Требования, принципы, практика создания отечественных аппаратно-программных платформ для автоматизированных систем в защищенном исполнении критической информационной инфраструктуры Российской Федерации

Михалевич И.Ф.

В работе изложена система требований и принципов, определяющих методологические аспекты создания отечественных аппаратно-программных платформ для автоматизированных систем в защищенном исполнении как основы критической информационной инфраструктуры Российской Федерации, описан опыт создания защищенной аппаратно-программной платформы «Синтез-АПП», в полном объеме удовлетворяющей самым строгим требованиям по информационной безопасности, надежности, масштабируемости, обеспечивающей независимость критической информационной инфраструктуры от зарубежных технологий и программ.

Ключевые слова: автоматизированная система в защищенном исполнении, аппаратно-программная платформа, информационная безопасность, критическая информационная инфраструктура, «Синтез-АПП»

1. Введение.

Бурное развитие информационных и телекоммуникационных технологий и систем сопровождается столь же бурным развитием технологий и средств нарушения информационной безопасности, направленных на совершение киберпреступлений и ведение кибервойн. Несанкционированное раскрытие информации, ее искажение или недоступность могут

привести к катастрофическим последствиям как для отдельных стран, так и миропорядка в целом, особенно, если эта информация касается функционирования критических инфраструктур, включающих объекты атомной и гидроэнергетики, здравоохранения, связи, оборонной промышленности, государственной власти и др. [1]. Поэтому укрепление позиций на мировой арене, построение цифровой экономики и реализация иных прорывных направлений развития страны невозможны без повышения защищенности критической информационной инфраструктуры Российской Федерации (далее – КИИРФ).

Доктриной информационной безопасности Российской Федерации [2], Стратегией развития информационного общества в Российской Федерации на 2017 - 2030 годы [3], Программой «Цифровая экономика Российской Федерации» [4] повышение защищенности КИИРФ неразрывно связано с ликвидацией зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности, повышением безопасности функционирования элементов информационной инфраструктуры, обеспечением безопасности информации, обрабатываемой в автоматизированных и информационных системах и передаваемой по сетям электросвязи, входящим в состав КИИРФ.

Принципиальной особенностью КИИРФ является то, что в ней обрабатывается информация от открытой до содержащей сведения, составляющие государственную тайну. Но и открытая информация КИИРФ должна быть надежно защищена, так как нарушение ее доступности и/или несанкционированное изменение (удаление) может повлечь критические последствия в социальной, политической, экономической и иных критически важных областях деятельности.

Данные условия существенно влияют на платформенные решения для КИИРФ, относят объекты КИИРФ к категории автоматизированных систем в защищенном исполнении, т.е. систем, реализующих информационные технологии выполнения установленных функций в соответствии с требованиями стандартов и/или иных нормативных документов по защите информации [5].

2. Методологические аспекты создания аппаратно - программных платформ для критической информационной инфраструктуры РФ

Создание аппаратно-программных платформ (далее – АПП) КИИРФ должно основываться на ключевых требованиях и принципах, обеспечивающих заданные уровни безопасности информации, информацион-

ной безопасности используемых информационных технологий и объектов КИИРФ в целом. Под безопасностью информации будем понимать состояние ее защищенности, при котором обеспечены ее конфиденциальность, доступность и целостность, а под безопасностью информационной технологии - состояние защищенности информационной технологии, при котором обеспечивается выполнение изделием, реализующим информационную технологию, предписанных функций без нарушений безопасности обрабатываемой информации [6]. По аналогии с [6] под информационной безопасностью объекта КИИРФ будем рассматривать состояние его защищенности, при котором на объекте КИИРФ обеспечивается безопасность информации и автоматизированных средств ее обработки.

С учетом положений [2] - [4], требований тактико-технических заданий на НИОКР по созданию автоматизированных систем в защищенном исполнении, отечественного опыта по обеспечению доверенной среды их функционирования [7, 8] АПП для КИИРФ должна обладать следующими основными свойствами и соответствовать следующим основным общим требованиям [9, 10]:

• полноценность – свойство, отражающее полноту состава и технологий платформы, обеспечивающих создание (модернизацию) и функционирование объектов КИИРФ различного назначения, разных классов защищенности, уровней топологической и архитектурной сложности;

• технологическая независимость и независимость от импорта (импортонезависимость) – свойство платформы сохранять полноценность, заявленные характеристики, развиваться, поддерживаться независимо от внешнеполитических и внешнеэкономических факторов, без применения импортных компонентов, без иностранного участия, принудительного обновления компонентов и управления из-за рубежа, передачи информации, в том числе технологической, за пределы РФ;

• промышленный уровень – свойство платформы сохранять производительность, отказоустойчивость и другие заявленные характеристики объектов КИИРФ при сложных топологии и архитектуре, высоких нагрузках и больших объемах данных в течение всего срока эксплуатации;

• универсальность - свойство платформы обеспечивать на основе собственных базовых компонентов создание (модернизацию) сегментов (объектов) КИИРФ различного назначения, разных классов защищенности и уровней топологической и архитектурной сложности;

• гарантии развития и поддержки – свойство платформы развиваться и обеспечивать эксплуатацию, обслуживание и модернизацию созданных на ее основе объектов КИИРФ.

К основным функциональным требованиям к АПП можно отнести следующие. Платформой, в частности:

• должно обеспечиваться создание (модернизация) и эксплуатация объектов КИИРФ разных классов защищенности, безопасное ведомственное, межведомственное, корпоративное взаимодействие объектов КИИРФ и их взаимодействие с зарегистрированными пользователями;

• должна создаваться защищенная (доверенная) среда функционирования специального программного обеспечения (далее – СПО), разработанного для конкретного сектора (сегмента и т.п.) критической инфраструктуры, обеспечиваться безопасность информации, исходя из класса защищенности объекта КИИРФ;

• должно обеспечиваться условие «мягкой» поэтапной модернизации объектов КИИРФ, предполагающее их функционирование при замене средств вычислительной техники и иного оборудования на новое;

• должно обеспечиваться условие «мягкой» поэтапной модернизации СПО, предполагающее использование СПО, ранее введенного в эксплуатацию;

• должны обеспечиваться организация производительного, устойчивого, масштабируемого вычислительного процесса, надежного хранения больших объемов информации, сохранение ее конфиденциальности, доступности и целостности;

• должна обеспечиваться поддержка основных сетевых служб системного и пользовательского уровней;

• должны обеспечиваться сбор, обработка и хранение данных в территориально распределенных сегментах КИИРФ, возможность безопасного удаленного доступа к этим данным (в установленном порядке), поддержка технологий интеграции вычислительных ресурсов и систем хранения данных, строительство (модернизация) и эксплуатация центров обработки данных;

• должна обеспечиваться поддержка многоуровневости и одновременной работы множества пользователей с одними и теми же данными баз (банков) данных, публикация, поиск, доступ к данным, управление контентом, резервирование и архивирование данных, синхронизация обновлений;

• должен обеспечиваться контроль и управление функционированием всех устройств, комплексов средств автоматизации (информатизации), программно-технических комплексов и т.п., входящих в состав объектов КИИРФ;

• должно обеспечиваться резервирование основных компонент объектов КИИРФ и содержащейся в них информации (данных);

• должна поддерживаться работа комплексов информационно-расчётных, аналитических, прогнозных задач, в том числе с применением Web-технологий обработки геопространственных данных и многоэкранного режима, текстовых, графических редакторов, обработка мультимедийной информации;

• должна поддерживаться доверенная среда разработки СПО.

К основным принципам, которые должны соблюдаться при создании отечественных АПП для КИИРФ, можно отнести следующие:

1. Принцип унификации программного обеспечения.

Проектирование программного обеспечения должно осуществляться таким образом, чтобы в структуре программ схожего назначения максимально применялись заранее учтенные (проверенные) функциональные модули (пакеты и т.п.).

2. Принцип локализации заимствованных программ (модулей, пакетов).

Заимствованные программные средства должны быть локализованы. Под локализацией понимается:

проверки отдельных модулей (пакетов) и программного обеспечения в целом на соответствие функциональному назначению, отсутствие недекларированных возможностей, совместимость с применяемыми в платформе и на объектах КИИРФ средствами защиты информации, невлияние на функционирование средств защиты информации;

доработки и иные мероприятия по приведению программного обеспечения в соответствие с требованиями национальных стандартов и нормативных документов российских регуляторов в сфере информационных технологий и информационной безопасности;

фиксация состояния локализованного программного обеспечения;

оформление программной, технической проектной, рабочей, конструкторской и эксплуатационной документации на локализованное программное обеспечение;

подготовка специалистов и техническая поддержка.

3. Принцип типизации технических решений.

Комбинированием компонент платформы должно обеспечиваться создание типовых технических решений (типовых конфигураций) для объектов КИИРФ различного назначения, разных классов защищенности и уровней топологической и архитектурной сложности.

4. Принцип масштабируемости.

Платформой должны обеспечиваться масштабируемость технических решений, их комплексирование в типовые конфигурации объектов КИИРФ. Платформа не должна быть чувствительной к топологической и архитектурной сложности объектов КИИРФ, численности пользователей, объемам обрабатываемой информации.

5. Принцип универсальности программных средств защиты информации.

Платформой должна обеспечиваться возможность изменения класса защищенности объекта КИИРФ путем изменения настроек программных средств защиты информации без их замены.

6. Принцип оптимизации ресурсов (кастомизации).

Платформой должна обеспечиваться возможность комбинирования технических решений и изменения настроек применяемых компонент под задачи конкретного объекта КИИРФ, снижение стоимости ее создания (модернизации) и владения.

7. Принцип программного доверия и наследования СПО.

Платформа должна обеспечивать возможность «погружения» в свою доверенную среду функционирования прикладных программ и СПО, заявленных владельцем (заказчиком) ведомственного (корпоративного) сегмента (объекта) КИИРФ, в том числе «наследуемых» из модернизируемых объектов КИИРФ.

8. Принцип «мягкой» модернизации.

Платформа должна позволять «мягкую» модернизацию ведомственных (корпоративных) сегментов (объектов) КИИРФ путем замены морально устаревшего оборудования и постепенного переноса существующих объектов КИИРФ на новую платформу без «останова» обслуживания пользователей.

9. Принцип аппаратного доверия.

Платформа должна содержать перечни рекомендованного оборудования для соответствующих классов защищенности и уровней сложности объектов КИИРФ.

10. Принцип динамичности научно-технического потенциала.

Применительно к платформе должны обеспечиваться возможности быстрого наращивания численности специалистов по ее компонентам, адаптации платформенных решений под характеристики сегментов (объектов) КИИРФ.

3.Аппаратно-программная платформа «Синтез-АПП»

В соответствии с тактико-техническими заданиями на инициативные ОКР серии «Синтез», согласованными с регулятором (ФГКУ «Войско-

вая часть 43753»), в 2012-2013 г.г. была разработана первая версия отечественной защищенной аппаратно-программной платформы «Синтез-АПП» (рис. 1), получены документы соответствия требованиям информационной безопасности при обработке открытой, конфиденциальной информации и информации с грифом секретности (до совершенно секретно включительно [11]), зарегистрирован торговый знак продуктов платформы – «СИНТЕЗАЙТИС» [12]. В 2013-2014 г.г. на платформе «Синтез-АПП» были построены первые десятки объектов КИИРФ, проведены обучение их пользователей и подготовка обслуживающего персонала, создана система технической поддержки, обеспечены условия развития платформы.

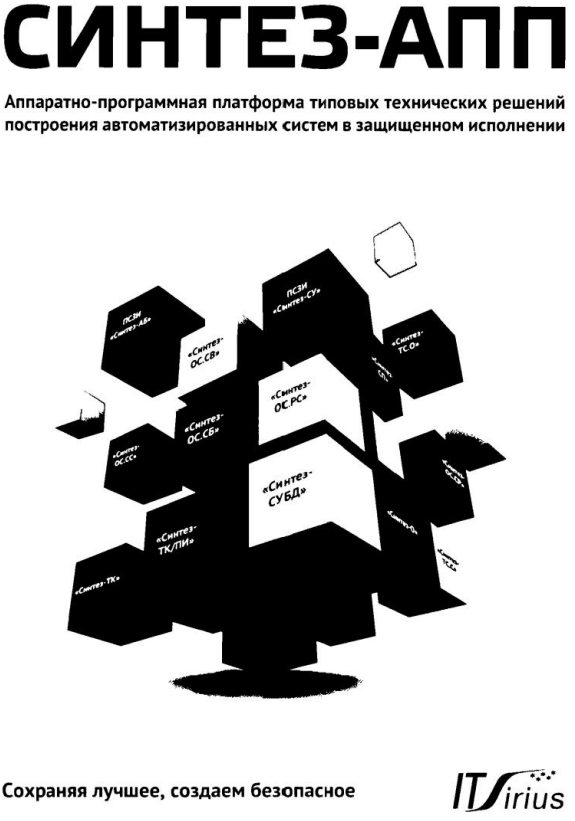

Рис. 1. Аппаратно-программная платформа «Синтез-АПП»

Решения по обеспечению полноценности платформы «Синтез-АПП»

Для обеспечения полноценности платформы «Синтез-АПП» базовый комплект программных средств разрабатывался в следующем составе: семейство защищенных операционных систем (для объектом малой, средней и большой сложности), защищенная система управления базами данных, сервер приложений, встроенные программные средства защиты информации и средства интеграции с внешними средствами защиты информации объектов КИИРФ, средства администрирования, разработки, офисный пакет и другие программы, перечисленные в таблице 1.

Таблица 1. Состав первичного комплекта программных средств платформы «Синтез-АПП»

Назначение изделия	Модификация и обозначение изделия
Операционные системы	серверная специальная «Синтез-ОС.СС»
	серверная вспомогательная «Синтез-ОС.СВ»
	серверная базовая «Синтез-ОС.СБ»
	для виртуальных машин и рабочих станций «Синтез-ОС.РС»
Сервер приложений	«Синтез-СП»
Терминальный сервер	специальный «Синтез-ТС.С»
	объединенный «Синтез-ТС.О»
Терминальный клиент	«Синтез-ТК»
Персональный идентификатор пользователя	«Синтез-ТК/ПИ»
Система управления базами данных	«Синтез-СУБД»
Офисные средства	«Синтез-О»
Программное средство защиты информации	Сервер управления «ПСЗИ «Синтез-СУ»»
	Агент безопасности «ПСЗИ «Синтез-АБ»»
Сервер хранения данных	«Синтез-СХД»
Сервер каталогов	«Синтез-СК»
Сервер обновлений	«Синтез-СО»
Сервер разработки приложений	«Синтез-РП»

Решения по обеспечению импорто- и технологической независимости платформы «Синтез-АПП»

Для достижения независимости платформы «Синтез-АПП» от импорта было принято решение о создании программных компонент на базе ядра Linux [13], их интеграции с локализованными заимствованными модулями открытого программного обеспечения (далее - открытое ПО), сертифицированными средствами защиты информации других российских компаний.

Для гарантированной технологической независимости сегментов (объектов) КИИРФ при проектировании платформы и построении системы технической поддержки были реализованы решения по созданию «воздушного зазора» (см. табл. 2). «Воздушный зазор» исключает возможность доступа к техническим средствам и информации (данным) объектов КИИРФ из-за пределов сегмента (объекта) КИИРФ, обеспечивает технологическое взаимодействие объектов КИИРФ только внутри сегмента КИИРФ и с разработчиком платформы «Синтез-АПП».

Таблица 2. Общая схема организации технической поддержки платформы «Синтез-АПП»

Объекты КИИРФ (запросы, получение ТП)	Уровень проблем ТП				
	1-й	2-й	3-й	уровень ПСЗИ платформы «Синтез-АПП»	уровень ядра Linux, нелокализованного ПО
	Внутренний контур ТП				Внешний контур ТП
	БД(БЗ)ПлС			БД(БЗ)ПлС-ПСЗИ	БД(БЗ)НЛПО
Оказание консультативной помощи (решение задач 1-го уровня сложности)					
→	→				
←	←				
Решение задач 2-го уровня сложности					
→	→	→			
←	←	←			
Текущее обслуживание (решение задач 3-го уровня сложности - обновление ПО и т.п.)					
→	→	→	→		
←	←	←	←		
Устранение ошибок программ и ПСЗИ «Синтез»					
→	→	→	→	→	
				←	
←	←	←	←		
Устранение ошибок ядра Linux, нелокализованного ПО					
→	→	→	→	→	
Воздушный зазор					
				→ → →	→ → →
				← ← ←	← ← ←
Воздушный зазор					
←	←	←	←		

Примечание.

БД(БЗ)ПлС – базы данных (базы знаний) ошибок (уязвимостей) программ платформы «Синтез-АПП», решений по их устранению.

БД(БЗ)ПлС-ПСЗИ – базы данных (базы знаний) ошибок (уязвимостей) программных средств защиты информации платформы «Синтез-АПП», решений по их устранению.

БД(БЗ)НЛПО – базы данных (базы знаний) ошибок (уязвимостей), выявленные в ядре Linux и нелокализованном ПО, решений по их устранению.

Решения по обеспечению промышленного уровня платформы «Синтез-АПП»

В целях быстрого достижения промышленного уровня платформы «Синтез-АПП» было принято решение о применении в качестве лока-

лизуемых программ продуктов компании Red Hat, как мирового лидера открытого ПО на основе ядра Linux (рис. 2).

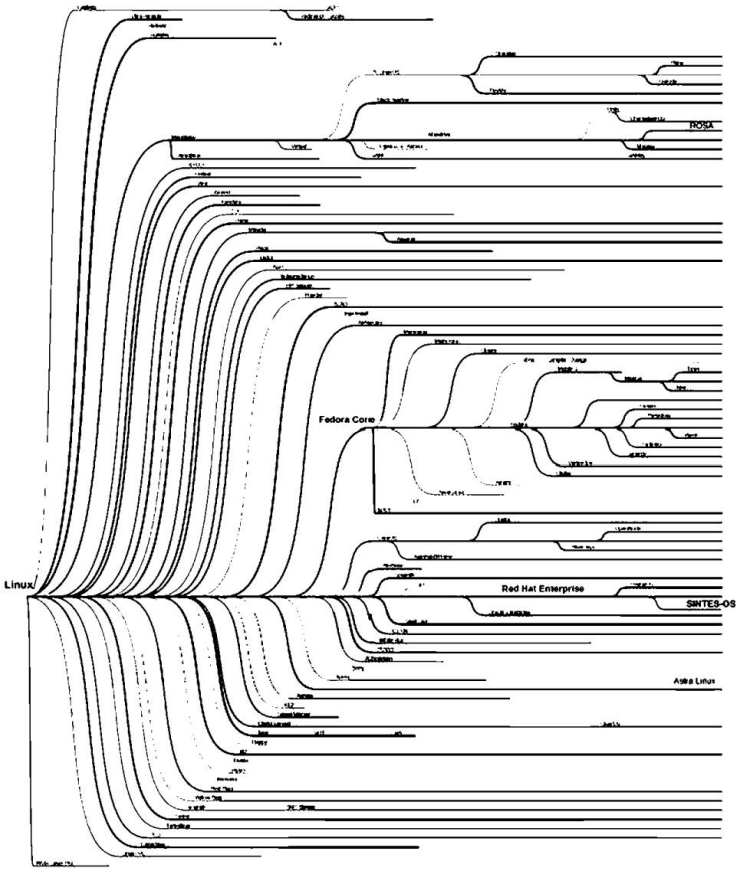

Рис. 2. Семейство операционных систем на основе ядра Linux

Для этой цели в 2012 г. под руководством и с участием автора разработчиком платформы «Синтез-АПП» было подписано соглашение с Red Hat [14], согласно которому в платформу было разрешено встраивание модулей и программ, прошедших внутреннюю сертификацию Red Hat, разработчику платформы был открыт доступ к базам данных (знаний) о совместимости программ и аппаратных средств, ошибках и уязвимостях программ, выявленных Red Hat, путях их устранения.

Взаимодействие с Red Hat обеспечило быстрое достижение компанией-разработчиком требуемого научно-технического потенциала, оперативную локализацию заимствованного ПО, разработку собственных программных средств защиты информации и средств взаимодействия с внешними средствами защиты информации, проведение комплексных нагрузочных и функциональных испытаний, испытаний на совместимость с аппаратными средствами, комплекса исследований на соответствие требованиям регуляторов в области информационной безопасности, создание системы технической поддержки и подготовки специалистов, формирование собственных баз данных (знаний) по продуктам платформы «Синтез-АПП».

Для разработки защищенной СУБД «Синтез-СУБД» было принято решение об использовании кода открытой СУБД PostgreSQL, в создании которого принимали участие известные российские разработчики мирового уровня [15].

По всем направлениям разработки программных компонент платформы обеспечивалось взаимодействие с сообществами разработчиков открытого ПО [16], организованное по образцу Red Hat (рис. 3 [17]).

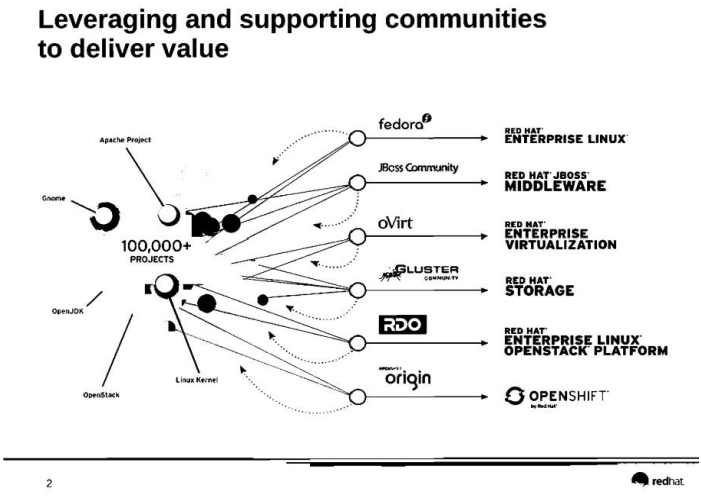

Рис. 3. Использование и поддержка сообществ открытого ПО

Решения по обеспечению универсальности платформы «Синтез-АПП»

Для достижения универсальности платформы было принято решение о создании семейства защищенных операционных систем «Синтез-ОС»

(см. таблицу 1) на основе технологий виртуализации и унификации программных модулей. Состав основных модулей семейства операционных систем «Синтез-ОС» приведен на рис. 4.

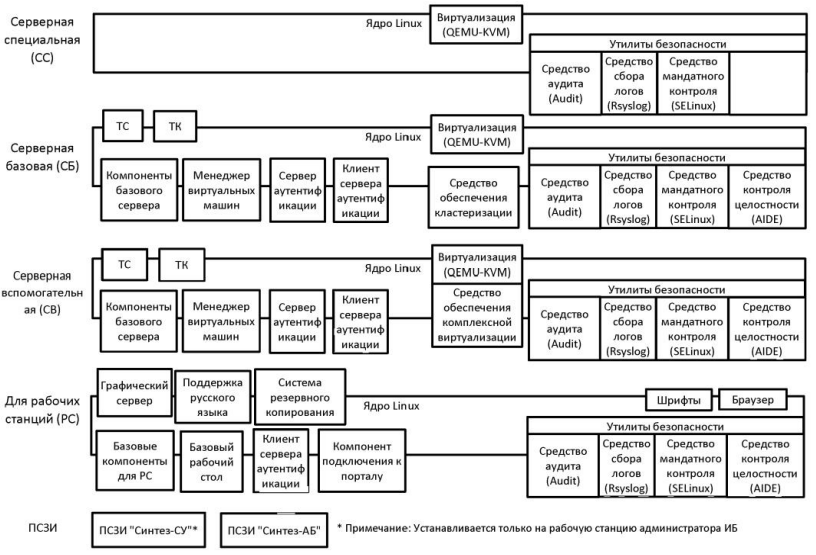

Рис. 4. Модульный состав семейства операционных систем «Синтез-ОС»

На объектах КИИРФ, созданных на платформе, обработка информации осуществляется на виртуальных машинах, развернутых на защищенных серверах. Программные компоненты платформы были разработаны для установки на серверах с аппаратной поддержкой виртуализации, рабочих станциях, терминалах.

Взаимодействие пользователя с виртуальной машиной осуществляется посредством терминального АРМ «Синтез-Т» (рис. 5), который обладает высокой безопасностью, малыми массой и габаритами, низким энергопотреблением, не требует для своего функционирования источников бесперебойного питания. АРМ не содержит собственных средств хранения информации, что исключает утрату защищаемой информации в случае выключения электропитания или хищения АРМ.

Рис. 5. Терминал «Синтез-Т»

Реализованные в платформе меры по защите среды виртуализации исключают несанкционированный доступ как к информации, обрабатываемой в виртуальной инфраструктуре, так и к компонентам виртуальной инфраструктуры: средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной и физической инфраструктуры, гостевым операционным системам, виртуальным машинам, системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям. Пример реализации объекта КИИРФ представлен на рис. 6.

Решения по обеспечению гарантий развития и поддержки платформы «Синтез-АПП»

Проектирование, развертывание, техническая поддержка и квалификационная поддержка (сертификация) подготовки эксплуатационного и обслуживающего персонала объектов КИИРФ по аппаратным и программным компонентам платформы обеспечиваются силами отечественных разработчиков, имеющих также доступ к ресурсам сообществ разработчиков открытого ПО.

Общая схема организации технической поддержки платформы «Синтез-АПП» представлена в таблице 2. Поддержка и развитие платформы, созданных на ней объектов КИИРФ обеспечиваются совокупностью следующих факторов.

1. Научно-техническим потенциалом отечественного разработчика платформы, авторским сопровождением объектов КИИРФ, созданных на платформе.

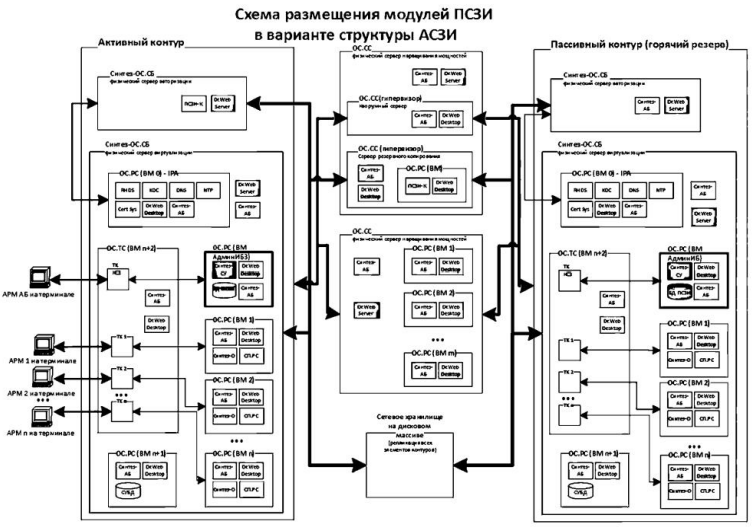

Рис. 6. Пример реализации объекта КИИРФ

2. Ведением разработчиком платформы баз данных (знаний) об ошибках (уязвимостях) программ платформы, имевшихся инцидентах на объектах КИИРФ.

3. Доступностью баз данных (знаний) об ошибках и уязвимостях в заимствованном до локализации программном обеспечении, выявленных сообществами разработчиков открытого ПО.

4. Доступностью для разработчика платформы баз данных (знаний) Red Hat об ошибках и уязвимостях в заимствованном до локализации программном обеспечении, выявленных в процессе внутренней сертификации Red Hat.

5. Доступностью для разработчика платформы сведений о результатах внутренней сертификации Red Hat аппаратных средств, программного обеспечения на их совместимость, производительность и отказоустойчивость различных тестовых реализаций технических решений.

6. Ведением разработчиком платформы баз данных о совместимости сертифицированных средств платформы с аппаратными средствами,

прикладными программами и СПО владельцев (заказчиков) объектов КИИРФ.

4. Система защиты информации платформы «Синтез-АПП»

Особенностью платформы «Синтез-АПП» является то, что ее система защиты информации обеспечивает создание объектов КИИРФ различных классов защищенности: от объектов, на которых информация является открытой до объектов, на которых обрабатывается конфиденциальная информация (для служебного пользования, персональные данные, банковская тайна, коммерческая тайна, врачебная тайна и т.п.) или имеющая гриф секретности (секретно, совершенно секретно).

Комплекс программ «Защищённая операционная система «Синтез» соответствует требованиям ФСБ России по защите информации от несанкционированного доступа с использованием средств криптографической защиты информации в автоматизированных информационных системах, расположенных на территории Российской Федерации, 1 класса, и может использоваться для обработки информации, содержащей сведения, составляющие государственную тайну [18].

Для удовлетворения требованиям по информационной безопасности в составе системы защиты информации платформы «Синтез-АПП» созданы подсистемы управления доступом, регистрации и учета, криптографическая подсистема, подсистемы обеспечения целостности и антивирусной защиты.

Соответствие требуемому классу защищенности объекта КИИРФ достигается многообразными настройками подсистем системы защиты информации. Конфиденциальный характер сведений о решениях и настройках подсистем системы защиты информации не позволяет в рамках статьи остановиться на них подробнее.

Реализованные в платформе механизмы защиты информации обеспечивают безопасное взаимодействие объектов КИИРФ разных классов защиты, в том числе объектов с разными уровнями конфиденциальности обрабатываемой информации. Пример организации безопасного взаимодействия объектов КИИРФ, применительно к классификации, разработанной в [19], приведен на рис. 7

5. Развитие платформенных решений для объектов критической информационной инфраструктуры

Стратегия импортозамещения существенно активизировала разработку отечественного программного обеспечения. По состоянию на ноябрь 2018 г. Единый реестр российских программ для электронных вычислительных машин и баз данных [20] уже содержал 46 продуктов толь-

ко класса «Операционные системы» и 47 продуктов класса «Системы управления базами данных».

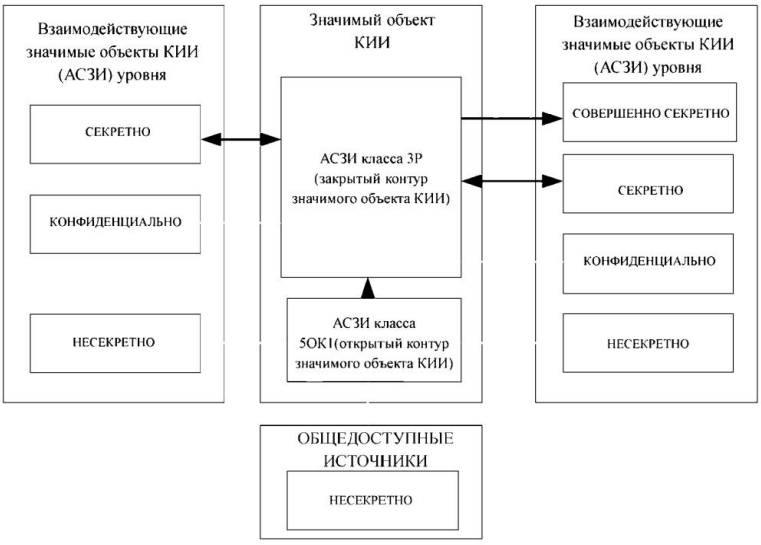

Рис. 7. Пример организации безопасного взаимодействия объектов КИИРФ

Следует отметить, что почти все операционные системы были разработаны на основе ядра Linux, однако далеко не все они могут быть использованы при создании и эксплуатации объектов КИИРФ, что обусловлено требованиями регуляторов в области информационной безопасности, очень немногие отвечают промышленному уровню, обеспечивают универсальность, возможности «наследования» действующих объектов КИИРФ, предоставляют надежные гарантии развития и поддержки.

С позиций изложенной выше методологии критериям «платформа», наряду с платформой «Синтез-АПП», наиболее близко соответствуют линейки продуктов семейства операционных систем «Astra Linux Special Edition» и программных комплексов семейства «Циркон». Подробная информация о данных платформах представлена на сайтах производителей. [21, 22].

Предположительно, платформа «Astra Linux Special Edition» была разработана на основе одного из дистрибутивов операционной системы Debian. Операционные системы Debian используют ядро Linux или FreeBSD [23].

Как отражено на сайте разработчика платформа «Циркон» была разработана на базе одного из дистрибутивов операционной системы CentOS. Операционная система CentOS представляет собой дистрибутив Linux, основанный на коммерческом Red Hat Enterprise Linux (RHEL) [24]. Однако, как неоднократно отмечалось Red Hat [17], операционные системы CentOS являются клонами RHEL, поддержка которых Red Hat не осуществляется.

Детальное сравнение платформ требует отдельного исследования, что в задачи данной статьи не входит. Но можно отметить, что в отличие от других, только платформа «Синтез-АПП» изначально базировалась на программных модулях (пакетах) дистрибутивов RHEL, RHEV (Red Hat Enterprise Virtualization), имевших и имеющих контроль и поддержку промышленного уровня. Это дает дополнительные гарантии защиты от непредвиденных ошибок (уязвимостей), обеспечивает оперативность устранения возможных инцидентов на объектах КИИРФ. В платформе «Синтез-АПП» была реализована описанная выше методология, которая применялась с этапа проектирования платформы и используется сейчас при сопровождении и технической поддержке созданных на ней объектов.

6. Заключение

Курс на импортозамещение программного обеспечения вызвал большое оживление разработчиков. Однако далеко не все разработчики изначально задумываются о необходимости обеспечить безопасность своих программ для информации, которая обрабатывается (хранится, передается, и т.д.) с их помощью или с которой они взаимодействуют. Поэтому, несмотря на значительный объем разработок, выполненных за последние годы, далеко не все программы могут быть применены на объектах КИИРФ. Изложенные в статье методологические аспекты и опыт создания отечественной аппаратно-программной платформы ориентированы на разработчиков программного обеспечения и платформенных решений. Их учет и применение обеспечит повышение качества и оперативности создания объектов КИИРФ и иных разнообразных автоматизированных систем в защищенном исполнении, гарантий их развития и поддержки.

Список литературы

[1] Maitland Hyslop. Critical Information Infrastructures: Resilience and Protection. -Springer, 2007. - 277 p.

[2] Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 05.12.2016 № 646.

3] Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы. Утверждена Указом Президента Российской Федерации от 09.05.2017 № 203.

4] Программа «Цифровая экономика Российской Федерации». Утверждена Постановлением Правительства Российской Федерации от 28.07.2017 г. № 1632-р.

[5] ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. – М.: Стандартинформ, 2000. – 10 с.

[6] ГОСТ Р 50.1.056-2006. Техническая защита информации. Основные термины и определения. – М.: Стандартинформ, 2006. – 20 с.

[7]Сабанов А.Г. Доверенные системы как средство противодействия киберугрозам // Защита информации. Инсайд. 2015, № 3 (63), с. 17-21.

[8]Муравник В.Б., Захаренков А.И., Добродеев А.Ю. Некоторые предложения по подходу и порядку реализации политики и стратегии импортозамещения в интересах национальной безопасности и укрепления обороноспособности Российской Федерации // Вопросы кибербезопасности. 2016, № 1 (14), с. 2-8.

[9]Михалевич И.Ф. Концепция создания доверенной среды функционирования автоматизированных систем в защищенном исполнении на базе операционной системы «Синтез-ОС». – М.: ООО «АйТиСириус», 2012. – 50 с. [Электронный ресурс]. URL: https://www.itsirius.su/resheniya/ (дата обращения: 20.12.2012).

[10]Михалевич И.Ф. Проблемы создания доверенной среды функционирования автоматизированных систем управления в защищенном исполнении / Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014, Москва). - М.: Институт проблем управления им. В.А.Трапезникова РАН, 2014. - С. 9201-9207.

[11]Аттестат № СФ/014-3065 от 10.02.2017 соответствия Комплекса программ «Защищённая операционная система «Синтез» требованиям ФСБ России по защите информации от несанкционированного доступа с использованием средств криптографической защиты информации в автоматизированных информационных системах, расположенных на территории Российской Федерации, 1 класса. Выдан ЦЛСЗ ФСБ России.

[12]Свидетельство на товарный знак (знак обслуживания) № 533289 «СИНТЕЗАЙТИС», приоритет товарного знака 03.12.2013 г., зарегистрировано в Государственном реестре товарных знаков и знаков обслуживания РФ 30.01.2015 г.

[13] Robert Love. Linux Kernel Development, 3rd Edition. - Pearson Education, Inc., 2010. - 468 p.

[14] Memorandum of intensions of the parties Red Hat Inc., EMEA Red Hat Limited, «ITSirius» LLC, 2012).[Электронный ресурс]. URL: https://www.itsirius.su/partnery/ (дата обращения: 25.06.2014).

[15] И. Панченко. PostgreSQL: вчера, сегодня, завтра // Открытые системы. СУБД, 2015, № 3, с. 34-37.

[16] Сообщества Linux в интернете.[Электронный ресурс]. URL: https://losst.ru/soobshhestva-linux-v-internete/ (дата обращения 08.01.2018).

[17] The Red Hat Enterprise Linux advantage over CentOS in your enterprise (presentation). 2014, Red Hat.

[18] Выписка из перечня средств защиты информации, сертифицированных ФСБ России. [Электронный ресурс]. URL: http://clsz.fsb.ru/certification.htm (дата обращения: 10.08.2018).

[19] Калашников А.О., Михалевич И.Ф. Унифицированная система классификации защищенности значимых объектов критической информационной инфраструктуры российской федерации по критериям безопасности информации // Информация и безопасность, 2018, т. 21, вып. 1. С. 6-17

[20] Единый реестр российских программ для электронных вычислительных машин и баз данных. [Электронный ресурс]. URL: https://reestr.minsvyaz.ru/reestr/ (дата обращения: 23.11.2018).

[21] Операционные системы «Astralinux». [Электронный ресурс]. URL: http://astralinux.ru/ (дата обращения: 23.11.2018).

[22] Программный комплекс «Циркон». [Электронный ресурс]. URL: https://www.swemel.ru/ (дата обращения: 23.11.2018).

[23] Проект Debian. [Электронный ресурс]. URL: https://www.debian.org/ (дата обращения: 23.11.2018).

[24] Проект CentOS. [Электронный ресурс]. URL: https://www.centos.org/ (дата обращения: 23.11.2018).

Requirements, principles, practice of creating domestic hardware-software platforms for automated systems in the protected execution of the critical information infrastructure of the Russian Federation

Mikhalevich I.F.

The paper sets out a system of requirements and principles that determine the methodological aspects of creating domestic hardware-software platforms for automated systems in the protected execution as the basis of the critical information infrastructure of the Russian Federation, describes the experience of creating a protected hardware-software platform "Sintez-HSP"that fully satisfies the most strict requirements for information security, reliability, scalability, ensuring the independence of critical information infra the structure of foreign technologies and software.
Keywords: automated systems in the protected execution, hardware-software platform, information security, critical information infrastructure, Sintez-HSP