Этап 5

Задачи 5 этапа

Основными задачами пятого этапа выполнения работ являлись:

- обобщение и оценка полученных результатов, в том числе:
  - обобщение результатов исследований;
  - сопоставление анализа научно-информационных источников и результатов теоретических и экспериментальных исследований;
  - оценка эффективности полученных результатов в сравнении с современным научно-техническим уровнем;
  - анализ выполнения требований ТЗ на ПНИ;
  - оценка полноты решения задач и достижения поставленных целей ПНИ;
- разработка технических требований и предложения по разработке, производству и эксплуатации продукции с учетом технологических возможностей и особенностей индустриального партнера — организации реального сектора экономики;
- проведение технико-экономической оценки рыночного потенциала полученных результатов;
- разработка проекта технического задания на проведение ОКР по теме: «Разработка инфраструктуры безопасности распределенных информационно-вычислительных систем на основе открытых протоколов»;
- проведение оценки РИД, полученных при выполнении ПНИ, с целью их вовлечения в хозяйственный оборот;
- проведение маркетинговых исследований с целью изучения перспектив коммерциализации РИД, полученных при выполнении ПНИ.

Выводы по результатам работ на 5 этапе

В результате работы, проделанной на пятом этапе, получены следующие основные выводы. Новые, разработанные в рамках проекта, принципы построения системы безопасности РИВС, основанные на использовании сессионных ключей с ограниченным сроком действия и подписанные хешами запросов в РИВС позволяют решить несколько проблем при построении систем безопасности РИВС:

- использование сессионных ключей решает проблему неограниченной неавторизованной отправки запросов в РИВС в случае кражи секрета; некоторое неудобство необходимости пользователем подтверждать аутентификацию не является существенным недостатком, так как легко может быть выполнено через сервис аутентификации;
- подписывание запросов уникальными хешами, обеспечивает невозможность изменения запроса в РИВС в процессе его обработки; неограниченность действия таких хешей по времени решает проблему необходимости продления действия прокси-сертификатов в традиционных системах безопасности РИВС, основанных на архитектуре открытых ключей.

Основой предложенной методики разработки системы безопасности РИВС является ее базирование на жизненном цикле разрабатываемого ПО в соответствии с ГОСТ 12207-2010.

Ключевым моментов методики является использование итеративная модели разработки отдельных компонентов системы безопасности РИВС так и ЭО ПК в целом. Такая методика предоставляет ряд существенных преимуществ разработчикам ЭО ПК. В частности, данная методика позволяет разработчикам четко структурировать процесс разработки ПО что, в свою очередь, обеспечивает хорошо спланированный по срокам достижение как промежуточных так и конечных целей разработки в строгом соответствии с требованиями ТЗ и ПГ. В то же время, данная методика оставляет разработчикам достаточную свободу в выборе способов достижения целей, что позволяет эффективно учитывать специфику проекта.

Использование архитектурного стиля REST для программирования модулей инфраструктуры безопасности РИВС и представление данных в формате JSON позволяет достигнуть решения поставленных задач выразительным способом, который обеспечивает компактную и наглядную форму как самих программ, так и данных, предназначенных для обмена между модулями. Все это обеспечивает высокое качество программ и их эффективность.

Разработанная в рамках проекта архитектура инфраструктуры безопасности РИВС базируется на новых принципах и подходах к построению системы безопасности, разработанных на первом этапе проекта, и не имеет прямых аналогов среди существующих инфраструктур безопасности. Это подтверждается результатами аналитического обзора современной научно-технической, нормативной, методической литературы (см. раздел 1.2). Разработанная архитектура полностью соответствует требованиям Технического задания.

Разработанные алгоритмы работы ИБ РИВС полностью соответствуют требованиям Технического задания и не имеют прямых аналогов среди существующих инфраструктур безопасности. Это подтверждается результатами аналитического обзора современной научно-технической, нормативной, методической литературы.

В ходе работ по проекту была успешно выполнена реализация всех модулей и алгоритмов предусмотренных техническим заданием. Проверка работы отдельных модулей РИВС в рамках экспериментальных исследований созданного экспериментального образца программного комплекса ИБ РИВС (ЭО ПК ИБ РИВС) показала, что положенные в их основу архитектурные решения и методы программирования полностью соответствуют требованиям технического задания.

Комплексные экспериментальные исследования работы инфраструктуры безопасности РИВС, проведенные в соответствии с Программой и методиками проведения экспериментальных исследований (протоколы проведения представлены в отчете за четвертый этап работ), позволили установить конкретные параметры ЭО ПК, подтвердили правильность положенных в основу разработки инфраструктуры безопасности архитектурных решений и методов программирования, показали полное соответствие созданного в ходе осуществления данного проекта ЭО ПК требованиям Технического задания.

Как показывает сравнение с ранее существовавшими решениями, предложенный в рамках данного проекта подход в комплексе приводит к существенному упрощению как регистрации новых пользователей в системе, так и их работы в РИВС. Некоторое снижение безопасности, связанное с использованием беспарольного сессионного ключа, компенсируется ограничением времени его действия. По истечении срока действия ключа пользователь запрашивает новый ключ либо через специальный веб-интерфейс, либо через API соответствующего сервиса. Важно отметить, что предложенный подход, архитектура и алгоритмы работы обеспечивают достаточную производительность и масштабируемость ИБ РИВС, соответствующую требованиям технического задания. Как показал анализ научно-информационных источников, полученные значения параметров отвечают требованиям к большинству существующих РИВС.

Прототип инфраструктуры безопасности по своим функциональным возможностям конкурентоспособен на мировом уровне. Полученные результаты работы могут быть использованы в облачных структурах, распределенных системах типа грид, системах обработки больших данных (Big Data). Также для организации удаленного доступа к суперкомпьютерам и вычислительным кластерам. Это позволит значительно расширить сферу использования РИВС как в научных исследованиях, так и в российской экономике, в первую очередь в таких высокотехнологичных областях как материаловедение, биотехника, геологоразведка, самолето- и судостроение , космос и другие. С ростом внедрения высокопроизводительных информационно-вычислительных систем и веб-технологий, потребность в РИВС и в веб-услугах по их применению будет многократно возрастать, что гарантирует рост потребностей в системах, обеспечивающих безопасность РИВС в сочетании с дружественными и удобными средствами доступа. Разработаны технические требования и предложения по разработке, производству и эксплуатации ПК ИБ РИВС с учетом технологических возможностей и особенностей индустриального партнера — ООО «Ниагара», организации реального сектора экономики. Выполнение разработанных требований и предложений позволит упростить и сделать дружественным для пользователя использование высокопроизводительных вычислительных ресурсов, таких как суперкомпьютеры, облачные и грид среды, системы обработки больших данных (Big Data) тем самым существенно расширить круг пользователей, время освоения ими этих передовых информационных технологий, что, в свою очередь, приведет к повышению эффективности использования высокопроизводительных ресурсов и, в конечном счете, ускорит разработку новой инновационной продукции. Результаты данного проекта значительно расширят сферу использования РИВС как в научных исследованиях, так и в российской экономике, в первую очередь в таких высокотехнологичных областях как материаловедение, биоинформатика, геологоразведка, самолето- и судостроение , космические исследования и другие.

Проведенная технико-экономическая оценка рыночного потенциала и научно-технического эффекта ПНИ позволяет сделать вывод, что работа существенно превосходит средний уровень, а верхняя оценка для срока окупаемости ПНИ составляет порядка 3 лет.

С целью доведения до потребителя результатов ПНИ, проведенных в рамках настоящего проекта, разработан проект технического задания для проведения последующего ОКР, в результате которой должен быть создан опытный образец ПК ИБ РИВС производственного уровня.

В результате работ по проекту получено два Свидетельства о регистрации прав на программное обеспечение (зарегистрированные РИД). Проведена оценка РИД, полученных при выполнении ПНИ, с целью их вовлечения в хозяйственный оборот и подготовлен отчет об оценке РИД, Основным выводом проведенной оценки является то, что разработанные в результате ПНИ результаты интеллектуальной деятельности базируются на новых принципах и подходах к построению системы безопасности, не имеют прямых аналогов среди существующих инфраструктур безопасности, и являются конкурентоспособными на мировом уровне. Для успешного вовлечения РИД, полученных при выполнении ПНИ, в хозяйственный оборот необходимо проведение ряда мероприятий, включающего проведение соответствующей ОКР, совершенствование программно-технической документации и инструкций для пользователей, а также внедрение разработанной инфраструктуры безопасности в крупные российские РИВС. Маркетинговые исследования показали, что несмотря на сравнительно долгий период развития промежуточного программного обеспечения, рынок коммерческих продуктов для организации распределенных вычислений в научных областях является плохо развитым. Подавляющее большинство продуктов распространяется на некоммерческой основе и на условиях открытых кодов. Сравнение на

основе анализа научно-информационных источников и экспериментальных исследований характеристик разработанного ЭО ПК с другими пакетами, обеспечивающими ИБ РИВС, показывает, что разработанные новые принципы и подходы, архитектура и алгоритмы работы ИБ РИВС являются конкурентоспособными по сравнению с лучшими мировыми образцами. Выборочный опрос ряда российских IT-компаний показал, что разработанное ПО ИБ РИВС представляет интерес для внедрения на предприятиях малого и среднего бизнеса и, таким образом, существуют хорошие перспективы для коммерциализации результатов ПНИ.

Работы по обеспечению и обслуживанию рабочих мест исследователей и разработчиков выполнены полностью. Подводя итог всему проекту в целом, необходимо подчеркнуть, что основные принципы, заложенные в предложенной архитектуре и алгоритмах работы модулей инфраструктуры безопасности соответствуют передовым технологиям, используемым для построения систем подобного рода, а конкретные функциональные возможности не имеют аналогов в мире. Новизна предложенного решения заключается в пересмотре подхода к построению инфраструктуры безопасности РИВС. В частности, предложено отказаться от использования прокси-сертификатов для доступа к ресурсам РИВС, а аутентификацию пользователей производить на время сессии посредством пары логин-пароль с возможностью использования многофакторной аутентификации в необходимых случаях. Четко разделен процесс первичной аутентификации пользователей и повторной аутентификации, а также предложено использовать сессионные ключи с ограниченным сроком действия. Каждый сформированный пользователем запрос подписывается специально сгенерированным хешем, который позволяет предотвратить возможность модификации данного запроса злоумышленником и, как следствие, под видом авторизованного пользователя, выполнить подложный запрос. Разработанные и реализованные в качестве программного комплекса архитектура и алгоритмы позволяют существенно упростить использование РИВС для конечных пользователей, а также эксплуатацию инфраструктуры безопасности. При этом уровень безопасности при работе РИВС превосходит уровень систем, построенных с использованием инфраструктуры открытых ключей.

Результаты работ, полученные в ходе осуществления проекта, представлены в публикациях [15 — 19], а также двух зарегистрированных РИД.