Рекомендации по разработке программного обеспечения, функционирующего в среде операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (релиз «Смоленск»)

1. Цель документа

Данный документ предназначен для разработчиков специального (прикладного) программного обеспечения (далее – ПО), предназначенного для функционирования в среде сертифицированной операционной системы специального назначения «Astra Linux Special Edition» (далее — ОС СН).

Настоящий документ содержит основные положения и рекомендации, которые необходимо учитывать при проектировании и разработке ПО в целях обеспечения его работоспособности совместно с комплексом средств защиты информации из состава ОС СН, его интеграции с механизмами защиты (функциями безопасности) ОС СН и невлияния на функции безопасности и характеристики ОС СН.

Выполнение рекомендаций настоящего документа при проектировании и разработке ПО позволит обеспечить корректное функционирование ПО в составе информационных (автоматизированных) систем, обрабатывающих любую информацию ограниченного доступа, в том числе предполагающих режим обработки информации различного уровня конфиденциальности.

При необходимости сертификации ПО в системах сертификации средств защиты информации ФСТЭК России и Министерства обороны Российской Федерации выполнение приведенных рекомендаций существенно упростит процесс его сертификации, а при отсутствии требований государственного заказчика по сертификации ПО — исключить необходимость обязательной сертификации ПО в системе сертификации средств защиты информации ФСТЭК России.

Данный документ содержит ссылки на руководящие и эксплуатационные документы разработчика ОС СН, положениями которых необходимо руководствоваться при проектировании и разработке ПО.

2. Руководящие указания по конструированию прикладного ПО

Документ «Руководящие указания по конструированию прикладного программного обеспечения для ОС СН» РУСБ.10015-01 размещен на официальном сайте разработчика ОС СН и доступен по ссылке:

https://astralinux.ru/assets/docs/RUK-OSSN-DEV_1-6.pdf.

В «Руководящих указаниях по конструированию прикладного программного обеспечения для ОС СН» (далее – РУК) приведены базовые принципы взаимодействия ПО с комплексом средств защиты (далее – КСЗ) ОС СН. В документе изложены:

– краткий обзор архитектурных особенностей ОС СН;

– рекомендации по использованию средств для разработки ПО;

– особенности разработки приложений с графическим интерфейсом, взаимодействующих с защищенным оконным менеджером Fly, включая рекомендации по разработке ПО для мобильных устройств;

– описание применения программных интерфейсов (API) средств защиты информации (подробное описание API мандатного разграничения доступа и использования API системы расширенного аудита);

– рекомендации по миграции приложений в среду ОС СН с других платформ и по интеграции других операционных систем семейства Linux с ОС СН.

3. Руководство по комплексу средств защиты. Часть1

Эксплуатационный документ «ОС СН. Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1 (далее – РУК КСЗ. Часть 1) входит в комплект поставки ОС СН, а также доступен на официальном сайте разработчика ОС СН по ссылке:

https://astralinux.ru/assets/docs/astra-linux-se/Ruk_KSZ_1__se_04-2020.pdf.

РУК КСЗ. Часть 1 содержит описание подсистем безопасности ОС СН и правила эксплуатации КСЗ ОС СН.

Разработчику ПО необходимо учитывать, что функционирование разрабатываемого ПО должно осуществляться с учетом приведенных в документе условий и ограничений по использованию, представленных в следующих разделах РУК КСЗ. Часть 1:

– в п. 17.2 и п. 17.3.1 содержится информация по настройке ОС СН перед началом ее эксплуатации и обязательных параметрах, а также условиях применения ОС СН в составе информационных (автоматизированных) систем в защищенном исполнении;

– в п. 17.3.2 приведены условия применения ПО для обеспечения и формирования совместно с ОС СН доверенной программной среды, а также ограничения, предъявляемые к ПО в целях исключения его возможного влияния на функционирование КСЗ ОС СН.

4. Рекомендации по построению ПО

Документ «Рекомендации по построению прикладного программного обеспечения для интеграции с механизмами идентификации, аутентификации, авторизации и разграничения доступа ОС СН» размещен на официальном сайте разработчика ОС СН и доступен по ссылке:

https://nas01.astralinux.ru/sharing/n62RYHgK7.

Документ содержит следующие сведения:

– особенности функционирования ПО в составе локальных и территориально-распределенных информационных (автоматизированных) систем;

– типичные ошибки, допускаемые разработчиками ПО при организации архитектурной модели трехзвенной архитектуры;

– преимущества обеспечения взаимодействия и интеграции ПО с КСЗ ОС СН;

– недостатки реализации в ПО собственных механизмов защиты информации (функций безопасности)[1] в целях реализации мер защиты информации в информационной (автоматизированной) системе;

– рекомендации по разработке сервера приложений с использованием программного интерфейса API SASL и механизмов взаимодействия с КСЗ ОС СН, предоставляющих сведения о текущем уровне доступа пользователя (процесса) из сетевой подсистемы ОС СН, что позволяет сохранить неизменным контекст безопасности работы пользователя в рамках информационной системы.

1 Настоящий пункт относится только к прикладному программному обеспечению, предназначенному для реализации специальных (прикладных) функциональных задач. Не относится к средствам защиты информации, нормативными документами для которых определены собственные функции безопасности (например, средства антивирусной защиты, межсетевые экраны и проч.)

Рекомендации по разработке сервера приложений содержат ссылку на документ «API аутентификации приложений SASL в Astra Linux», доступный на официальном сайте разработчика ОС СН:

https://nas01.astralinux.ru/sharing/yX3tRc1sF.

В документе приводится краткое описание библиотеки SASL, поддерживаемых библиотекой механизмов аутентификации и протоколах передачи данных, примеры программного интерфейса клиентского и серверного приложений.

5. Контрольный пример

Для практического изучения приведенных рекомендаций по построению прикладного ПО был разработан контрольный пример, который демонстрирует:

– принципы взаимодействия компонентов ПО трехзвенной клиент-серверной архитектуры с использованием встроенных механизмов защиты информации (КСЗ) ОС СН;

– работу пользователя в определенном ему при входе в систему контексте безопасности со всеми компонентами системы (приложением, сервером приложений и сервером баз данных) без необходимости дополнительной аутентификации и идентификации, в том числе в СУБД;

– механизмы разграничения доступа в СУБД PostgreSQL.

В качестве сервера приложений в контрольном примере используется Web-сервер Apache, сервера баз данных – СУБД PostgreSQL из состава ОС СН. Обращения к серверу приложений осуществляется из Web-браузера, функционирующего в среде ОС СН.

Подробное описание контрольного примера доступно по ссылке:

https://nas01.astralinux.ru/sharing/29GxqKNwd

6. Условия применения средств разработки

При проектировании, выборе архитектуры и технологий разработки ПО, предназначенного для функционирования в среде ОС СН и (особенно) подлежащего сертификации на соответствие требованиям безопасности информации, важно руководствоваться условиями применения различных средств разработки ПО, приведенными в таблице 6.1.

Под средствами разработки подразумевается набор инструментальных программ (программные платформы, прикладные/системные библиотеки, утилиты, среды разработки, интерпретаторы, компиляторы и т.д.), используемых разработчиком для создания программного кода.

ВАЖНО!

При применении любых средств необходимо соблюдать условия применения ПО для обеспечения и формирования совместно с ОС СН доверенной программной среды, а также ограничения, предъявляемые к ПО в целях исключения его возможного влияния на функционирование КСЗ ОС СН, указанных в п.17.3.2 эксплуатационного документа «ОС СН. Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1.

При этом включать в состав установочного диска ПО средства разработки (сборки) и отладки программ не рекомендуется, т.к. это может привести к невозможности использования ПО в системах, обрабатывающих информацию ограниченного доступа, и противоречит требованиям нормативных документов по защите информации к информационным (автоматизированным) системам.

В соответствии с требованиями руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992 г.) включение в состав установочного диска ПО средств разработки (сборки) и отладки программ и использование таких средств в составе информационных (автоматизированных) систем запрещено.

Таблица 6.1

№	Источник средств разработки	Тип средств	Условия и особенности применения	Дополнительные условия
1.	ОС СН Установочный диск	Средства из состава КСЗ ОС СН	К КСЗ ОС СН относятся средства, размещенные на установочном диске и реализующие функции безопасности, а также поддерживающие их или взаимодействующие с ними. Указанные средства и порядок их настройки приведены в эксплуатационной документации ОС СН (Руководстве по КСЗ, Руководстве администратора). Рекомендуется к использованию в приоритетном порядке. Устанавливаются в систему с установочного диска. Все используемые средства из состава КСЗ ОС СН и порядок взаимодействия с ними ПО должны быть описаны в эксплуатационной документации ПО.	
2.		Иные программные средства	К иным средствам относятся средства, размещенные на установочном диске, не реализующие функции защиты и не входящие в состав КСЗ ОС СН. Использование данных средств рекомендуется при разработке ПО. Устанавливаются в систему с установочного диска. В документации на ПО разработчик ПО должен указать сведения о необходимости наличия (установки) этих средств в информационную систему для обеспечения функционирования ПО.	1
3.	ОС СН Диск со средствами разработки		Средства разработки, размещенные на отдельном диске из комплектности поставки ОС СН. Использование данных средств рекомендуется при разработке ПО. Для использования указанных средств при сборке или в целях обеспечения функционирования ПО необходимо официально получить (приобрести) диск со средствами разработки ОС СН, включить его в спецификацию на ПО, при этом в Руководстве по сборке (или ином документе, в котором приведен порядок сборки ПО) указывать, конкретные наименования используемых средств, их контрольные суммы и порядок их копирования и применения при	1,2

№	Источник средств разработки	Тип средств	Условия и особенности применения	Дополнительные условия
			сборке (компиляции) ПО.	
4.	Средства с открытым исходным кодом	Средства с открытым исходным кодом, не реализующие функции безопасности	Применение средств с открытым исходным кодом возможно. На этапе проектирования необходимо проверить их работоспособность и целесообразность применения в составе ПО. Для обеспечения дальнейшей сертификации ПО исходные тексты должны быть включены в исходные тексты ПО, проведена их компиляция («сборка») в составе ПО, получен установочный диск. При этом, если в ходе эксплуатации ПО в указанных средствах будут обнаружены уязвимости, разработчик ПО должен устранять их самостоятельно в соответствии с условиями систем сертификации средств защиты информации МО РФ и ФСТЭК России.	1, 2, 3, 4
5.		Средства с открытым исходным кодом, реализующие функции безопасности	Применение средств с открытым исходным кодом, реализующих функции безопасности, является основанием для проведения обязательной сертификации и должно быть согласовано с подразделением по защите информации. В таком случае необходимо оценить целесообразность применения таких средств, возможности их сертификации в соответствии с требованиями актуальных документов по безопасности информации. При этом необходимо учитывать дополнительные организационные, временные и финансовые затраты на сертификацию ПО. Применение таких средств не рекомендуется.	1, 3, 4
6.		Средства с открытым исходным кодом, реализующие механизмы выполнения (интерпретации) программного кода (Runtime)	Применение таких средств является основанием для проведения обязательной сертификации и должно быть согласовано с подразделением по защите информации. В таком случае необходимо оценить целесообразность применения указанных средств, возможности их сертификации в соответствии с требованиями актуальных документов по безопасности информации. При этом необходимо учитывать дополнительные организационные, временные и финансовые затраты на сертификацию ПО. Применение таких средств не рекомендуется.	1, 3, 4
7.	Проприетарные	Средства,	В состав ПО включаются как покупные составные части.	1,4

№	Источник средств разработки	Тип средств	Условия и особенности применения	Дополнительные условия
	средства	предоставляемые правообладателями на основании лицензионных соглашений	Если ПО подлежит сертификации по требованиям безопасности информации, то такие покупные составные части должны иметь собственный сертификат соответствия и/или должен быть проведен анализ возможности сертификации ПО с составными частями. Проприетарные средства не рекомендуется включать в состав ПО без наличия сертификата на них, а использовать только как среду разработки с обязательным наличием лицензионных соглашений на применение у разработчика ПО. При необходимости использования проприетарных средств для обеспечения функционирования ПО в документации на ПО разработчик должен указать сведения о необходимости наличия (установки) этих средств в информационную систему.	

Дополнительные условия.

1. На этапе проектирования разработчик должен проверить корректность работы ПО при «ненулевом» уровне конфиденциальности (если требуется поддержание работоспособности в условиях разграничения доступа к информации разных уровней конфиденциальности).
2. Если средства содержат собственные функции безопасности (например, разграничение доступа), то их необходимо классифицировать как средства с открытым исходным кодом, реализующие функции безопасности (п.5 Таблицы 6.1) и применять соответствующие правила.
3. Перед применением необходимо проверить условия использования и лицензионных соглашений на возможность использования средств с открытым исходным кодом.
4. Применяемые средства не должны конфликтовать с КСЗ ОС СН и используемыми в информационной системе средствами защиты информации.