Сравнительный анализ систем безопасности централизованных и распределенных банковских систем обработки информации

Тепляков Анатолий Адамович, директор ЗАО «НТЦ Контакт»

Справка ТБ

Тепляков Анатолий Адамович. Образование высшее, инженер электронной техники. В 1975 году окончил Минский радиотехнический институт, в 1982 — Белорусский институт народного хозяйства по специальности инженер-экономист. Начинал работу в Минском управлении ЦНПО «КАСКАД» инженером. С 1992 по 2003 — директор НТЦ «КОНТАКТ», 2003-2007 — заместитель директора по науке Научно-исследовательского республиканского института технической защиты информации. 2007-2008 — начальник отдела безопасности УП «ИВЦ Минфина», с 2009 — заместитель директора, с 2011 — директор ЗАО «НТЦ КОНТАКТ». С 2000 года — преподаватель Академии управления при Президенте Республики Беларусь. Опыт работы по созданию систем и элементов защиты информации с 1994 года по настоящее время. Руководил разработкой более чем 20 средств и систем защиты информации, которые применяются по сей день. Автор 11 книг и пособий по защите информации.

Системы обработки информации в своем историческом развитии пережили несколько этапов. Сначала для обработки больших информационных массивов применялись майнфреймы — большие универсальные вычислительные машины. Они стоили больших денег, имели большую вычислительную мощность и обслуживали большое число пользователей. Операционная система майнфреймов была одна на всех, приложения и другие программы — тоже. И все это стоило неимоверно дорого.

С течением времени на смену майнфреймам пришли маленькие, мощные (конечно, не настолько мощные, как майнфреймы, но зато дешевые) персональные ЭВМ. Они позволили решать задачи для каждого отдельного пользователя, имели удобные интерфейсы, дешевые операционные системы, системы управления базами данных, коммуникационные пакеты и емкие накопители, объем которых постоянно возрастал. Быстро росли и вычислительные мощности процессоров. Постепенно они становились все больше и больше — причем настолько, что их мощность уже становилась избыточной для персональных вычислений. В это же время появились скоростные каналы связи. ПЭВМ начали объединять в локальные вычислительные сети, которые со временем разрослись до размеров страны. Высокая пропускная способность сетей стала позволять объединять процессоры в мощные локальные комплексы, загрузить которые одиночные пользователи уже не могли — и на сцену опять пришли централизованные вычисления, правда, на другой технологической основе. Как видим, круг замкнулся — но уже на принципиально ином, более высоком технологическом витке.

Достоинства и недостатки централизованных и распределенных вычислений в ограниченных рамках данной статьи мы рассмотрим лишь в одном аспекте, а именно — с точки зрения их влияния на создание системы защиты информации, опираясь на практический опыт одного из старейших разработчиков и производителей средств защиты информации в Республике Беларусь — закрытого акционерного общества «НТЦ Контакт».

Состав защищаемых информационных ценностей в распределенных и централизованных системах обработки информации примерно одинаков. Информационные ценности и в одной и в другой системе одни и те же: для банка — это персональные данные клиентов, классификаторы, справочники, архивы, данные систем защиты и т.п. А вот модели нарушителей в этих системах немного различаются, хотя бы из-за того, что в централизованных системах количество администраторов намного меньше, чем в распределенных.

Сравнение рисков и угроз. В централизованных системах существенными являются угрозы для центра обработки и типового пользователя. Для распределенных систем угрозы будут теми же, плюс угрозы, связанные с межузловыми обменами. При этом следует иметь в виду, что компоненты распределенной системы в узлах частично дублируются, но в ней есть и уникальные данные в узлах, которые могут быть выведены из строя, так что стоимость резервирования из-за большого количества для них высока. Централизованные системы резервировать проще — создается резервный центр, соединяемый с основными скоростными каналами связи. Конечно, затраты на это решение достаточно высоки, но в пересчете на одно рабочее место они значительно ниже, чем в распределенной системе.

Риски для сравнимых угроз в централизованных и распределенных системах приблизительно одинаковы — это риски утечки, искажения, навязывания, подмены информации и т.п. Но в распределенных системах эти риски действуют для множества различных классов пользователей, использующих различные ресурсы, в связи с чем суммарные риски возрастают. Для централизованных систем эти риски стабилизируются и являются фиксированной величиной, их гораздо проще контролировать. Например, в распределенной системе достаточно распространены случаи, когда произошел инцидент, его ликвидировали и никому об этом не сообщили. В централизованных системах это невозможно, поскольку все сведения об инцидентах накапливаются в централизованных журналах.

Кроме того, в распределенных системах чрезвычайно усложнено управление версиями. Часто поддерживается множество версий одного и того же продукта, да и продуктов обычно несколько. Поддержание одних и тех же форматов становится для распределенных систем очень большой проблемой. К примеру, всегда найдется какой-то узел, заявляющий об отсутствии средств для перехода на новую версию. Всегда может возникнуть причина, по которой версионность будет разной, а это значит, что будут неодинаковые форматы, что потребует дополнительных средств на поддержание старых форматов. Учитывая, что уровень безопасности системы определяется самым слабым звеном, синхронизация версий становится одной из важнейших и трудно разрешимых задач распределенных систем. В централизованной системе данная проблема решается просто — каждая новая версия программы инсталлируется автоматически, не требуя дополнитель-

ных организационных и человеческих ресурсов (как пример — реализованная ЗАО «НТЦ КОНТАКТ» автоматическая инсталляция новых версий криптозащиты для одного из белорусских банков).

Сравнение средств и методов защиты. В связи с тем, что риски и угрозы централизованных и распределенных систем различаются, то, безусловно, будут различаться средства и методы защиты. Поскольку, как мы уже говорили, угроз в распределенной системе больше и вероятность их реализации выше, то для нее потребуются средства защиты более высокого уровня, которые должны будут дублироваться. С другой стороны, нужно понимать, что если в распределенной системе отказал весь узел, система все равно работает — она только деградирует. То есть выживаемость распределенных систем при прочих равных условиях всегда выше. Для централизованных же систем нужно использовать дополнительные методы повышения надежности и выживаемости, например, такие, как дублирование, которое позволяет сохранить основные функции в случае отказов. Если взять живой пример из практики ЗАО НТЦ «КОНТАКТ», для решений на основе продуктов SAP AG управление открытыми ключами использует разнесенные серверы для удостоверяющих центров, работающих в режиме горячего резерва, а для исключения разрушения самих хранилищ центров хранения сертификатов их синхронные копии — репозитории — выносятся за пределы защищенной зоны, что приводит к большей устойчивости системы.

Защита от утечки информации по техническим каналам. В настоящее время значение этих каналов для любых систем чаще всего недооценивается. Однако следует иметь в виду, что в последнее время стоимость систем технической разведки сильно снизилась, а их эффективность возросла. Разведывательная аппаратура, которая десять лет назад стоила миллионы и сотни тысяч долларов, сейчас стоит на два-три порядка дешевле, т.е. становится более доступной. А это значит, что к возможности ее использования надо относиться серьезно.

Конечно, здесь основной проблемой является стоимость средств защиты. Чаще всего, в связи с необходимостью больших затрат, технической защитой пренебрегают, выполняя мероприятия по защите только госсекретов.

Если сравнивать централизованную и распределенную системы с точки зрения утечки информации по техническим каналам, то разница между ними очень велика. В распределенной системе средства защиты от утечки нужно ставить в каждой точке обработки, а в централизованной можно поставить сверхнадежную, мощную защиту в одном месте, и расходы для обеспечения одного и того же уровня защищенности одного рабочего места будут на порядок меньше. Например, при разработке ЗАО «НТЦ КОНТАКТ» системы безопасности для централизованной системы обработки данных одного из банков нам было достаточно установить всего 2 устройства защиты ПЭВМ от НСД — ПАК «Барьера» — для защиты корневых сертификатов с учетом наличия основного и резервного центров. Для распределенной системы таких устройств понадобилось бы в разы больше, соответственно, затраты увеличились бы на порядок.

Физическая защита. В централизованных системах физическая защита всегда лучше, поскольку средства затрачиваются на мероприятия, касающиеся небольшого количества пользователей, имеющих физический доступ к системе. Несмотря на то, что затраты на защиту центра больше, экономический эффект при защите централизованной системы выше, что позволяет создавать за те же деньги более качественную защиту. В ЦОДе можно ввести многофакторный контроль (например, веса входящих и видеоконтроль перемещения в защищаемых помещениях) и т.п.

Организационные решения. Конечное количество пользователей будет одинаковым в обеих системах, но в распределенной системе количество администраторов, которые поддерживают управление, естественно, будет больше (на каждом узле по администратору). И, конечно же, обеспечить качество персонала в централизованной системе будет проще, чем в распределенной.

Криптографическая защита. Одна из угроз связана с нарушением конфиденциальности информации. Решением является применение криптографических средств. Они относительно дешевы — при больших партиях составляют порядка 20-30 долларов за рабочее место. При этом основные затраты приходятся на систему управления ключевой информацией. А это значит, логично было бы вывести из отдельно взятого предприятия систему управления открытыми ключами, сделать ее общей для группы организаций. Но каждый здесь должен сам для себя решить, нужен ли ему собственный удостоверяющий центр. На сегодняшний день вся республика разбита на маленькие островки, которые управляют своими ключами сами. Необходимо было бы собрать их в единую систему. Но для создания и существования такой системы основное значение будет иметь стоимость ее сертификатов. Если цена сертификата будет низкой, будет преобладать тенденция к укрупнению систем

USB-СЕЙФ «МЕРКУРИЙ»
СЮИК 466216.001

Идеальный носитель для защищенного хранения личного ключа, участвующего в формировании ЭЦП

Персональное устройство для защиты информации при ее обработке и хранении под управлением ОС MS Windows 2000/XP/2003/Vista/7

Сертификат ОАЦ при Президенте РБ
№ BY/112 03.03/ 036 00159

Принцип работы USB-сейфа «Меркурий»:
Встроенное программное обеспечение защищает секретность и целостность информации путем шифрования **национальными** криптографическими методами по ГОСТ 28147-89

ЗАО НТЦ «КОНТАКТ»
Минск, пер. Студенческий, 7
Тел./факс: (017) 222-73-18

УНП: 100037461

управления ключами. При высокой цене сертификата будет преобладать тенденция к созданию собственных систем управления. Надеяться на то, что в республике может успешно работать монопольная структура, которая будет выпускать сертификаты открытых ключей по 100 долларов США за штуку, сейчас не приходится, поскольку организация, которой нужно 1000 сертификатов в год, конечно же, скорее всего за 100 000 долларов купит собственную систему управления сертификатами и будет тратить один раз в десять лет 1000 долларов на то, чтобы купить один корневой сертификат. Экономя, таким образом, 99900 долларов США в год.

Подводя итог, можно сказать, что и централизованные, и распределенные системы обработки данных имеют свои преимущества и недостатки. Однако можно с уверенностью сказать — постепенно мы идем к централизованным вычислениям, как в малых офисных решениях, так и в больших, масштаба республики, системах. Опыт ЗАО «НТЦ Контакт» показывает преимущества централизованных систем, в том числе и в области защиты информации.

P.S. Надо понимать, что система безопасности — это всего лишь вспомогательный компонент, который помогает экономить средства за счет уменьшения количества инцидентов. Но поскольку финансирование мероприятий по безопасности осуществляется из чистой прибыли, это значит, на каждый рубль, который мы вкладываем в безопасность, мы уже заплатили как минимум два рубля налогов и иных отчислений. Поэтому как только Ваши затраты на систему безопасности начинают «съедать» более 10 процентов от стоимости того, что она защищает, по нашему мнению, ее нужно срочно оптимизировать. ■