЕТОМ НОВЫХ ТРЕБОВАНИЙ

Операционные системы играют ключевую роль в области защиты информации, так как они служат основой для работы программного обеспечения, управления ресурсами и обеспечения взаимодействия между аппаратными компонентами и пользователями. С учетом текущей политической ситуацией и Указом Президента № 250, переход на отечественные операционные системы становится важной стратегической задачей для государственных учреждений и организаций. ОС Astra Linux Special Edition 1.8 обеспечивает надежную платформу для обработки и хранения данных и разработана с учетом требований российских регуляторов. Ее правильная настройка с учетом требований нормативно-правовых актов поможет предотвратить утечку конфиденциальной информации.

Информационная безопасность, государственные информационные системы, операционные системы, ФСТЭК России, Astra Linux Special Edition.

Важным аспектом обеспечения информационной безопасности на предприятиях и в организациях является соблюдение требований Федеральной службы по техническому и экспортному контролю (ФСТЭК России).

Приказ ФСТЭК России от 11 февраля 2017 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и недавно опубликованные изменения к нему устанавливают обязательные требования по защите информации в государственных и иных информационных системах [1, 2].

Помимо требований ФСТЭК России, Указ Президента РФ № 250 от 30 марта 2022 года обязывает государственные органы и организации использовать российское программное обеспечение [3].

Операционная система Astra Linux Special Edition версии 1.8 представляет собой оптимальное решение для организаций, стремящихся соответствовать требованиям нормативных актов и повысить уровень безопасности своих информационных систем. Данная ОС была выпущена весной 2024 года, и вендор еще не успел опубликовать рекомендации по настройке для соответствия требованиям приказов ФСТЭК России, а продукт уже активно используется в ИС.

Для того, чтобы ОС ALSE версии 1.8 удовлетворяла требованием безопасности информации необходимо правильно ее настроить. В данной статье будут даны рекомендации по настройке ОС для соответствия требованиям Приказа ФСТЭК России № 17 с учетом недавно опубликованных изменений.

Для реализации поставленной задачи требуется проведение анализа нормативно-правовых актов в сфере информационной безопасности, проведения практических экспериментов по настройке ОС.

Описание ОС ALSE версии 1.8

Astra Linux Special Edition – это российская операционная система, сертифицированная по требованиям безопасности ФСТЭК России, со встроенными средствами защиты информации.

ALSE имеет три уровня защищенности [4]:

Первый уровень – базовый – «Орел», применяется для информации, доступ к которой не ограничен в соответствии с законодательством Российской Федерации в значимых объектах КИИ, где не обязательно использовать сертифицированные ФСТЭК России средства защиты информации [5].

Второй уровень – усиленный – «Воронеж», используются для обработки информации ограниченного доступа в ГИС, ИСПДн и значимых объектах КИИ.

Третий уровень – максимальный – «Смоленск», применяется для работы с информацией любой категории доступа в ГИС, ИСПДн, значимых объектах КИИ и иных системах, которые обрабатывают конфиденциальные данные.

Среди всех рассмотренных уровней защищенности максимальный и усиленный обладают действующим сертификатом соответствия ФСТЭК России, который подтверждает их соответствие следующим требованиям:

– «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016);

– «Профиль защиты операционных систем типа "А" первого класса защиты ИТ.ОС.А1.ПЗ»;

– «Профиль защиты операционных систем типа "А" второго класса защиты ИТ.ОС.А2.ПЗ»;

– «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения

безопасности информационных технологий» (ФСТЭК России, 2020).

Операционная система Astra Linux Special Edition 1.8 включает в себя следующие функции защиты [4]:

– идентификация и аутентификация пользователей;

– мандатное управление доступом;

– мандатный контроль целостности;

– защита систем управления базами данных и средств виртуализации;

– управление доступом в режиме дискретности;

– регистрация событий безопасности;

– мониторинг за подключенными носителями информации;

– контроль целостности данных.

Выбор мер защиты информации

Для определения класса защищенности государственной информационной системы в соответствии с требованиями Приказа ФСТЭК России № 17 необходимо выявить уровень значимости обрабатываемых данных (низкий, средний, высокий) и масштаб системы (объектовый, региональный, федеральный).

В данной статье будет описана реализация мер защиты информации, которые входят в базовый набор для ИС третьего класса защищенности (К3). Подсистема защиты информации должна реализовывать следующие функции [1, 2]:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защита машинных носителей информации;

– регистрация событий безопасности;

– антивирусная защита;

– контроль (анализ) защищенности информации;

– обеспечение целостности информационной системы и информации;

– защита среды виртуализации;

– защита технических средств;

– защита информационной системы, ее средств, систем связи и передачи данных;

– защита информационной системы от атак, направленных на отказ в обслуживании.

Рекомендации по настройке

С помощью ОС невозможно реализовать все необходимые функции защиты, рассмотренные выше. Рекомендации по настройке даны только для тех мер защиты, реализация которых осуществляется посредством ОС ALSE 1.8 без применения дополнительных СЗИ, и представлены в таблице [6–8].

Таблица

Рекомендации по настройке

Обозначение меры	Рекомендации по настройке	Реализация с помощью средств ALSE
Идентификация и аутентификация субъектов и объектов доступа (ИАФ)		
ИАФ.1	Для всех видов доступа пользователей должны быть реализованы идентификация и аутентификация. Пароли, аппаратные средства, биометрические данные должны использоваться для аутентификации пользователей в системе. В системе необходимо гарантировать возможность точного сопоставления идентификатора пользователя с процессами, выполняемыми от его имени.	Данная мера реализуется в операционной системе через механизм PAM.
ИАФ.3	Для реализации данной меры необходимо: – создать уникальный идентификатор, с помощью которого будут распознаваться пользователи и/или устройства; – блокировать возможность повторного применения идентификатора; – удалять идентификатор пользователей после периода бездействия, который устанавливается для каждой системы отдельно.	Управлять идентификаторами пользователей (UID) и устройств (UUID) можно с помощью командной строки.
ИАФ.4	Управление средствами аутентификации осуществляется с помощью: – изменения аутентификационных данных, которые задаются производителем ОС ALSE; – генерации и предоставления начальные аутентификационные данные пользователей; – задание параметров пароля: длина – не меньше 6 символов, алфавит – от 60 символов, количество неудачных попыток аутентификации – от 3 до 10, при достижении которых, устройство или учетная запись должны быть заблокированы. – смены паролей раз в 120 дней.	Для реализации централизованной аутентификации пользователей нужно настроить систему Kerberos.
ИАФ.5	Защита обратной связи между системой и пользователем в процессе аутентификации достигается путем скрытия реальных значений аутентификационной информации и (или) количества вводимых символов.	По умолчанию в Astra Linux скрывается аутентификационная информация при вводе информации в диалоговом интерфейсе.
ИАФ.6	Внешние пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться в соответствии с ИАФ.1.	Реализация данной меры осуществляется с помощью средств, описанных в мере ИАФ.1

Обозначение меры	Рекомендации по настройке	Реализация с помощью средств ALSE
Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.1	Для выполнения требований данной меры необходимо: – определить тип учетной записи (внутренний/внешний пользователь; системная/ гостевая/временная и т.д.); – верифицировать пользователей с помощью подтверждения их личности в соответствии с занимаемыми должностями во время создания учетной записи; – создавать, активировать, блокировать и удалять учетные записи всех пользователей системы; – удалять учетные записи временных пользователей, создающиеся для выполнения задач в установленное время; – обеспечивать пользователям различные уровни доступа к системе, в зависимости от их задач и взаимодействия с другими ресурсами; – блокировать временные учетные записи по истечении установленного срока их действия.	Данная мера может реализоваться с помощью средств управления доменным пользователями ALD.
УПД.2	Метод управления доступом определяется в зависимости от требований системы. Для реализации данной меры нужно: – управлять доступом пользователей при входе в информационную систему; – контролировать доступ пользователей к техническим средствам, устройствам и внешним подключениям; – регулировать доступ пользователей к объектам, которые создаются с помощью общесистемным ПО.	Способ управления и правила разграничения можно настроить с помощью мандатного контроля целостности (МКЦ) и управления доступом. Уровни целостности назначаются автоматически при включении модуля контроля целостности. При необходимости можно настроить их вручную.
УПД.4	В системе необходимо четко разграничить полномочия (роли) между привилегированными и непривилегированными пользователями системы в зависимости от их должностных обязанностей.	Это достигается благодаря использованию МКЦ, что позволяет обеспечить дополнительный уровень безопасности и контроля доступа. Для каждого пользователя, системного файла, папки или процесса устанавливаются соответствующие уровни целостности.
УПД.5	Для реализации данной меры в системе необходимо установить права для: – непривилегированных пользователей системы и процессов, которые они запускают; – привилегированных пользователей, которые отвечают за функционирование системы. Только у определенных пользователей в Модели угроз пользователей должен быть доступ к системе.	Реализация данной меры осуществляется с помощью средств, описанных в мере УПД.4
УПД.6	При достижении лимита попыток входа должна быть настроена блокировка устройства или учетной записи пользователя. Реализация данной меры осуществляется с помощью средств, описанных в мере ИАФ.4	Это достигается с помощью инструмента управления политикой безопасности доменных пользователей ALD.
УПД.10	Для реализации данной меры нужно обеспечить автоматическое завершение сеанса пользователя после установленного периода бездействия или по его запросу. Все действия, связанные с доступом к информации и ее отображением, должны быть заблокированы, за исключением тех, которые необходимы для разблокировки сеанса.	Управление параметрами политики блокировки осуществляется с помощью средств управления рабочим столом Fly (fly-admin-theme)
УПД.11	Необходимо определить перечень действий, которые может выполнять пользователь до завершения процедур идентификации и аутентификации. Действия, которые не были разрешены, должны быть заблокированы. До процедуры идентификации и аутентификации пользователь может получить доступ к общедоступной информации. Только привилегированный пользователь системы может обойти эти процедуры, если ему необходимо восстановить работу ИС в случае сбоев.	Пользователи могут получать доступ к системе, проходить идентификацию и аутентификацию, а также выполнять разрешенные действия. Для этого необходимо настроить графический вход в систему через fly-admin-dm, изменить параметры системного загрузчика Grub и управлять системными блокировками.
УПД.15	Реализация данной меры должна включать: – установку разрешенных видов доступа (беспроводного, проводного и т.д.) к объектам информационной системы с помощью мобильных устройств. – блокирование запуска программного обеспечения для взаимодействия с мобильными средствами без команды пользователя.	Эта мера осуществляется с помощью инструмента для управления доступом к подключаемым устройствам (udev).

Обозначение меры	Рекомендации по настройке	Реализация с помощью средств ALSE
Ограничение программной среды (ОПС)		
ОПС.3	Для обеспечения безопасности информационной системы оператор устанавливает перечни разрешенного («белый список») и запрещенного («черный список») ПО. В разрешенный перечень входят компоненты, необходимые для корректной работы системы, а в запрещенный – программы, представляющие угрозу для безопасности Установка ПО должна производиться исключительно от имени администратора, в строгом соответствии с УПД.5.	Реализация данной меры возможна с помощью системы управления программными пакетами (synaptic) и проверки целостности системы fly-admin-int-check.
Защита машинных носителей информации (ЗНИ)		
ЗНИ.1	Учет машинных носителей информации подразумевает присвоение каждому из них регистрационного или учетного номера. Эти номера должны быть зафиксированы в базах данных, используемых для учета устройств под управлением Astra Linux.	Реализуется аналогично, как и мера УПД.15.
ЗНИ.8	Для реализации удаления файлов нужно: – реализовать запись в файлы случайной битовой последовательности; – стереть все упоминания об этих файлах; – почистить журнал, в который записывается информация о файловой системе; – перезаписать адресные пространства машинных носителей информации случайными битами для подготовки к дальнейшему форматированию.	Для осуществления данной меры необходимо настроить механизм очистки внешней памяти astra-secdel-control.
Контроль (анализ) защищенности информации (АНЗ)		
АНЗ.2	Для контроля установки обновлений нужно удостоверится, что версий системных, прикладных и специальных ПО соответствуют версии, представленной на сайте вендора, а также актуальности баз данных для средств антивирусной защиты.	Перед установкой обновлений Astra Linux можно использовать инструменты для регулярного контроля целостности. После успешной установки обновления динамический контроль целостности файлов на установочном диске поможет вам убедиться в целостности программных пакетов. Для этого вам потребуется утилита fly-admin-int-check и файл gostsums.txt для регламентного контроля целостности. Чтобы контролировать процесс установки обновлений операционной системы, вы можете воспользоваться автоматизированным инструментом «Проверка обновлений» из пакета fly-update-notifier. Эта программа позволит вам отслеживать и проверять установленные обновления в режиме реального времени.
АНЗ.4	Необходимо проводить контроль состава программного обеспечения и СЗИ.	Контроль целостности осуществляется с помощью утилиты fly-admin-int-check, а также с помощью средств аудита zabbix.
АНЗ.5	Для реализации данной меры необходимо: – осуществлять контроль процесса генерации и смены паролей пользователей, которые реализованы с помощью мер ИАФ.1 и ИАФ.4; – контролировать создание и удаление учетных записей пользователей в соответствии с мерой УПД.1; – разграничивать доступ пользователей в соответствии с УПД.2; – контролировать использование полномочий пользователями в соответствии с мерами УПД.4 и УПД.5.5.	В Astra Linux события безопасности регистрируются с помощью специальной подсистемы, которая состоит из двух компонентов – auditd и syslog-ng-mod-astra, – которые осуществляют ведение журналов аудита событий безопасности. Для просмотра и анализа результатов регистрации событий безопасности в ОС можно использовать встроенные средства просмотра журналов: fly-event-viewer и ksystemlog.
Обеспечение целостности информационной системы и информации (ОЦЛ)		
ОЦЛ.3	Для восстановления объектов файловой системы в нештатных ситуациях необходимо обеспечить: – восстановление из резервных копий; – возврат ФС в начальное состояние, обеспечивающее штатную работу.	Для того чтобы система могла быть восстановлена в случае сбоя, предусмотрен специальный режим восстановления и средства резервного копирования. Это можно реализовать с помощью функций командой строки (tar, rsync).

Как можно заметить, на данный момент с помощью внутренних возможностей ОС ALSE 1.8 невозможно обеспечить реализацию всех необходимых мер защиты информации, описанные в Приказах ФСТЭК России. Для некоторых групп мер требуются дополнительные средства защиты информации.

Выводы

Исходя из проведенного анализа функций защиты информации, которые могут быть реализованы с помощью операционной системы для выполнения требований Приказа ФСТЭК России № 17, включая недавно внесенные изменения, которые предъявляются для обеспечения защиты ГИС, были определены те, которые можно обеспечить только посредством ОС. Особое внимание уделено рекомендациям по настройке ОС ALSE 1.8 с учетом реализации мер защиты информации для информационных систем третьего класса защищенности (К3). Однако для полного соответствия требованиям приказа недостаточно использовать только ОС. Обеспечение безопасности информационных систем требует комплексного подхода, включающего использование различных СЗИ, таких как межсетевые экраны, средства антивирусной защиты и другие инструменты, способствующие созданию надёжной подсистемы защиты.

Литература

1. О внесении изменений в требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17, и требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации, утвержденные приказом федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 : Приказ ФСТЭК России от 28.08.2024 г. № 159. – https://www.consultant.ru/document/cons_doc_LAW_488983/ (дата обращения: 05.03.2025). – Текст : электронный.

2. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ ФСТЭК от 11.02.2013 № 17 : в редакции от 25.11.2022. – URL: https://docs.cntd.ru/document/499002630 (дата обращения: 05.03.2025). – Текст : электронный.

3. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : указ Президента РФ от 1.05.2022 г. № 250 : в редакции от 13.06.2024 г. – URL: https://base.garant.ru/404561984/ (дата обращения: 05.03.2025). – Текст : электронный.

4. Astra Linux Special Edition. – URL: https://ric-1c.ru/product/sistemnoe-programmnoe obespechenie/rossiyskoe_programmnoe_obespechenie/astra_linux/astra_linux_special_edition/ (дата обращения: 23.09.2024). – Text : electronic.

5. Методы обеспечения безопасности Astra Linux special Edition / П. С. Зылева, И. Е. Пестов, Тремель И. С., Юрова У. С. // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция : сборник научных статей : в 4 томах. – Санкт-Петербург : СПбГУТ, 2023. – Т. 1. – С. 553–558.

6. Операционная система Astra Linux Desktop. – URL: https://astralinux.ru/os/astra-linux-desktop/ (дата обращения: 23.09.2024). – Текст : электронный.

7. Возможности реализации мер защиты информации в соответствии с приказом ФСТЭК России № 17 средствами операционной системы специального назначения Astra Linux Special Edition РУСБ.10015-01 очередное обновление 1.7 и РУСБ.10152-02 очередное обновление 4.7. – URL: https://wiki.astralinux.ru/pages/viewpage.action?pageId=181666089 (дата обращения: 24.09.2024). – Текст : электронный.

8. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8). Эксплуатационная и дополнительная документация. – URL: https://wiki.astralinux.ru/pages/viewpage.action?pageId=302043140 (дата обращения: 01.10.2024). – Текст : электронный.

V.A. Shipunova

Moscow Institute of Electronics and Mathematics named after A.N. Tikhonov of the Higher School of Economics

RECOMMENDATIONS FOR CONFIGURING OPERATING SYSTEMS TO MEET THE REQUIREMENTS OF ORDER NO. 17 OF FEDERAL SERVICE FOR TECHNICAL AND EXPORT CONTROL

Operating systems play a key role in information security, as they serve as the basis for software operation, resource management, and interaction between hardware components and users. Taking into account the current political situation and Presidential Decree No. 250, the transition to domestic operating systems is becoming an important strategic task for government agencies and organizations. The Astra Linux Special Edition 1.8 OS provides a reliable platform for data processing and storage and is designed to meet the requirements of Russian regulators. Its correct configuration, taking into account the requirements of regulatory legal acts, will help prevent the leakage of confidential information.

Information security, state information systems, operating systems, FSTEC of Russia, Astra Linux Special Edition.