О ПРОБЛЕМАХ БЕЗОПАСНОСТИ В КОНТЕКСТЕ ОТКРЫТОЙ СИСТЕМНОЙ АРХИТЕКТУРЫ

А.Р.Дабагов[*], *С.А.Соколов*[**]

[*]*ЗАО «Медицинские Технологии ЛТД»*
[**]*ИРЭ им. В.А.Котельникова РАН*

Расматриваются некоторые вопросы, связанные с обеспечением информационной безопасности в рамках архитектуры, использующей принцип открытых систем.

Безопасность, понимамаемую в самом общем смысле, можно трактовать как объединение, состоящее из следующих (вообще говоря, могущих иметь общие элементы) подмножеств, или аспектов:

- Организационного,
- Политико-правового,
- Экономического,
- Криминологического,
- Информационного.

Под *информационной безопасностью* обычно понимают:

1) Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз, и

2) Состояние информации, информационных ресурсов и информационных систем, при котором в рамках некоторых непротиворечивых правил обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования информации.

Соответственно, *защита информации* (информационная безопасность) — это:

1) Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

2) Комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации.

Под гарантированно защищенной системой будем понимать систему, доказательно удовлетворяющую критериям принятой в организации политики безопасности.

В настоящее время становится все более очевидной важность применения *принципов и технологий открытых систем* [1], понимаемых сейчас в самом широком смысле и обеспечивающих, как мимимум, продление жизненного цикла и уменьшение стоимости производимой продукции. При этом имеются в виду не только собственно информационные системы, но большой класс номенклатур изделий, от ширпотреба до продукции специального назначения[1]. Что касается информационно-телекоммуникационных и вычислительных систем, то «архитектура открытых систем может быть выполнена на основе модели OSI как руководства, следуя которому можно обеспечить требуемые характеристики» (Википедия). На концептуальном уровне одной из основных архитектурных спекцификаций является руководство ISO/IEC TR 14252 [1-3], послужившее основой как для технологии открытых систем в целом [1], так и для ряда связанных с ним документов. Согласно [1] основной принцип открытых систем состоит в создании среды включающей программные и аппаратные средства, службы связи, интерфейсы, форматы данных и протоколы, которая в своей основе имеет развивающиеся, доступные и общепризнанные стандарты и обеспечивает переносимость, взаимодействие и масштабируемость приложений и данных. Сюда, повидимому, следует добавить и продукты с открытым исходным кодом (Open Source, Open Source Architecture – OSA, строящиеся, как правило, на принципах

[1] Так например, доработка комплексов БРПЛ Trident (D5) группой TRIDENT Open System Architecture Team на принципах открытой системной архитектуры позволило существенно увеличить жизненный цикл и сократить стоимость владения (total cost of ownership), сэкономив для МО США 1,2 млрд. долл [4].

открытых систем и использующие доступные общепризнанные стандарты), имеющие ряд преимуществ и востребованные на всех уровнях - от конечного пользователя до государственнных учреждений в ряде стран.

Среди документов, выработанных бюро телекоммуникационных стандартов Международного союза электросвязи (ITU-T, CCITT) серия X представляет собой рекомендации в области сетей передачи данных и коммуникаций в открытых системах, имеющие статус международных стандартов. Из них серия X.800 – X.849 представляет собой рекомендации в области безопасности [2] [3]. К ним, прежде всего, относятся *архитектура безопасности открытых систем* (X.800 и др).

Архитектура безопасности создается для того, чтобы определить для поставщиков сервисов, предприятий и заказчиков глобальные задачи безопасности применительно к окружению открытых систем. Она адресует соображения безопасности для менеджмента, контроля и конечных пользователей, для использования в инфраструктуре, сервисах и приложениях. Архитектура безопасности предоставляет всеохватывающую «сверху-вниз» перспективу окружения (environment) открытой системы и может быть применена к ее элементам, сервисам и приложениям для определения, предсказания и устранения уязвимостей в системе безопасности.

Архитектура безопасности адресует три существенных вопроса:

- какие виды защиты необходимы и против каких угроз,
- какие типы оборудования и группы сервисов должны быть защищены,
- какие типы деятельности должны быть защищены.

Рис. 1. *Архитектура безопасности открытой системы согласно документам серии X.800*

[2] Полный список посвященных вопросам безопасности стандартов ITU-T приведен на сайте IEEE в разделе http://grouper.ieee.org/groups/2600/drafts/June2004-Plan/iTU%20Security

[3] Для краткости мы не рассматриваем здесь документ ISO/IEC 7498-2 по причине практически полного совпадения излагаемого материала.

Эти вопросы адресуются трем компонентам архитектуры: измерениям безопасности (security dimensions), слоям (layers) безопасности, и плоскостям (планам, planes) безопасности. Схематически строение архитектуры безопасности показано на рис. 1.

Как мы видим, на рис. 1 отсутствует раздел требований доверия. В рекомендациях X.800 сказано, что детальное рассмотрение требований доверия, главным образом из-за его сложности, находится вне рассмотрения документа, однако все связанные с безопасностью функции должны быть доверенными.

В технологии открытых систем [1] большое значение имеет понятие *профиля*. Термин «профиль» трактуется сейчас в самых разных смыслах, и часто употребляется в теории защиты информации (профили защиты, профили безопасности). В области безопасности построено уже достаточное количество таких профилей, однако ни один из них не содержит требований открытости [5]. На сегодня существует значительное число теоретических моделей, позволяющих описывать практически все аспекты безопасности и обеспечивать средства защиты формально подтвержденной алгоритмической базой. Однако на практике не всегда удается воспользоваться результатами этих исследований, потому что слишком часто теория защиты не согласуется с реальной жизнью. Теоретические исследования в области ЗИ в информационных системах зачастую носят разрозненный характер и не составляют комплексной теории безопасности [5,6]. Отсутствует общая терминология, которая адекватно бы воспринималась всеми специалистами по теории безопасности. Более того, при рассмотрении ряда специфических информационных процессов исследователи отмечают, что "сегодняшняя экономика покоится на сложных системах, точки уязвимости которых еще не до конца выяснены"[4].

Детальная проработка вопросов безопасности по схеме рис. 1 в методике документа [7] позволит в дополнение к «профилю среды открытой системы организации-пользователя» получить набор требований безопасности в открытой, в т.ч. распределенной системе.

Подход к проектированию Профилей среды открытой системы, заложенный в [7], формулируя бизнес- и технические требования к информационно-телекоммуникационным системам организации-пользователя, может выявить и ряд специфических угроз, которые несет в себе неполное соответствие стандартам или просто принятым между пользователями соглашениям, а также оказать помощь при разработке таких документов как Политика и Задание безопасности, и ряда внутренних документов, необходимых для функционирования информационной системы организации-пользователя.

Оценка защищенности организации-пользователя может быть сделана, учитывая все требования, разработанные для организации-пользователя и исходя из стандартизованных методик на базе стандарта ИСО/МЭК 15408 "Общие критерии оценки безопасности информационных технологий" и имеющихся стандартизованных профилей защиты. Как известно, профили защиты (ПЗ) - одно из основных понятий этого стандарта. В тексте оно определяется следующим образом: "профиль защиты…независимая от реализации совокупность требований безопасности для некоторой категории продуктов или ИТ-систем, отвечающая специфическим запросам потребителя". То-есть, другими словами, под профилями защиты понимаются конкретные наборы требований и критериев для тех или иных продуктов и систем ИТ, выполнение которых необходимо, однако, проверять (требования доверия) [8]. Совместно с Профилем вводится концепция объекта защиты, т.е. набора требований, которые могут быть подготовлены с помощью ПЗ. Профиль защиты допускается создавать как непосредственно для продукта, который представляет собой средство защиты, так и для защитной подсистемы какого-либо программного продукта. Более того, можно написать один профиль для целой совокупности программных продуктов. Так, существуют проекты профилей для межсетевых экранов, СУБД и т. д. Официально принятые профили защиты должны образовать и используемую на практике нормативную базу в области информационной безопасности (ИБ) (ГОСТ Р ИСО/МЭК 15408-3-2002). Эти профили (или их подмножество) должны базироваться на документах, не имеющих противоречий.

Защита информации и специфика угроз безопасности. Итак, защита информации – это обеспечение её безопасности от любых (в т.ч. санкционированных) событий, влекущих за собой ее несанкционированную утрату, модификацию либо хищение. Угрозы, статистика, характер

[4] Ссылку на этот отчет Молландера и др. из корпорации RAND об information warfare мы не смогли обновить (прим. авт.).

нарушений ИБ и др., вообще говоря, несколько меняются во времени. На основе исследования публикуемых данных можно составить примерный список нарушений ИБ и их последствий:

- Утечка информации по техническим каналам: 20%
- Человеческий фактор: 80%

Основные типы нарушений ИБ:

- Хищение, модификация и порча информации
- DOS атаки «отказ в обслуживании»
- Инциденты с вирусами, иными вредоносными программами, в том числе через электронную почту
- Критичные аппаратные отказы, в т.ч. «наведенные»
- Проявления халатности со стороны собственных сотрудников
- Атаки со стороны собственных сотрудников
- Иные причины (ошибки конфигурации, несовпадение стандартов, несоблюдение жизненного цикла систем и др.)

Общий годовой ущерб от нарушений ИБ в мире - более 100 млрд. $ (по оценкам фирмы McAfee 2008 г., до $1 трлн).

По данным Майкрософт, из опрошенных 530 компаний:

Общие убытки от нарушений безопасности – $201 млн. Из них:

- $70 млн. – похищение информации
- $65 млн. – из-за атак типа «отказ в обслуживании»
- $27 млн. – из-за вирусных атак (кроме атак типа «отказ в обслуживании»)
- 82% компаний подвергались вирусным атакам
- 77% компаний подвергались атакам со стороны своих сотрудников
- 40% компаний подвергались атакам со стороны конкурентов

(источник: 2003 CSI/FBI Computer Crime and Security Survey).

Политики безопасности и модели защиты. Среди моделей политик безопасности можно выделить два основных класса: дискреционные (произвольные) и мандатные (нормативные). В документах серии X.800 рекомендована ролевая модель, которая опирается на усовершенствованную модель Харрисона-Руззо-Ульмана, однако ее нельзя отнести ни к дискреционным, ни к мандатным, потому что управление доступом в ней осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов. Поэтому ролевая модель представляет собой особый тип политики, основанной на компромиссе между гибкостью управления доступом, характерной для дискреционных моделей, и жесткостью правил контроля доступа, присущей мандатным моделям [5].

Ценность информации. Как известно, стоимость системы защиты не должна превышать стоимости самой защищаемой информации, для этого необходимо последнюю как-то оценить. Для решения этой задачи вводятся вспомогательные структуры, описывающие ценность информации. Моделей оценки, вообще говоря, две: модель на основе порядковой шкалы ценностей, лежащая в основе государственных стандартов защиты информации (1), и модель, использующая аддитивную оценку и анализ рисков (2) [10].

Согласно (1) производится оценка на основе порядковой шкалы ценностей с введением решетки ценностей относительно бинарного отношения $\leq$ [10]. Этот подход лежит в основе государственных стандартов защиты информации (так называемая решетка MLS - Multilevel Security).

Согласно (2) предполагается, что информация представлена в виде конечного множества элементов. Оценка строится на основе экспертных оценок компонент. При этом строится единая весовая шкала для всех компонент и таким образом определяется суммарная стоимость информации. Оценка возможных потерь строится на основе полученных стоимостей компонент, исходя из прогноза угроз этим компонентам. Возможности угроз оцениваются вероятностями соответствующих событий, а потери подсчитываются как сумма математических ожиданий потерь для компонент по распределению возможных угроз. Рассмотрение потерь в контексте самого проекта, т.е. жизненного цикла самой системы, даст нам методики на основе жизненного цикла, принятого за основу построения профилей среды открытой системы в Р 50.1.041-2002 и заключающиеся в обеспечении бесперебойного функционирования бизнес-процессов организации-пользователя на основе минимизации рисков, связанных с информационной

безопасностью на основе современных концепций управления рисками NIST 800-30, BS 7799 и аналогичных. Согласно стандарту NIST 800-30 система управления рисками должна быть интегрирована в систему управления жизненным циклом ИТ.

Заключительные замечания. Как мы можем видеть, тематика, охват и архитектурные подходы на основе открытых систем сейчас бурно развиваются, так, уже стандартизуется и сертифицируется собственно архитектура предприятий. Наиболее продвинутые разработки в этом направлении представлены консорциумом The Open Group, к настоящему времени выпустившему 9-ю версию своего метода разработки архитектуры предприятий и содержащему ряд весьма полезных решений и рекомендаций [11]. К сожалению, вопросы безопасности и ее «архитектуры» пронизывают все уровни конструкций архитектуры предприятия, все они оказываются связанными. При усложнении архитектуры предприятия связанная с безопасностью сложность возрастает многократно, возникает ряд новых вопросов, которые, вообще говоря, необходимо задавать «на входе» процедуры проектирования. Соответственно возрастает и стоимость, кроме того, истинная цена ошибки может иногда превышать допустимые пределы. Информационно-телекоммуникационную структуру предприятия (или организации, в ее наиболее общем определении, даваемом в [11]), сравнительно несложно построить согласно некоторому плану. Затратно, но возможно также протестировать и аттестовать ее на соответствие всем требованиям безопасности, вытекающим из соответствующей документации (trusted system) и поддерживать ее в этом состоянии. Однако она очевидно не будет охватывать всех аспектов безопасности, более того, для них, по всей вероятности, потребуется также разрабатывать свое особое программно-аппаратное обеспечение. Здесь мы вплотную подходим к понятию архитектуры комплексной безопасности (см. напр. [12]), одной из основ которой также является технология открытых систем [там же]. Подход этот в области обеспечения безопасности представляется нам наиболее плодотворным.

1. Технология открытых систем. Под общей редакцией А.Я.Олейникова.// «Янус-К», М., 2004, 287 стр.
2 *В. Сухомлин*. *НИВЦ МГУ*, учебные материалы конференции «Индустрия Программирования 96», // *http://www.citforum.ru/programming/prg96/sukhomlin.shtml#5*
3. И.К.Ермаков, С.А.Соколов. Полнотекстовая база данных по стандартам открытых систем. //Информационные технологии и вычислительные системы, 3, 2003, с. 33-38.
4. Fleet Ballistic Missile TRIDENT Open System Architecture Team Earns DOD Acquisition Reform Award, // http://www.lockheedmartin.com/news/press_releases/2001/FleetBallisticMissileTRIDENTOpenSys.html
5. М.О.Гусев, С.А.Соколов. Открытые системы и защита информации в академическом институте. //Информационные технологии и вычислительные системы, 3, 2006, с. 69-78.
6. Д.П.Зегжда, А.М.Ивашко. Основы безопасности информационных систем. // М., Горячая линия – Телеком, 2000. 452 стр.
7. З 50.1.041-2002. Руководство по проектированию профилей среды открытой системы организации-пользователя; Руководство по проектированию профилей среды открытой системы, Рекомендации Института инженеров по электротехнике и электронике (IEEE). Пер. с англ. под общей редакцией А.Я.Олейникова. // М., «Янус-К», 2002, 158 стр.
8. Профили защиты на основе "Общих критериев" Аналитический обзор. В.Б. Бетелин (член-корреспондент РАН), В.А. Галатенко, М.Т. Кобзарь, А.А. Сидак, И.А. Трифаленков, бюллетень Jet Info №3 (2003), // в эл. сб. http://www.jetinfo.ru/2003
9. РД Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. // ГТК РФ, 2003
10. А.А.Грушо, Е.Е.Тимонина. Теоретические основы защиты информации. // М., 1996, 188 стр.
11. TOGAF version 9. // http://www.togaf.info.
12. С.А. Прохоров, А.А. Федосеев, В.Ф. Денисов, А.В. Иващенко. Методы и средства проектирования профилей интегрированных систем обеспечения комплексной безопасности предприятий наукоемкого машиностроения. http://window.edu.ru/window_catalog/redir?id=62296&file=13_isokbp.pdf , 2009, 199 стр.