DOI 10.58351/2949-2041.2025.21.4.013

Пинчук Антон Сергеевич, студент
Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознаменное училище имени генерала армии С.М. Штеменко
г. Краснодар

АНАЛИЗ ОШИБОК КОНФИГУРАЦИИ МЕХАНИЗМОВ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ПРАВ ДОСТУПА В ОС ASTRA LINUX

Аннотация: В первой главе выполнен анализ механизмов защиты информации и разграничения прав доступа в операционной системе специального назначения Astra Linux, а также рассмотрены типовые ошибки их конфигурации. Проведен обзор существующих решений для обнаружения ошибок настроек и выявлены их ограничения. Особое внимание уделено актуальным проблемам обеспечения безопасности вследствие некорректных настроек. По результатам анализа сформулирована задача разработки специализированного программного средства для автоматизированной проверки конфигураций.

Ключевые слова: Astra Linux; безопасность ОС; ошибки конфигурации; аудит безопасности.

Введение. Актуальность рассматриваемой темы обусловлена ростом числа киберугроз и высокой ценностью защищаемых данных в современных информационных системах. В государственных и корпоративных структурах широкое применение находят защищённые операционные системы, способные обрабатывать конфиденциальную информацию. Отечественная ОС специального назначения Astra Linux Special Edition относится к числу таких систем, обладая сертификатами ФСТЭК и Минобороны России для работы с информацией вплоть до уровня «совершенно секретно». В Astra Linux изначально интегрирован комплекс механизмов защиты, однако эффективность этих механизмов напрямую зависит от корректности их настройки администраторами. Ошибки конфигурации компонентов безопасности могут свести на нет преимущества встроенных средств защиты, создавая уязвимости и каналы для несанкционированного доступа. В связи с этим возникает необходимость тщательного анализа существующих механизмов защиты Astra Linux, типичных ошибок их настройки и инструментов, позволяющих выявлять такие ошибки. Настоящая глава посвящена указанному анализу, результаты которого послужат основой для дальнейшей разработки специализированного программного обеспечения, автоматизирующего выявление ошибок конфигурации. В рамках главы рассмотрены встроенные механизмы обеспечения безопасности и управления доступом в Astra Linux, проведена классификация наиболее распространённых ошибок настройки, а также проанализированы существующие подходы и утилиты для диагностики неправильной конфигурации. Это позволит определить недостатки текущих решений и обосновать необходимость создания нового программного средства для повышения безопасности за счет своевременного обнаружения ошибок конфигурации.

Обзор механизмов защиты информации и прав доступа в ОС СН Astra Linux. Операционная система Astra Linux Special Edition (ОС специального назначения) включает в себя комплекс встроенных средств защиты информации. К ключевым механизмам относятся:

1. **Дискреционный контроль доступа (DAC)** – классическая модель *UNIX*-подобных систем, основанная на разделении прав доступа на основе владельцев и групп, а также списков контроля доступа (ACL). Администратор и владельцы объектов могут задавать разрешения на чтение, запись и выполнение для файлов и каталогов. В Astra Linux поддерживаются стандартные POSIX-разрешения и расширенные ACL, что позволяет гибко настраивать права доступа. Однако DAC по своей природе допускает, что владелец объекта может намеренно или случайно изменить права доступа к своему ресурсу на менее строгие.

2. **Мандатное управление доступом (MAC)** – механизм принудительного (мандатного) разграничения доступа, при котором каждому объекту и субъекту системы присваиваются метки безопасности (уровень конфиденциальности, категории) согласно политике безопасности. Доступ определяется на основе сравнения меток: даже если дискреционные права позволяют доступ, мандатные ограничения могут его запретить, предотвращая утечку информации более высокого уровня секретности. В Astra Linux реализована полноценная поддержка MAC на уровне ядра, графического интерфейса, баз данных и сетевого взаимодействия. В частности, режим безопасности «Смоленск» предусматривает использование мандатных меток в сетевых протоколах IPv4/IPv6 согласно ГОСТ Р 58256-2018 для защиты данных при передаче по сети. Мандатное управление доступом существенно повышает уровень защищённости системы, блокируя несанкционированный доступ даже в случаях, когда пользователи по ошибке или злоумышлено ослабляют дискреционные права доступа. Иными словами, MAC обеспечивает дополнительную защиту от угроз, связанных с неправильной настройкой DAC, которая не запрещает владельцу ресурса открывать доступ к нему другим.

3. **Контроль целостности и аудит событий.** Astra Linux включает средства мандатного контроля целостности (МКЦ) – назначение уровня доверия (целостности) для процессов и объектов, что препятствует влиянию процессов низкого уровня доверия на более критичные процессы и файлы. Одновременно система обеспечивает ведение журнала аудита: регистрации действий пользователей и событий безопасности. Специальная подсистема аудита фиксирует попытки НСД (несанкционированного доступа) и другие значимые инциденты, предоставляя администратору безопасности полную картину происходящего. Журналы событий защищены от несанкционированного изменения и могут размещаться на выделенном узле или рабочем месте администратора безопасности. Наличие полномасштабного аудита позволяет выявлять попытки обхода настроек безопасности и реакцию механизмов защиты на инциденты. Контроль целостности, в свою очередь, обеспечивает выявление несанкционированных изменений системных файлов, конфигураций и исполняемых модулей, что важно для своевременного обнаружения компрометации системы.

4. **Идентификация, аутентификация и управление учетными записями.** В Astra Linux реализована стандартная для UNIX-систем подсистема PAM (Pluggable Authentication Modules) для гибкого управления аутентификацией. Через настройку PAM-модулей администратор может определять политику сложных паролей, правила блокировки учетных записей, порядок проверки учетных данных по различным источникам (локальные файлы, LDAP/ALD и т.п.). Надежная аутентификация пользователей и разграничение учетных записей с различными привилегиями (обычные пользователи, администраторы, пользователи с повышенными правами) являются важной частью общей системы защиты. В Astra Linux также присутствует собственная система каталогов и доменной аутентификации (ALD – Astra Linux Directory), упрощающая централизованное управление пользователями и их правами в масштабах сети. Корректная настройка механизмов идентификации и аутентификации предотвращает несанкционированный доступ под видом легитимных пользователей.

Перечисленные компоненты образуют комплексную систему защиты Astra Linux, соответствующую строгим требованиям регуляторов. Все механизмы должны быть грамотно сконфигурированы и совместно использоваться администраторами для обеспечения многоуровневой защиты от несанкционированного доступа, утечки информации и нарушений целостности. Далее рассмотрены типовые ошибки, которые допускаются при настройке этих механизмов на практике.

Классификация типовых ошибок конфигурации. На основе анализа эксплуатационной документации и опыта администрирования ОС Astra Linux можно выделить несколько категорий наиболее распространённых ошибок в настройке средств защиты:

1. **Ошибки в мандатной политике безопасности.** Неправильная маркировка файлов, процессов и сетевых ресурсов уровнями конфиденциальности либо некорректное присвоение категорий. Например, файл с конфиденциальными сведениями может быть помечен более низким грифом секретности, чем требуется, что теоретически позволит пользователям с недостаточным допуском получить к нему доступ. Другая распространённая ошибка – отсутствие необходимых мандатных ограничений (MAC отключен или находится в режиме, допускающем нарушение политики разграничения). Администраторы могут намеренно ослаблять требования MAC ради упрощения работы, что приводит к снижению уровня защищенности. К этой же категории относятся нарушения правил мандатного разграничения при сетевом взаимодействии – несоответствие меток безопасности узлов или неправильно настроенные фильтры по меткам, из-за чего пакеты блокируются либо, напротив, проходят без должного контроля.

2. **Ошибки дискреционных прав доступа.** Эта группа ошибок связана с некорректными настройками прав файловой системы и ACL. Типичные примеры: установка чрезмерно широких прав доступа на файлы и каталоги (например, *777*, дающий чтение/запись/исполнение всем пользователям), оставление критических файлов и конфигураций с правами по умолчанию, которые позволяют чтение посторонним, неправильное владение файлами (ключевые файлы или скрипты, принадлежащие привилегированным пользователям, оставлены с правами записи для группы или других). Также сюда относятся случаи, когда администратор забывает удалить или обезопасить учетные записи по умолчанию, гость и т.п., или не ограничивает возможности использования команд *sudo* только необходимыми действиями. Ошибки DAC часто возникают по причине человеческого фактора и недостаточного внимания к принципу минимальных привилегий. Без дополнительного контроля такие просчёты могут позволить злоумышленнику эскалировать привилегии или получить доступ к закрытым данным.

3. **Неправильные настройки аутентификации и PAM.** Сюда включаются ошибки, связанные с управлением учетными записями и политиками паролей. Примеры: использование тривиальных или единых паролей на критических учетных записях, отключение или неправильная настройка политики сложных паролей, отсутствие ограничения на количество неудачных попыток входа (что открывает возможность перебора пароля), неверный порядок модулей PAM, что может позволять обход отдельных этапов проверки. Возможны случаи, когда администратор не настроил требование регулярной смены паролей или не отключил/удалил неиспользуемые учетные записи. Также в эту категорию попадают ошибки конфигурации системы доменной аутентификации ALD/LDAP – например, некорректно настроенное взаимодействие с каталогом, вследствие чего проверка учетных данных может переходить в автономный режим с устаревшими данными либо, наоборот, допускать вход только при доступности контроллера домена, что может нарушить доступность. В совокупности такие ошибки облегчают злоумышленнику подбор или компрометацию учетной записи либо приводят к отказам в обслуживании легитимных пользователей.

4. **Ошибки конфигурации подсистем целостности и других средств защиты.** В эту группу можно отнести различные упущения при включении и настройке встроенных средств безопасности, не относящиеся непосредственно к правам доступа. Например, администратор мог отключить модуль мандатного контроля целостности (МКЦ) или настроить его некорректно, позволив недоверенным процессам изменять критичные файлы. Либо не были установлены или обновлены списки доверенного ПО для механизма «замкнутая программная среда» (если такой используется), из-за чего система не блокирует запуск потенциально опасных программ. Сюда же можно включить ошибки в настройке SELinux или аналогичных политик, если такие механизмы задействованы в системе (в некоторых конфигурациях Astra Linux могут использоваться политики SELinux/AppArmor для дополнительных ограничений). Неправильное задание политик безопасности (профилей) для подобных механизмов может привести либо к излишне строгим ограничениям, мешающим работе, либо к избыточным

разрешениям, не предотвращающим атаки. Также можно упомянуть недостатки в конфигурации антивирусных средств или систем обнаружения вторжений, если они интегрированы: например, несвоевременное обновление сигнатур, отключение отдельных проверок и т.д. Каждая из этих ошибок сама по себе может не быть прямой уязвимостью, однако в комплексе ослабляет общий уровень защиты системы.

5. **Ошибки настройки сетевых служб и межсетевого экранирования.** Данная категория охватывает промахи в конфигурировании встроенных сетевых защит. Astra Linux, как и другие UNIX-системы, полагается на подсистему *netfilter/iptables* для фильтрации трафика, а также может работать совместно с внешними межсетевыми экранами. Типичные ошибки: оставленные без фильтрации открытые сетевые порты, разрешение лишних сервисов, работающих с повышенными привилегиями, неправильно настроенные правила брандмауэра (например, разрешающие больше, чем нужно, или нарушающие мандатные метки в «Смоленске»). Кроме того, к настройкам сети относится конфигурация удаленного доступа и SSH: отсутствие ограничения по IP-адресам, разрешение входа под учетной записью *root* по SSH, отключение двухфакторной аутентификации там, где она необходима. Ошибки подобного рода упрощают сетевому злоумышленнику задачу проникновения в систему или развития атаки внутри защищенного контура. Несмотря на то, что эти промахи часто лежат вне собственно ОС (на стыке с сетью), они непосредственно связаны с неверной реализацией механизмов защиты информации на уровне конфигурации системы.

Предложенная классификация охватывает наиболее распространённые ошибки конфигурации, способные негативно сказаться на безопасности Astra Linux. Выявление таких ошибок на ранней стадии позволяет предотвратить инциденты, поэтому в следующем разделе рассмотрены существующие средства и методы для автоматизированного поиска ошибок настройки.

Анализ существующих решений по выявлению ошибок конфигурации. В настоящее время для обнаружения уязвимостей и проблем конфигурации в операционных системах используются как общесистемные инструменты аудита, так и специализированные продукты. Рассмотрим наиболее известные подходы и их применимость к Astra Linux.

Одним из стандартных подходов является использование фреймворка **SCAP (Security Content Automation Protocol)** – набора спецификаций для описания требований безопасности и проверки системы на соответствие им. Существуют открытые реализации SCAP, в частности проект **OpenSCAP**, который позволяет сканировать систему на предмет соответствия заданным политикам безопасности. С помощью OpenSCAP можно автоматически проверить параметры конфигурации безопасности системы и выявить признаки отклонений, используя правила, основанные на стандартах (OVAL, XCCDF и др.). Многие операционные системы имеют готовый SCAP-контент (профили настроек) – например, проверка соответствия рекомендациям Центра интернет-безопасности (CIS Benchmarks) или требованиям регуляторов. Однако для Astra Linux специализированный контент SCAP публично недоступен, и профили, разработанные для других дистрибутивов (Ubuntu, Red Hat и др.), лишь частично применимы из-за отличий в механизмах (например, наличие мандатного доступа). Таким образом, OpenSCAP может быть применён в Astra Linux для базовой проверки (например, наличия важных обновлений, общих уязвимостей и некоторых настроек), но не охватывает специфические аспекты безопасности ОС специального назначения без разработки отдельных модулей проверки.

Другим распространённым инструментом аудита безопасности является **Lynis** – открытая утилита для анализа конфигурации и «усиления» (hardening) UNIX-систем. Lynis выполняет последовательность тестов конфигурации: проверяет права критических файлов, параметры ядра, настройки служб, наличие ненужных пакетов, параметры аутентификации и т.д. Отчет Lynis содержит предупреждения о потенциально неверных настройках и рекомендации по повышению безопасности. Преимущество Lynis в том, что он не требует предварительно подготовленных профилей – программа сама включает знания о типовых лучших практиках. Для Astra Linux Lynis может выявить, к примеру, отсутствие требований к

сложным паролям, отключенный аудит или слишком широкие права на ключевые каталоги. Однако у Lynis нет понимания мандатных меток и специфических компонентов Astra Linux; соответственно, он не сможет оценить правильность применения, скажем, мандатных политик или настроек МКЦ. Тем не менее, как инструмент общего назначения Lynis полезен для начального аудита и может использоваться администраторами Astra Linux в отсутствие лучшей альтернативы.

Существуют и коммерческие продукты, нацеленные на аудит соответствия систем требованиям безопасности. В российской практике известны решения, интегрирующие методики ФСТЭК: например, комплекс **RedCheck** от компании «Инфотекс» либо продукты НПО «Эшелон». Так, в Astra Linux заявлена поддержка взаимодействия с модулем **«Сканер-ВС»** – компонентом комплекса анализа защищённости и мониторинга безопасности от НПО «Эшелон». Подобные сканеры позволяют проводить комплексную проверку узла на наличие известных уязвимостей, несоответствий настройкам и даже имитацию атак. Использование «Сканер-ВС» в связке с Astra Linux удовлетворяет требованиям регуляторов по наличию средств контроля эффективности защиты и может обеспечить централизованный мониторинг безопасности в инфраструктуре. Однако доступность таких решений ограничена их коммерческим характером и узкой специализацией: они, как правило, доступны крупным организациям и требуют обновляемых баз знаний. Кроме того, детали реализации этих сканеров закрыты, и неизвестно, насколько глубоко они анализируют внутренние механизмы Astra Linux, например правильность мандатных меток или политики целостности, либо фокусируются преимущественно на известных уязвимостях и общих настройках.

Помимо автоматизированных сканеров, применяются **регламенты и чек-листы безопасности**, по которым администраторы вручную проверяют конфигурацию. Для Astra Linux, как сертифицированной ОС, существуют руководства администратора и контрольные списки настроек для соответствия требованиям ФСТЭК. Например, документирован перечень параметров, которые необходимо проверить при вводе системы в эксплуатацию (конфигурация DAC/MAC, параметры аудита, настройки сетевой безопасности и др.). Ручная проверка по таким методическим указаниям надежна, но трудоемка и зависит от квалификации проверяющего. Человеческий фактор может привести к пропуску ошибки или неверной интерпретации требований. Таким образом, автоматизация проверки настроек выглядит весьма актуальной.

Анализ показал, что ни одно из существующих решений полностью не удовлетворяет потребности в обнаружении специфических ошибок конфигурации механизмов защиты Astra Linux. Универсальные инструменты (SCAP, Lynis) охватывают лишь часть проблем и не учитывают особенностей отечественной ОС специального назначения. Коммерческие сканеры, хоть и обещают глубокий анализ, недоступны широкой аудитории и непрозрачны в работе. Налицо пробел, который целесообразно заполнить путем разработки специализированного программного обеспечения, способного автоматически проверять конфигурацию Astra Linux на наличие типовых ошибок, описанных ранее. Такое ПО должно учитывать архитектуру безопасности Astra Linux, включая мандатное разграничение доступа, МКЦ, PAM и другие компоненты, и предоставлять администратору понятные отчёты с указанием обнаруженных несоответствий и рекомендациями по исправлению.

В рамках первой главы проведено исследование современных механизмов обеспечения безопасности в ОС Astra Linux и проблем, возникающих при их неправильной настройке. Были рассмотрены принципы работы дискреционного и мандатного контроля доступа, системы целостности и аудита, а также идентификации и аутентификации, показана их роль в общей защите информации. На основе обзора практики эксплуатации выполнена классификация распространённых ошибок конфигурации, охватывающая различные аспекты – от управления правами доступа до настройки сетевых фильтров. Проанализированы существующие инструменты выявления ошибок настройки и уязвимостей: как открытые утилиты (SCAP/OpenSCAP, Lynis), так и интегрированные или коммерческие решения. Установлено, что на данный момент отсутствует открытое специализированное средство,

полностью удовлетворяющее задачам проверки конфигурации Astra Linux с учётом всех её особенностей. Таким образом, проделанная работа является первым этапом комплексного исследования. По результатам данного этапа в дальнейшем планируется разработка и внедрение собственного программного обеспечения для автоматизированного выявления ошибок конфигурации механизмов защиты информации и прав доступа в Astra Linux. Реализация такого инструмента призвана повысить надёжность и безопасность информационных систем за счёт своевременного обнаружения и устранения неправильных настроек до того, как ими смогут воспользоваться нарушители.

Список литературы:

1. Операционная система специального назначения Astra Linux Special Edition. Руководство по комплексу средств защиты информации. Часть 1: руководство администратора безопасности (РУСБ.10015-01 97 01-1) [Текст]. – М.: НПО РусБИТех, 2020. – 184 с.

2. ГОСТ Р 58256-2018. Защита информации. Технология защиты информации в компьютерных сетях на основе протокола IP [Текст]. – М.: Стандартинформ, 2018. – 47 с.

3. Методические рекомендации по обеспечению безопасности информации в ОС Astra Linux Special Edition. – М.: НПО РусБИТех, 2023. – 85 с. (Согласовано ФСТЭК России 31.01.2024).