Согласовано ФСТЭК России
от 31.01.2024 г.

Методические рекомендации по исключению влияния на функции безопасности операционной системы специального назначения «Astra Linux Special Edition» при проектировании, разработке и эксплуатации программного обеспечения

(Листов - 8)

Москва
2023

СОДЕРЖАНИЕ

АННОТАЦИЯ

Настоящий документ предназначен для разработчиков программного обеспечения (далее – ПО), средой функционирования которого является операционная система специального назначения «Astra Linux Special Edition» (далее – ОС), и администраторов информационных (автоматизированных) систем, обрабатывающих информацию ограниченного доступа, функционирующих под управлением ОС.

Настоящий документ содержит требования и методические рекомендации, которые необходимо учитывать при проектировании, разработке и эксплуатации ПО в целях исключения влияния на сертифицированные функции безопасности и характеристики ОС.

Изготовитель ОС: Общество с ограниченной ответственностью «РусБИТех-Астра».

1. ОБЩИЕ ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

1.1. ПО не должно нарушать условия эксплуатации ОС, приведенные в эксплуатационной документации ОС.

1.2. ПО должно соответствовать условиям применения ПО, приведенным в эксплуатационной документации.

1.3. ПО не должно заменять или модифицировать компоненты ОС, реализующие функции безопасности.

При необходимости, замена или модификация функций безопасности ОС может допускаться только при соблюдении всех нижеприведенных условий:

– изготовитель ОС допускает при штатной работе ОС отключение соответствующего компонента без влияния на остальные функции безопасности;

– изготовитель ОС допускает подобную замену/модификацию в эксплуатационной документации на ОС или официально подтверждает возможность такой замены с отсутствием влияния на остальные функции безопасности.

– ПО, заменяющее компонент, используемое для реализации мер защиты в информационной системе, должно быть сертифицировано на соответствие требованиям по безопасности информации.

1.4. ПО не должно вносить изменения в алгоритмы принятия решений функций безопасности ОС, описанные в эксплуатационной документации.

1.5. Взаимодействие с функциями безопасности ОС должно осуществляться в соответствии с рекомендациями изготовителя ОС, приведенными в документации на ОС и/или рекомендациях, предназначенных для разработчиков ПО.

2. УСЛОВИЯ ИСКЛЮЧЕНИЯ ВЛИЯНИЯ НА ФУНКЦИИ БЕЗОПАСНОСТИ ОС

2.1. Условия использования привилегий

2.1.1. ПО должно использовать минимально необходимые для функционирования права пользователей, функции и привилегии ядра ОС и подсистемы безопасности.

2.1.2. К привилегиям ПО, влияющим на функции безопасности ОС, относятся:

– использование прав суперпользователя и функционирование от имени суперпользователя;

– использование прав высокоцелостного администратора;

– возможность повышения собственных привилегий и привилегий других программ;

– внесение изменений в права доступа субъектов к объектам доступа;

– использование установленных флагов доступа SUID/SGID;

– запуск процессов с использованием специальных привилегий;

– установка специальных разрешений на файлы/каталоги;

– функционирование в пространстве ядра linux;

– использование мандатных привилегий (при наличии);

– возможность функционирования на высоких уровнях мандатного контроля целостности (при наличии).

2.1.3. В случае, если использование привилегий необходимо для корректного функционирования ПО, использование привилегий должно осуществляться в порядке, определенном изготовителем ОС (в эксплуатационной документации и методических документах (рекомендациях), предназначенных для разработчиков ПО).

2.1.4. В документации ПО должны быть приведены соответствующее обоснование указанной необходимости и описание алгоритмов и сценариев работы.

2.1.5. Необходимость, виды и объемы испытаний ПО, использующего указанные привилегии, на соответствие требованиям по безопасности информации, определяются в соответствии с действующими нормативными документами систем сертификации средств защиты информации Российской Федерации.

2.2. Исключение влияния на ядро ОС

2.2.1. ПО не должно представлять собой модуль ядра ОС.

2.2.2. ПО не должно подменять файлы образа ядра vmlinuz-*, файлы модулей ядра, находящиеся в каталоге /lib/modules, и прочие файлы, входящие в состав ОС или стороннего ПО:

– обращаться к файлам образа ядра и модулей ядра, в том числе для обновления ядра ОС и изменения загрузочной конфигурации ОС;

– нарушать целостность (вносить изменения в характеристики и контрольные суммы) файлов образа ядра и модулей ядра, а также иных файлов, не являющихся компонентами ПО и не создаваемых в процессе его использования, в ходе установки и выполнения.

2.2.3. ПО не должно динамически вносить изменения в сегмент кода ядра ОС и использовать неэкспортируемые символы ядра ОС:

– обращаться к файлам управления параметрами ядра с целью внесения изменений;

– обращаться к командам ОС, предназначенной для изменения системных переменных ядра, в том числе при установке;

– обращаться к sysctl-функциям ядра;

– обращаться к экспортируемым функциям механизма kallsyms;

– обращаться к таблице системных вызовов sys_call_table;

– вычислять адреса функций, предназначенных для обработки системных вызовов и выделения памяти в пространстве ядра.

2.2.4. В случае, если для корректного функционирования ПО необходимо:

– функционировать в пространстве ядра;

– загружать исполняемый код в пространство ядра;

– обращаться к командам, предназначенным для управления модулями ядра, в том числе при установке;

в документации ПО должны быть приведены соответствующее обоснование указанной необходимости и описание алгоритмов и сценариев работы.

2.3. Исключение влияния на загрузку ОС

2.3.1. ПО не должно переопределять основной процесс ОС в конфигурационном файле загрузчика путем установки параметра init=<полный_путь_к_исполняемому_файлу>;

2.3.2. ПО не должно подменять файлы образов временной файловой системы начальной загрузки /boot/initrd.img-*, находящиеся в каталоге /boot. В случае явной необходимости обновления отдельных компонентов, входящих в состав образа, должны быть выполнены действия, предусмотренные п. 3 раздела «Общие требования к программному обеспечению» и п.2.1 настоящего раздела.

2.4. Исключение влияния на подсистемы безопасности ОС

2.4.1. Вызов функций, входящих в подсистему безопасности ОС, должен осуществляться в соответствии с рекомендациями изготовителя ОС, приведенными в документации на ОС и/или методических документах (рекомендациях), предназначенных для разработчиков ПО).

2.4.2. ПО не должно содержать скрытых или явных возможностей, позволяющих:

а) статически или динамически вносить изменения в таблицу системных вызовов и поля структуры типа security_operations и иных структур типа *security*;

б) вносить изменения в параметры аутентификации в конфигурационных файлах PAM-сценариев, находящихся в директории /etc/pam.d, устанавливать подгружаемые модули аутентификации (PAM-модули), определяющие атрибуты и привилегии сессии пользователя:

– обращаться к файлу /etc/pam.conf и файлов, расположенных в директории /etc/pam.d;

– нарушать целостность (вносить изменения в характеристики и контрольные суммы) файла /etc/pam.conf и файлов, расположенных в директории /etc/pam.d, в ходе установки и выполнения;

в) получать доступ к памяти других процессов ПО;

г) обращаться к памяти процесса с использованием привилегии CAP_SYS_PTRACE и системного вызова ptrace;

д) вносить изменения в системное время;

е) заменять интерпретаторы из состава ОС.

2.4.3. Сборка ПО не должна осуществляться совместно со сборкой ядра ОС.

2.4.4. Использование в ПО (при необходимости) механизмов идентификации/аутентификации пользователей должно осуществляться в соответствии с рекомендациями изготовителя ОС, приведенными в документации на ОС и/или методических документах (рекомендациях), предназначенных для разработчиков ПО).

3. УСЛОВИЯ ИСКЛЮЧЕНИЯ ПОТЕНЦИАЛЬНО-ОПАСНЫХ АЛГОРИТМОВ ПО

3.1. ПО не должно осуществлять передачу управления в область данных:

– ПО не должно вносить изменения в параметры защиты страниц памяти, в том числе с помощью системных вызовов.

3.2. ПО не должно осуществлять самоидентификацию или изменение кода или данных других программ в оперативной памяти и на внешних носителях:

– ПО не должно содержать возможности по открытию на запись файлов компонентов ПО;

– ПО не должно обращаться к файлам устройств, представляющих собой отображение содержимого оперативной памяти или носителя информации;

– ПО не должно содержать возможности по присоединению файловых систем к файловой системе ОС и содержать описания прикладного программного интерфейса библиотек функций, реализующих функциональные возможности присоединения файловых систем к файловой системе ОС;

– ПО не должно обращаться к файлам, расположенным в файловых системах типа proc в поддиректориях с именами, соответствующими идентификаторам выполняемых процессов.

3.3. ПО не должно осуществлять самодублирование и подменять собой другие программы или переносить свои фрагменты в области оперативной и внешней памяти, не принадлежащие ему.

3.4. ПО не должно иметь доступ к областям оперативной памяти, не принадлежащих ему.

3.5. ПО не должно скрывать свое присутствие в программной среде:

– процессы, порождаемые при выполнении исполняемых файлов ПО, должны присутствовать в выводе стандартных утилит обзора процессов;

– состав компонентов ПО, расположенных в файловой системе, должен соответствовать составу компонентов, входящих в пакет ПО, как после установки, так и в процессе выполнения исполняемых файлов.

3.6. ПО не должно определять факт работы кода в виртуальной среде и противодействовать отладке.

3.7. ПО не должно вносить изменения в программы микроконтроллеров, в том числе BIOS, и поддерживать низкоуровневую работу с портами ввода/вывода;

3.8. При необходимости использования перечисленных алгоритмов в документации ПО должны быть приведены соответствующее обоснование указанной необходимости и описание алгоритмов и сценариев работы.