УДК 004.056

ПРОБЛЕМЫ И ПУТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АППАРАТНО-ПРОГРАММНЫХ ПЛАТФОРМ ДЛЯ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

И.Ф. Михалевич
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: mif-orel@mail.ru

Ключевые слова: аппаратно-программная платформа, информационная безопасность, кибербезопасность, критерии доверия, критическая информационная инфраструктура, принципы доверия.

Аннотация: Проблема обеспечения безопасности критических информационных инфраструктур должна учитываться на всех этапах жизненного цикла и не может быть решена при использовании аппаратно-программной платформы, безопасность которой не была проверена или в последующем была скомпрометирована. В работе приводится анализ национальных и межнациональных целей и ролей в области кибербезопасности критических инфраструктур и обслуживающих их сетей связи, на основе которого была разработана система критериев и принципов доверия к аппаратно-программным платформам. Представлен пример и результаты разработки платформы «Синтез-АПП», удовлетворяющей системе предложенных критериев и принципов доверия.

1. Введение

Защита критических информационных инфраструктур (далее – КИИ) входит в число приоритетов Российской Федерации [1-4] и других стран [5-9]. В критических информационных инфраструктурах может содержаться как открытая информация, так и сведения, составляющие государственную тайну. Открытая информация должна быть доступной. Несанкционированное получение конфиденциальной или секретной информации должно быть гарантированно исключено. Эти специфические условия должны гарантироваться аппаратно-программными платформами (далее – АПП или платформа) информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей и сетей связи, обеспечивающих функционирование объектов критических информационных инфраструктур (далее – элементы КИИ).

На всех этапах жизненного цикла платформ для КИИ названные условия должны соблюдаться неукоснительно. Доверие платформе не должно вызывать сомнений.

Что понимать под доверием, каким критериям оно должно соответствовать и какие принципы должны соблюдаться при разработке платформ? Можно ли соблюсти эти критерии и принципы? Данные вопросы рассмотрены в статье.

2. Критерии и принципы доверия платформам

Задача обеспечения доверия платформе для КИИ вытекает из национальных и межнациональных целей и ролей в области кибербезопасности общества, критических инфраструктур и обслуживающих их сетей связи. Пример целей и ролей в области кибербезопасности, основанный на анализе [1-9], приведен в таблице 1.

Таблица 1. Примеры национальных и межнациональных целей и ролей в области кибербезопасности.

Страна или организация	Цель или роль
РФ	Улучшение кибербезопасности критической инфраструктуры, автоматизированных и информационных систем и сетей электросвязи КИИ за счет применения доверенных аппаратно-программных платформ, не зависящих от зарубежных информационных технологий и средств обеспечения информационной безопасности
США	Улучшение кибербезопасности федеральных сетей, критической инфраструктуры, нации
ООН	Отчет Группы правительственных экспертов ООН по вопросам развития на местах информации и телекоммуникаций в контексте международной безопасности, опубликованный в июле 2015 года, в частности, рекомендует некоторые меры по укреплению доверия и дает комментарии относительно того, как применяется международное право
Совет Европы	Помогает защищать общества во всем мире от угрозы киберпреступности в рамках Конвенции о киберпреступности (Совет Европы 2011) и программ технического сотрудничества по киберпреступности
Организация по безопасности и сотрудничеству в Европе (ОБСЕ)	В марте 2016 года приняла решение «Меры укрепления доверия для снижения рисков конфликтов, связанных с использованием информационных и коммуникационных технологий» (ОБСЕ 2016)
Организация экономического сотрудничества и развития (ОЭСР)	Поддержка инициатив в области конфиденциальности, безопасности, цифровой идентификации и электронного рынка
Организация Североатлантического договора (НАТО)	Совместный центр сотрудничества киберзащиты НАТО (CCDCoE): «… роль кибербезопасности НАТО может быть разделена на две широкие темы ... Первым приоритетом является защита своих собственных сетей, как это было согласовано союзниками на саммите НАТО в Уэльсе в 2014 году (NATO 2014). Второй приоритет НАТО – помочь своим членам в развитии их собственных возможностей и потенциала в области кибербезопасности (Н. Робинсон, 2016). Европейский союз и НАТО подписали техническое соглашение о реагировании на компьютерные инциденты (NCIRC) и CERT-EU (NATO 2016)
Африканский союз (АС)	Принятие основ кибербезопасности и защиты данных
Организация американских государств (ОАГ)	Помощь американским государствам в разработке и применении мер киберзащиты
Ассоциация государств Юго-Восточной Азии (АСЕАН)	Сосредоточение внимания на возможностях кибербезопасности и укреплении доверия

Критерии доверия платформам, разработанные на основе национальных требований по информационной безопасности и защите КИИ [1-4], общих и функциональных требований к АПП для КИИ [10-11], приведены в таблице 2.

Таблица 2. Критерии доверия платформам для КИИ.

Критерий доверия	Описание
Полнота состава компонентов	свойство платформы обеспечить нормативные показатели функционирования элементов КИИ без привлечения базовых компонентов других платформ
Универсальность	свойство платформы на основе своих базовых компонентов обеспечить создание (модернизацию) элементов КИИ различного назначения, масштаба, классов защиты, уровней топологической и архитектурной сложности
Устойчивость	свойство платформы сохранять в норме показатели функционирования при воздействиях на элементы КИИ
Промышленный уровень	свойство платформы сохранять в норме показатели функционирования в течение всего срока эксплуатации элементов КИИ при больших нагрузках и объемах данных
Гарантии развития	свойство платформы наращивать состав своих компонентов для соблюдения новых требований со стороны КИИ в процессе функционирования ее элементов
Гарантии поддержки	свойство платформы поддерживать полную работоспособность своих компонентов в течение всего срока службы созданных на платформе элементов КИИ
Независимость от импорта	свойство платформы сохранять полноту состава компонентов, универсальность, гарантии развития и поддержки без применения импортных компонентов
Технологическая независимость	свойство платформы сохранять в норме показатели функционирования без принудительного обновления компонентов и управления из-за рубежа, передачи технологической информации за рубеж

Доверие к платформе для КИИ может быть основано на принципах, которые вытекают из условий соблюдения требований по информационной безопасности и защите КИИ [1-4], общих и функциональных требований к АПП для КИИ [10-11]. Данные принципы отражены в таблице 3.

Таблица 3. Критерии доверия платформам для КИИ.

Принцип доверия	Описание
модульности ПО	наличие законченных функциональных программных модулей для многократного применения
унификации ПО	максимальное использование программных модулей общего и специального назначения
локализации заимствованного ПО	проверки заимствованных пакетов, модулей, программ на соответствие назначению, отсутствие уязвимостей, недекларированных возможностей и ошибок, совместимость и отсутствие влияния на функционирование средств защиты информации, доработка, фиксация кода и документирование ПО, обеспечение гарантий развития и поддержки
типизации технических решений	создание типовых конфигураций элементов КИИ (типовых технических решений) путем комбинирования базовых компонентов платформы
масштабируемости	увеличение вычислительных мощностей и объемов данных, усложнение архитектуры элементов КИИ кластеризацией типовых конфигураций базовых компонентов платформы
универсальности ПСЗИ	изменение классов защиты элементов КИИ без замены программных средств защиты информации (ПСЗИ) платформы
оптимизации ресурсов (кастомизации)	комбинирование базовых компонентов АПП под задачи элементов КИИ для минимизации стоимости их создания и владения
программного доверия и наследования СПО	«погружение» в доверенную среду, созданную платформой, прикладных программ и СПО, заявленных владельцами или «наследуемых» в процессе модернизации элементов КИИ
«мягкой» модернизации	замена морально устаревшего оборудования или перенос существующих элементов КИИ на платформу без «останова» функционирования элементов КИИ и обслуживания пользователей
аппаратного доверия	наличие перечней рекомендованного оборудования для элементов КИИ по классам защиты, уровням сложности

Принцип доверия	Описание
динамичности потенциала	быстрое наращивание производства компонентов АПП и увеличение численности специалистов

4. Пример разрешения проблем безопасности, опыт разработки платформы «Синтез-АПП» для критической информационной инфраструктуры

Аппаратно-программная платформа «Синтез-АПП» была разработана в рамках инициативных ОКР серии «Синтез». Доверие к платформе подтверждено заключениями и аттестатами соответствия, разрешающим создание элементов КИИ с наивысшим уровнем конфиденциальности информации [12]. С 2013 г. на платформе «Синтез-АПП» под торговой маркой «СИНТЕЗАЙТИС» успешно создаются элементы КИИ.

Полнота состава компонентов платформы была обеспечена разработкой комплекта базовых компонентов в составе: семейство защищенных операционных систем «Синтез-ОС», защищенная система управления базами данных «Синтез-СУБД», сервер приложений, средства защиты информации, контроля и администрирования, офисный пакет, средства разработки СПО [10-11].

Универсальность платформы была достигнута применением защищенных технологий виртуализации, созданием на их основе семейства защищенных операционных систем «Синтез-ОС», которыми совместно с встроенными средствами защиты информации, контроля и администрирования создается доверенная среда «Синтез».

Устойчивость платформы была обеспечена разработкой встроенных программных средств защиты информации и их интеграции с антивирусными и другими взаимодействующими средствами защиты информации, применяемыми в КИИ, средств мониторинга и администрирования.

Промышленный уровень платформы был достигнут локализацией продуктов Red Hat. В 2012 г. с участием автора с Red Hat было подписано соглашение. В платформу «Синтез-АПП» было разрешено встраивание модулей и программ, прошедших внутреннюю сертификацию Red Hat, был открыт доступ к базам данных и банкам знаний о совместимости программ и аппаратных средств, ошибках и уязвимостях, выявленных Red Hat при внутренней сертификации программ и их дальнейшей эксплуатации, путях устранения проблем.

В качестве базы для разработки защищенной СУБД «Синтез-СУБД» была принята открытая СУБД PostgreSQL, имеющая в РФ дополнительную высококвалифицированную поддержку.

Гарантии развития обеспечены использованием ядра Linux, на котором возможна разработка программ любого назначения и любого уровня сложности.

Гарантии поддержки платформы обеспечены авторским сопровождением объектов КИИ российским разработчиком платформы, который ведет базы данных и банки знаний об инцидентах в функционировании базовых компонентов платформы, а также об ошибках и уязвимостях в заимствованном нелокализованном ПО, осуществляет проверки совместимости, производительности и отказоустойчивости сертифицированных базовых компонентов платформы с аппаратными средствами, прикладными программами и СПО владельцев (заказчиков) элементов КИИ.

Независимость от импорта платформы обеспечена применением средств собственной разработки и сертифицированных средств российских компаний, а также локализованного заимствованного ПО с открытым исходным кодом.

Технологическая независимость платформы «Синтез-АПП» обеспечена отсутствием непосредственного взаимодействия элементов КИИ с серверами, размещенными за границей. Кроме этого, для объектов КИИ, на которых обрабатывается информация ограниченного доступа (содержащая сведения конфиденциального характера или составляющие государственную тайну), гарантируется «воздушный зазор», исключающий возможность несанкционированного сетевого взаимодействия

5. Заключение

В статье представлены подходы и опыт решения проблем безопасности аппаратно-программных платформ, сформулированы критерии и принципы доверия к аппаратно-программным платформам для критических информационных инфраструктур. Предложенные решения предназначены для использования при разработке доверенных аппаратно-программных платформ, а также при создании на их основе защищенных критических информационных инфраструктур.

Список литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
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 Распоряжением Правительства Российской Федерации от 28.07.2017 № 1632-рп).
5. National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014.
6. Executive order 13800 (2017) of President of USA “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”.
7. A Generic National Framework for Critical Information Infrastructure Protection (CIIP). ITU, 2007.
8. Critical Information Infrastructures Protection approaches in EU. TLP: Green, July 2015.
9. Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU. Study. Science and Technology Options Assessment. EPRS/STOA/SER/16/214N. European Parliamentary Research Service, European Parliament: Scientific Foresight Unit (STOA), PE 603.175: Brussels – 2017.
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, 16-19 июня 2014 г. М.: Институт проблем управления им. В.А.Трапезникова РАН, 2014. С. 9201-9207.
11. Mikhalevich I.F. Methodological foundations of creation of national protected hardware-software platforms for critical information infrastructures // T-Comm.,(2018. Vol. 12, No.3, P. 75-81.
12. Аттестат № СФ/014-3065 от 10.02.2017 соответствия Комплекса программ «Защищенная 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. http://clsz.fsb.ru.