О.В. Лукинова

Об использовании инструментов функциональной стандартизации при создании информационных систем в защищенном исполнении

На уровне методологических описаний представлены вопросы формирования стандартизованных профилей, описывающих разработку системы защиты, которая рассматривается как неотъемлемая составная часть информационной системы. Используются инструменты функциональной стандартизации и теории открытых систем.

Ключевые слова: система защиты, информационная система, профиль, модель OSE/RM, функциональная стандартизация.

Управление ресурсами любой достаточно крупной организации не обходится без использования интегрированной информационно-телекоммуникационной среды, представляющую собой сложную распределенную информационную систему (далее – ИС), неотъемлемой частью которой является и компонента безопасности. При этом сложность рассматривается не только с точки зрения архитектуры самой системы как единого объекта, но также методов его проектирования, сопровождения, развития, т. е. жизненного цикла. Разработку таких объектов необходимо производить на основе описания на уровне базовых стандартов и/или уникальных спецификаций отдельных компонент объекта и интерфейсов между ними.

Наиболее полному и комплексному описанию сложных объектов соответствуют инструменты методологии функциональной стандартизации (далее – ФС), основным из которых является профиль. Под профилем понимается «совокупность нескольких (или

© Лукинова О.В., 2017

подмножество одного) базовых стандартов (и других нормативных документов) с четко определенными и гармонизированными подмножествами обязательных и факультативных возможностей, предназначенных для реализации заданной функции или группы функций»[1]. ФС предлагает к использованию следующие виды профилей: функциональный, технологический, интеграционный.

Совокупность всех трех профилей, разработанных для каждой компоненты ИС (включая и компоненту безопасности), составляет полный профиль системы. В работе[2] были рассмотрены вопросы профилирования целевой ИС, в данной статье рассматриваются методологические предпосылки и особенности построения указанных видов профилей для системы безопасности ИС.

Представление системы защиты ИС на основе модели открытых систем

Применение методологии функциональной стандартизации для профилирования информационной системы, включая и систему защиты, дает хорошие результаты, если ее удается представить совокупностью отдельных компонент. Для этой цели необходимо использовать функциональную референсную модель открытых систем OSE/RM (Open System Environment/Reference Model) IEEE POSIX[3], в соответствии с которой система представляется двумя частями (рис. 1):

– прикладной, т. е. приложениями системы, реализующими целевую функциональность (бизнес-процесс);

– платформенной, которая обеспечивает функционирование приложений посредством системных сервисов.

Базовая структуризация указанных компонент отражается матрицей, по горизонтали которой содержатся группы функций аппаратного слоя – HW, операционного – OW, промежуточного (системно-прикладного) – MW. А по вертикали – функции интерфейса пользователей (колонка «User»); бизнес-логики приложения (колонка «System»); организации данных (колонка «Information»); возможности коммуникации системы (колонка «Communication»). В совокупности с платформенной компонентой 6 рисунка 1 столбца «System» протоколы и средства колонки «Communication» обеспечивают взаимодействие распределенных элементов информационной системы. Стандартизованные возможности программных средств, конкретизирующих указанные компоненты, должны быть включены в интеграционный профиль системы. Интерфейсы

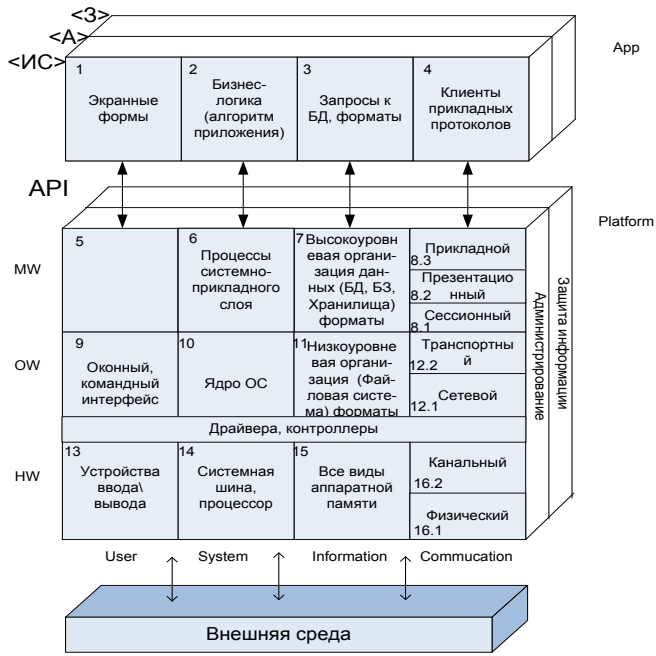

Рис. 1. Референсная модель OSE/RM

между приложениями и платформой, а также функциональными компонентами реализуются с помощью системных вызовов в виде API-функций.

Помимо плоскости целевых функций (плоскость <ИС> рисунка 1), модель содержит также плоскости административных (плоскость <А>) и защитных (плоскость <З>) функций. При этом плоскость <З>, ассоциируемая с системой защиты, имеет два представления:

1) <З`> – межкатегорийное, «клетки» которого включают совокупности защитных механизмов (*Mx*), обеспечивающих безопасность реализаций соответствующих «клеток» базовой плоскости <ИС>, администрирования <А> в соответствии с векторами требований по безопасности $\overline{KS^{ИС}}(C, D, K, ...)$, $\overline{KS^{А}}(C, D, K, ...)$, где *C* – требования по целостности ресурсов, *D* – требования по доступности, *K* – требования по конфиденциальности;

2) <З``> – проектное, т. е. представление системы защиты, структурированное в виде базовой функциональности передней плоскости модели.

Определение 1. Системой защиты (далее – СЗ), обеспечивающей безопасность целевой системы (<ИС>), включая ее администрирование (<А>), назовем совокупность программно-технических средств защиты, реализующих механизмы *Mx* межкатегорийной плоскости <З`>, построенную в соответствии с проектным представлением <З``>.

Методологические предпосылки профилирования системы

Основное назначение стандартизованного описания информационной системы в виде семейства профилей (функционального, технологического, интеграционного для распределенной системы) в том, чтобы фиксировать принятые технические решения для конкретных классов информационных систем на уровне возможностей и параметров базовых стандартов. При разработке и сопровождении сложных систем это условие является решающим, т. к. оно способствует снижению трудоемкости, длительности, стоимости, повышению качества разработки, улучшению других технико-экономических показателей проектов ИС.

Построение функционального профиля СЗ

Функциональный профиль информационной системы на основании[4] регламентирует на уровне стандартов и открытых спецификаций архитектуру и структуру системы и ее компонентов. Если функциональный профиль зарегистрирован государственной или международной организацией по стандартизации, он приобретает статус функционального стандарта соответствующего уровня для рассматриваемого класса систем.

Для СЗ функциональный профиль должен включать два документа: профиль межкатегорийного представления <З`> и профиль проектного представления <З``>. Кроме того, требуется комплекс документов не только профилирующих компоненты <З`> и <З``>, но и описания факторов и критериев для выбора того или иного технического решения.

Построение профиля межкатегорийного представления <З`>

Определение 2. Под механизмом защиты будем понимать способ обеспечения требований безопасности $\overline{KS}(C, D, K, ...)$ к соответствующей компоненте, представляющий собой иерархию рефе-

ренсности: механизм защиты *Mx* – метод реализации механизма *M* – алгоритм реализации метода (*A*): *Mx*(*M*(*A*)).

Выбор конкретной цепочки *Mx*(*M*(*A*)) зависит:

1) от уровня безопасности, задаваемого вектором значений $\overline{KS^{ИС}}(C, D, K, ...)$ или $\overline{KS^{A}}(C, D, K, ...)$ для каждой «клетки» модели OSE/RM;

2) от требований нормативных регуляторов для государственных систем;

3) от параметров эффективности алгоритмов (затратами памяти, временем на выборку значений, удобством ведения данных о субъектах и объектах доступа, удобством отслеживания ограничений и зависимостей по наследованию полномочий и др.), а для криптоалгоритмов – оценок стойкости.

Поэтому в профиль целесообразно включать[5]:

а) ГОСТы или иные нормативные документы, описывающие выбранный алгоритм, так как, особенно для криптоалгоритмов, именно стандарт позволяет реализовать алгоритм с более достоверной оценкой стойкости. Это позволяет обеспечить защитные свойства механизмов в соответствии с уровнем критериев $\overline{KS}(C, D, K, ...)$ или требованиями регуляторов;

б) спецификации, отражающие те критерии и требования, на основе которых происходил выбор метода или механизма.

Построение профиля проектного представления <З``>

Проектная плоскость <З``> связана с тем, что система защиты сама является информационной системой, поэтому она также может быть представлена моделью OSE/RM. Поэтому проектный профиль содержит:

а) профили приложений, реализующих защитные механизмы межкатегорийной плоскости <*З`*> на программном уровне. При этом очевидно, что в виде приложений реализуется только часть механизмов *Mx*. Поэтому объектами стандартизации профиля приложений являются компоненты приложений в структуризации USIC (рис. 1), а также программные интерфейсы между компонентами и платформой;

б) профили среды, которая определяет: традиционные сервисы, предоставляемые платформенной компонентой (промежуточный слой) приложениям; услуги операционных систем, а также требования и интерфейсы к устройствам аппаратного слоя. Кроме того, часть защитных механизмов может быть реализована в виде программно-аппаратных средств и локализована на платформенной компоненте.

Построение технологического профиля

Трехмерность модели OSE/RM позволяет интегрировать все три плоскости, что позволяет проектировать ИС как единый объект. Таким образом, проектирование информационной системы и защиты к ней возможно и необходимо осуществлять одновременно, но с учетом специфики защитной компоненты. К тому же в 2014 г. в Российской Федерации впервые введен ГОСТ, декларирующий одновременное проектирование ИС и ее системы безопасности[6]. Методологически жизненные циклы обеих систем одинаковы и включают однотипные работы.

1. Формирование требований как для информационной системы, так и требований безопасности в виде $\overline{KS^{ИС}}(C, D, K, ...)$, $\overline{KS^{A}}(C, D, K, ...)$ для СЗ. При этом для ИС на этапе консалтинга строятся бизнес-процессы как основа для формирования требований к ИС; для СЗ осуществляется оценка ценности бизнес-процессов как основа для формирования векторов $\overline{KS}(C, D, K, ...)$, дополнительно – модель угроз бизнес-процессов на референсном уровне.

2. Этап концептуального проектирования осуществляется в виде разработки функциональной архитектуры для ИС и межкатегорийной плоскости механизмов <З`> для СЗ.

3. На этапе детального проектирования производится: разработка системно-технической структуры системы с учетом функциональной плоскости <З`>; конкретизация модели OSE/RM по целевым плоскостям и проектной плоскости <З``>, а также модели угроз; интеграция программно-аппаратных реализаций целевой системы и защитных механизмов для СЗ.

4. Вводиться в эксплуатацию обе системы могут и должны одновременно. Поэтому временные диаграммы Ганта, сопровождающие разработку и внедрение систем, должны быть построены с учетом единой точки ввода обеих систем.

5. На стадии сопровождения осуществляется реинжиниринг бизнес-процессов и соответственно модификация ИС, а также перепроектирование СЗ по результатам анализа осуществления ею защитных действий, изменений бизнес-условий или требований безопасности, включая изменения нормативно-законодательной базы.

Технологический профиль системы представляет собой набор стандартов, открытых спецификаций и нормативно-правовых документов, которые описывают выполнение процессов жизненного цикла (далее – ЖЦ) системы в соответствии с какой-либо моделью ЖЦ. Такими документами являются стандарты ЖЦ[7]. В данном случае в силу комплексности выполняемых работ, описанных

выше, технологический профиль – это многоплановый документ, который должен включать также нормативные документы, регламентирующие специфические для систем защиты виды деятельности.

Построение интеграционного профиля

Для обеспечения способности взаимодействовать между собой системы должны обладать свойством интероперабельности (interoperability). Под интероперабельностью понимается «способность двух или более систем или элементов к обмену информацией и к использованию информации, полученной в результате обмена»[8].

Взаимодействие систем любой природы основывается на стеке интероперабельности[9], обобщенный вид которого приведен ниже:

1) политический уровень – предполагает формирование согласованного между партнерами информационного обмена видения достижения общих целей;

2) нормативный уровень – предполагает взаимодействие систем в единой нормативной среде;

3) организационный уровень – относится к организационным аспектам функционирования информационных систем и предполагает интеграцию бизнес-процессов, реализуемых средствами приложений, и регламентов их функционирования;

4) семантический уровень – определяет способность систем одинаково понимать смысл информации, которой они обмениваются;

5) синтаксический уровень – определяет возможность обмена данными, способность систем к интеграции;

6) технический уровень – организация взаимосвязи между системами.

Хотелось бы отметить, что первые 3 уровня стека характеризуют взаимодействие элементов распределенной системы в стратегической и управленческой области.

Три последних уровня «работают» при обеспечении интеграции элементов ИС. Эти уровни легко отображаются компонентами модели OSE/RM. Технический уровень представлен моделью взаимосвязи открытых систем OSI/RM (Open System Interconnection) – столбец «Communication». Для обеспечения синтаксической интероперабельности (уровень 5) необходимо предусмотреть наличие программного средства для активации средств коммуникации столбца «Communication» (компонента 6 рис. 1). К таким средствам в настоящее время относятся:

1. Механизм Web-сервисов, который основывается на следующих стандартах, разработанных консорциумом W3C (World Wide Web Consortium): XML – стандарт описания данных; SOAP – стандарт передачи данных между системами; WSDL – стандарт описания сервисов, в том числе входных и выходных данных; UDDI – стандарт для хранения описаний сервисов и предоставления доступа к описаниям сервисов.

2. Механизм MOM (Message-Oriented Middleware) – программное обеспечение промежуточного слоя, обеспечивающее обмен сообщениями между системами. В настоящее время существуют различные реализации механизма взаимодействия систем на основе сообщений (например: WebSphere MQ, TIBCO, Herald, Hermes, SIENA и др.), поставляемые разными провайдерами.

Для обеспечения семантической интероперабельности приложений (уровень 4) в компоненте 7 (рис. 1) модели OSE/RM должно быть предусмотрено интегрированное средство представления знаний предметных областей, в которых «работают» приложения.

При информационном взаимодействии элементов распределенной информационной системы на сегодняшний день принято рассматривать следующие варианты интеграции:

1) интеграция приложений (Application Integration) – взаимодействие двух или нескольких систем при решении ими одной общей задачи (взаимодействие приложений по управлению);

2) интеграция данных (Data Integration) – взаимодействие двух или нескольких систем с целью использования общих информационных ресурсов, например баз данных или экспорта/импорта данных, содержащихся в отдельных файлах (взаимодействие приложений по данным или интеграция данных);

3) интеграция платформ (Platform Integration) – осуществляется с целью обеспечения безопасного и оптимального обмена информацией между различными приложениями.

Регламентация возможностей программно-аппаратных средств, реализующих свойство интероперабельности компонент СЗ, осуществляется посредством интеграционного профиля. Таким образом, интеграционный профиль гетерогенной инфраструктуры распределенной системы – это документ, включающий профилирование механизмов и средств интероперабельности, а также стандартизованное описание варианта интеграции.

* * *

В статье на методологическом уровне рассмотрены вопросы профилирования системы безопасности распределенной ИС в части функционального назначения системы защиты, интеграционных взаимодействий, управления процессами жизненного цикла системы. Очевидно, что профили системы позволяют фиксировать принятые архитектурные и интеграционные решения. Это обеспечивает: расширяемость и масштабируемость системы по набору защитных механизмов и размерности решаемых задач; возможности функциональной интеграции системы защиты; переносимости приложений между разными аппаратно-программными платформами. Профиль технологический представляет собой стандартизованное описание видов деятельности (процессов) вдоль жизненного цикла системы защиты с учетом единых реперных точек с жизненным циклом целевой системы.

В целом можно сказать, что наличие полного стандартизованного описания ИС и системы защиты к ней как единого объекта способствует улучшению показателя эффективности по соотношению параметров стоимости и качества компонентов обеих систем при их разработке, приобретении, развитии и модернизации.

Примечания

1 GOST P ISO IEC TR 10000-1-99 Information technology. Bases and taxonomy of the international functional standards. Part 1. General provisions and bases of documenting. 1999.

2 *Boichenko A.V., Lukinova Olga*. Functional Standardization of Life Cycle of Information System // Proceedings of the 2016 Conference on Information Technologies in Science, Management, Social Sphere and Medicine. Atlantis Press Amsterdam – Beijing – Paris 2016. № 51.

3 IEEE Std 1003.0-1005, IEEE Guide to the POSIX Open System Enviroment (OSE) – N. Y.: The Institute of Electrical and Electronics Engineers, 1995; ISO/IEC TR 14252:1996. Information Technology. Guide to the POSIX Open System Environment (OSE).

4 GOST P ISO IEC TR 10000-1-99.

5 *Лукинова О.В., Пугачев А.В*. Особенности построения профилей систем безопасности ИС // Открытое образование. 2015. №4. С. 80–87.

6 ГОСТ ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. 2014.

7 GOST 34.601-90. The automated systems. Creation stages; GOST R ISO/IEC 12207-2010. Information technology. Processes of life cycle of software;

GOST P ISO IEC 15288-2005. Information technology. System engineering. Processes of life cycle of systems.

[8] ISO/IEC 24765-Systems and Software Engineering. Vocabulary.

[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services. [Электронный ресурс] URL: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf (дата обращения: 3.08.2017); *Бойченко А.В., Корнеев Д.Г., Лукинова О.В.* Интероперабельность информационных систем на основе стека EIF и модели OSE/RM // Теория активных систем ТАС-2014: Материалы междунар. науч.-практ. конф. 17–19 ноября 2014 г. М., 2014. С. 230–234. [Электронный ресурс] URL: http://www.mtas.ru/upload/library/tas2014/TAS_2014.pdf (дата обращения: 3.08.2017).