УСЛОВИЯ ЭКСПЛУАТАЦИИ

УСЛОВИЯ ПРИМЕНЕНИЯ ИЗДЕЛИЯ

требования изложены в п. 4.1 документа РУСБ.10015-16 30 01 «Операционная система специального назначения «Astra Linux Special Edition». Формуляр» (далее – ФО)

- допускается использование изделия в качестве СЗИ от НСД класса Б1. При использовании изделия в качестве СЗИ от НСД класса А1 необходимо провести дополнительные тематические исследования на соответствие требованиям специального технического задания, согласованного экспертной организацией;
- должны выполняться требования документов: РУСБ.10015-16 31 01 и РУСБ.10015-16 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition. Руководство по КСЗ. Часть 1»;
- при необходимости обработки информации, содержащей сведения, составляющие ГТ, изделие должно функционировать на аппаратных средствах, прошедших тематические исследования BIOS и специальные исследования и проверки установленным порядком, в соответствии с требованиями предписания на эксплуатацию;
- проверка целостности ядра ОС и других компонентов при загрузке/перезагрузке должна осуществляться путем применения внешних по отношению к изделию средств, прошедших тематические исследования установленным порядком;
- не допускается использование изделия в АС ЗИ, подключаемых к сетям общего пользования, без проведения дополнительных тематических исследований;
- ПО, находящееся на DVD-дисках РУСБ.10015-16 12 01-2 «Операционная система специального назначения «Astra Linux Special Edition. Текст программы. Загрузочный модуль. Исполнение 1. Часть 2. Средства разработки» и РУСБ.10015-16 12 02-2 «Операционная система специального назначения «Astra Linux Special Edition. Текст программы. Загрузочный модуль. Исполнение 2. Часть 2. Средства разработки», не может использоваться в АС ЗИ без проведения дополнительных тематических исследований;
- для создания защищённой среды виртуализации изделие должно применяться совместно с аппаратным обеспечением, поддерживающим соответствующие технологии VT/SVM, в том числе при необходимости предоставления доступа виртуальным машинам к физическим устройствам.

УСЛОВИЯ ПРИМЕНЕНИЯ ПО, ОБРАЗУЮЩЕГО СОВМЕСТНО С ИЗДЕЛИЕМ ДОВЕРЕННУЮ ПРОГРАММНУЮ СРЕДУ

требования изложены в п. 4.2 ФО

- необходимость и корректность использования в ПО привилегий суперпользователя root, прикладного программного интерфейса подсистемы безопасности PARSEC, мандатных привилегий, функционирования в пространстве ядра или только на высоком уровне механизма мандатного контроля целостности должны быть обоснованы в рамках соответствующих тематических исследований;

- ПО, использующее интерпретаторы из состава изделия, должно пройти тематические исследованиям совместно с ними.

требования изложены в 17.3 Руководство по КСЗ. Часть 1

- для ПО, функционирующего от имени суперпользователя root, должна быть обоснована необходимость и корректность использования привилегий суперпользователя;
- ПО, использующее интерпретаторы PHP, Perl, Python, TCL из состава изделия,должно пройти сертификационные исследования совместно с ними. При проведении таких сертификационных исследований должен быть определен перечень сценариев ПО, исполняемых интерпретаторами, зафиксированы их контрольные суммы и определен регламент контроля их целостности;
- ПО при обработке запросов пользователей не должно взаимодействовать с защищенной СУБД из состава изделия от имени пользователя с привилегиями PARSEC_CAP_SETMAC и PARSEC_CAP_CHMAC, позволяющими изменять мандатные атрибуты защищаемых объектов в СУБД;
- ПО, содержащее сетевые сервисы (программы, обрабатывающие запросы пользователей с применением протоколов стека TCP/IP), которые используют привилегии (PARSEC_CAP_SETMAC и PARSEC_CAP_PRIV_SOCK) и прикладной программный интерфейс подсистемы безопасности PARSEC из состава изделия, должно пройти сертификационные исследования, подтверждающие корректность реализации указанных сервисов;
- программный компонент RabbitMQ не применять при одновременной обработке данных с различными уровнями конфиденциальности либо для обеспечения взаимодействия процессов с различными уровнями доступа;
- модуль wsgi_mod для Apache не применять при включенном режиме AstraMode (см. РУСБ.10015-16 95 01-1);
- ПО, обрабатывающее одновременно данные с различными уровнями конфиденциальности, не должно использовать программные пакеты Erlang.

ПО, ОБРАЗУЮЩЕЕ СОВМЕСТНО С ИЗДЕЛИЕМ ДОВЕРЕННУЮ ПРОГРАММНУЮ СРЕДУ, НЕ ДОЛЖНО ИЗМЕНЯТЬ АЛГОРИТМ ПРИНЯТИЯ РЕШЕНИЯ О ПРЕДОСТАВЛЕНИИ ДОСТУПА СУБЪЕКТОВ (ПОЛЬЗОВАТЕЛЕЙ) К ОБЪЕКТАМ ОС И СОДЕРЖАТЬ СКРЫТЫХ ИЛИ ЯВНЫХ ВОЗМОЖНОСТЕЙ (БЕЗ СООТВЕТСТВУЮЩЕГО ОБОСНОВАНИЯ), ПОЗВОЛЯЮЩИХ:

требования изложены в п. 4.3 ФО

- подменять файлы образа ядра vmlinuz-*, находящиеся в директории /boot, файлы модулей ядра, находящиеся в директории /lib/modules, и прочие файлы, входящие в состав изделия или стороннего ПО;
- статически или динамически изменять таблицу системных вызовов и поляструктуры типа security_operations и иных структур типа *security*;
- переопределять основной процесс ОС в конфигурационномфайле загрузчика изделия путем установки параметра init=<полный_путь_к_исполняемому_файлу>;
- изменять параметры аутентификации пользователей в конфигурационных файлах PAM-сценариев, находящихся в каталоге /etc/pam.d;
- устанавливать подгружаемые модули аутентификации (PAM-модули), определяющие мандатные атрибуты сессии пользователя с использованием функций API подсистемы безопасности PARSEC;
- устанавливать PAM-модули, определяющие привилегии PARSEC сессии пользователя с использованием функций API подсистемы безопасности PARSEC;
- устанавливать серверы печати, позволяющие осуществить вывод на печать документов в обход защищенного сервера печати из состава изделия;
- получать доступ к памяти других процессов ПО;
- изменять системное время;
- динамически изменять сегмент кода и системные переменные ядра ОС, а также использовать неэкспортируемые символы ядра ОС;
- осуществлять доступ к файлу ctl файловой системы parsecfs посредством системного вызова ioctl, минуя системные функции API-библиотек libparsec-*.

требования изложены в 17.3 Руководство по КСЗ. Часть 1

- подменять образы ядра изделия vmlinuz-*, находящиеся в каталоге /boot корневой файловой системы;
- статически или динамически изменять таблицу системных вызовов и поля структуры типа security_operations и иных структур типа *security*;
- переопределять основной процесс ОС в конфигурационном файле загрузчика изделия путем установки параметра init=<полный_путь_к_исполняемому_файлу>;
- изменять параметры аутентификации пользователей в конфигурационных файлах PAM-сценариев, находящихся в каталоге /etc/pam.d;
- устанавливать подгружаемые модули аутентификации (PAM-модули), определяющие мандатные атрибуты сессии пользователя с использованием функций API библиотеки libparsec-mac подсистемы безопасности PARSEC, имена которых начинаются с префиксов mac_set_, parsec_ или pdp_;
- устанавливать PAM-модули, определяющие привилегии PARSEC сессии пользователя с использованием функций API библиотеки libparsec-cap подсистемы безопасности PARSEC, имена которых начинаются с префиксов mcap или parsec_;
- устанавливать серверы печати, позволяющие осуществить вывод на печать документов в обход защищенного сервера печати из состава изделия;
- устанавливать интерпретаторы команд, заменяющие интерпретаторы, входящие в состав изделия (bash, dash, PHP, Perl, Python, TCL);
- получать доступ к памяти других процессов ПО с использованием привилегии CAP_SYS_PTRACE и системного вызова ptrace;

- изменять системное время (если наличие возможностей по изменению времени не предусмотрено функциональным назначением ПО);
- динамически изменять сегмент кода ядра ОС и использовать неэкспортируемые символы ядра ОС;
- осуществлять доступ к файлу ctl файловой системы parsecfs посредством системного вызова ioctl, минуя системные функции API-библиотек libparsec-*.

УКАЗАНИЯ ПО ПОДГОТОВКЕ И ПРОВЕДЕНИЮ ОЦЕНКИ ПО ПРИВЕДЕНЫ В ДОКУМЕНТЕ «МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОЦЕНКЕ ВЛИЯНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ФУНКЦИОНИРОВАНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОПЕРАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION». (требования изложены в п. 4.4 ФО)

ДОПОЛНИТЕЛЬНЫЕ УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ ИЗДЕЛИЯ В СОСТАВЕ АС ЗИ
требования изложены в соотвествующих разделах документов РУСБ.10015-16 95 01-1 и РУСБ.10015-16 95 01-2 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора» (далее – РА)

- с помощью организационно-режимных или технических мер должна быть ограничена установка ПО, не входящего в состав АС ЗИ (раздел 1 РА часть 1)
- организационно-режимные меры защиты информации, обрабатываемой в ОС, должны вклю-чать в себя регламент обращения с носителями информации ОС как с носителями соответствующей степени секретности (раздел 1 РА часть 1)
- состав ПО, устанавливаемого на СВТ АС ЗИ помимо ОС, должен определяться главным конструктором (предприятием-разработчиком) АС ЗИ по согласованию с экспертной организацией(в/ч 43753) (раздел 1 РА часть 1)
- в эксплуатационной документации на АС ЗИ должен быть определен порядок действий администратора АС ЗИ при обнаружении попыток несанкционированного доступа (раздел 1 РА часть 1)
- должен быть установлен порог на число следующих подряд неудачных попыток предъявления аутентифицирующей информации от одного пользователя посредством установки в конфигурационном файле/etc/pam.d/common-auth в строке для PAM-модуля pam_tally.so значения для параметра deny. Данное значение должно составлять не более 8 (раздел 1 РА часть 1)
- при настройке подсистемы тестирования комплекса средств защиты администратору ОС необходимо настроить занесение в регистрационный протокол информации об удачном/неудачном прохождении тестов (раздел 1 РА часть 1)
- непосредственно перед выполнением процедуры тестирования комплекса средств защиты ОС необходимо осуществлять контроль целостности всего набора тестовых утилит (используемых скриптов и бинарных файлов) (раздел 1 РА часть 1)
- при использовании разделов подкачки в ОС необходимо активировать в файле/etc/parsec/swap_wiper.conf их очистку (раздел 1 РА часть 1)
- в эксплуатационной документации на АС ЗИ должен быть определен согласованный с экспертной организацией порядок генерации паролей пользователей (раздел 1 РА часть 1)

- в эксплуатационной документации на АС ЗИ должна быть установлена периодичность смены паролей пользователей (раздел 1 РА часть 1)
- до загрузки СВТ должен проводиться контроль целостности изделия (в соответствии со списком, приведенным в РУСБ.10015-16 97 01-1 «Операционная система специального назначения«Astra Linux Special Edition. Руководство по КСЗ. Часть 1») и ПО, установленного на СВТ АС ЗИ помимо ОС (раздел 1 РА часть 1)
- в эксплуатационной документации на АС ЗИ должен быть определен регламент контроля целостности файлов данных (конфигурационных файлов) встроенными средствами ОС (в соответствии со списком, приведенным в РУСБ.10015-16 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition. Руководство по КСЗ. Часть 1») (раздел 1 РА часть 1)
- в эксплуатационной документации на АС ЗИ должен быть определен порядок действий администратора АС ЗИ по полной очистке регистрационных протоколов и автоматической регистрации факта очистки с указанием даты, времени и информации о лице, производившем операцию(раздел 1 РА часть 1)
- в эксплуатационной документации на АС ЗИ должны быть определены: регламент проведения тестов, описанных в РУСБ.10015-16 97 01-2 «Операционная система специального назначения «Astra Linux Special Edition. Руководство по КСЗ. Часть 2», и действия администратора при обнаружении неисправностей (раздел 1 РА часть 1)
- в эксплуатационной документации на АС ЗИ должен быть определен порядок использования тестов, описанных в РУСБ.10015-16 97 01-2 «Операционная система специального назначения«Astra Linux Special Edition. Руководство по КСЗ. Часть 2», для самоконтроля системы защиты от НСД АС ЗИ и ее самоблокирования посредством завершения работы всех сетевых сервисов, предоставляющих удаленный вход в систему, и создания файла /etc/nologin, предотвращающего локальный вход в систему (файл может содержать описание причины блокировки системы) (раздел 1 РА часть 1)
- процедура самоконтроля ОС должна осуществляться не реже двух раз в сутки (раздел 1 РА часть 1)
- должен быть указан в эксплуатационных документах АС ЗИ порядок использования загрузчика(раздел 1 РА часть 1)
- в качестве файловых систем на носителях информации компьютеров с ОС должны использоваться только файловые системы Ext2 и Ext3, поддерживающие расширенные (в т.ч. мандатные) атрибуты пользователей (п. 3.3.1 РА часть 1)
- монтирование сетевых дисков в файловую систему ОС должно осуществляться только с использованием файловой системы CIFS, поддерживающей расширенные (в т.ч. мандатные) атрибуты пользователей (п. 3.3.2 РА часть 1)
- в конфигурационном файле защищенного сервера печати из состава изделия/etc/cups/cupsd.conf не допускается установка значения None параметра DefaultAuthType (отключение аутентификации) и внесение изменений в параметры политики PARSEC, не соответствующих эксплуатационной документации(п.11.3.1 РА часть 1)
- при использовании защищенного сервера СУБД из состава ОС в режиме мандатного разграничения доступа необходимо в конфигурационном файле кластера postgresql.conf для параметра enable_bitmapscan установить значение

off и для параметра ac_ignore_socket_maclabel установить значение false (п.1.3 РА часть 2)

- при использовании защищенного сервера СУБД из состава ОС в режиме мандатного управления доступом не допускается отключать аутентификацию субъектов доступа установкой в конфигурационном файле кластера pg_hba.conf режима trust (без аутентификации) (п. 9 Описание защищённой СУБД)
- при использовании защищенного комплекса программ электронной почты из состава ОС в режиме мандатного разграничения доступа конфигурационные параметры агента передачи электронной почты Exim и агента доставки электронной почты Dovecot не должны допускать отправку и прием сообщений электронной почты без аутентификации (п.13.2 РА часть 1)
- при использовании Astra Linux Directory не допускается внесение изменений в параметры монтирования домашних каталогов пользователей, устанавливаемые в конфигурационном файле/etc/security/pam_mount.conf.xml (п. 7.2.3 РА часть 1)
- не допускается отключение расширения XPARSEC посредством запуска X-сервера с ключом -extension XPARSEC=Disable или установкой значения Disable для опции XPARSEC в конфигурационных файлах X-сервера (п. 8 РА часть 1)