Обеспечение безопасного функционирования больших информационных систем

А. Ю. Даниленко

Рассматриваются подходы к доработке информационных систем для обеспечения необходимого уровня защищенности данных.

Введение

Как отмечалось в [1], одной из причин повышенного внимания к проблемам информационной безопасности является необходимость доработки существующих информационных систем для придания им уровня защищенности данных, требуемых законодательством и заказчиками программных комплексов. В частности, серьезное значение приобретает то, что многие организации, как государственные, так и коммерческие, хранят в информационных системах (ИС) данные ограниченного доступа. Особое значение в этих условиях приобретает то обстоятельство, что многие эксплуатируемые сейчас системы были разработаны в то время, когда правила работы с конфиденциальными данными еще не были разработаны или были не столь жесткими.

Строго говоря, закрытая информация хранится в информационных системах государственных ведомств уже десятки лет, однако именно сейчас это становится серьезной проблемой, поскольку прежде работа с этими данными, хранящимися в вычислительных комплексах на основе больших ЭВМ, таких, как ЕС, БЭСМ, IBM, Univac, существенно отличалась от современных стандартов. Доступ к хранящимся в этих системах данным был возможен только через операторов, выполнявших поиск и выдачу данных только по распоряжению руководства,

что означает применение организационных мер защиты. Сейчас в связи с широким распространением персональных ЭВМ легальные пользователи закрытой информации предпочитают работать с ней так же, как они это делают с любыми другим данными, что приводит к необходимости применения специально разрабатываемых технических средств защиты.

Кроме того, в нашей стране успешно используется большое число информационных систем, изначально не предназначенных для обработки и хранения таких данных, в то время как их функциональные возможности желательно использовать в интересах силовых и других государственных ведомств, имеющих дело с закрытой информацией. Все это делает задачу доработки имеющихся информационных систем для обеспечения требуемых уровней защиты данных весьма актуальной.

1. Используемые механизмы защиты

Как известно, под защитой информации понимается решение нескольких взаимосвязанных задач. Это защита данных от несанкционированного доступа, куда входит как разграничение доступа само по себе, так и средства подтверждения подлинности субъекта, обратившегося к данным. Кроме того, требуется обеспечить доступность информации, противодействуя преднамеренному выводу из строя информационных систем. Следующей задачей является обеспечение целостности (неизменности) как хранимых данных, так и программного обеспечения (в первую очередь средств защиты информации — СЗИ). К этим проблемам примыкает аудит — средства протоколирования фактов доступа к данным и других событий в информационной системе, а также средства просмотра протоколов с разграничением прав доступа к их данным.

Рассмотрим кратко основные технические способы решения перечисленных задач [1–3].

- Идентификация и аутентификация (авторизация). Под авторизацией понимается определение субъекта и проверка подлинности предъявленных идентификационных данных.
- Управление доступом (дискреционное, ролевое и мандатное), позволяющее определить доступность информационных объектов для каждого конкретного пользователя.

- Контроль целостности данных.
- Контроль целостности математического обеспечения, в первую очередь входящего в состав СЗИ.
- Электронно-цифровая подпись (ЭЦП) для контроля неизменности данных при передаче и хранении.
- Криптозащита данных, включающая шифрование трафика и данных на жестких дисках, а также вычисление хэш-значений для контроля целостности и формирования ЭЦП.
- Протоколирование (аудит) для контроля действий пользователей и административного персонала, а также для фиксации и последующего анализа попыток взлома системы защиты.
- Защита от неправомерного использования файлов на жестких дисках серверов и клиентских рабочих мест.
- Управление печатью, что включает целый комплекс мер по учету отпечатанных документов и управлению использованием принтеров.
- Контроль экспорта во внешние приложения и копирования файлов в незащищенные области памяти, в том числе на внешние носители, что может привести к утечке информации, хранимой и обрабатываемой в ИС.
- Оповещения административного персонала и блокировки пользователей и объектов ИС в случаях, трактуемых как несанкционированный доступ или нарушение целостности информационных объектов.

Следует отметить, что большинство из перечисленных механизмов защиты данных обычно реализовано в исходной конфигурации ИС, подлежащих доработке. Они являются существенной частью их функционала и часто рассредоточены по всему программному коду системы, что делает задачу оценки их корректности (например, при проведении сертификации) трудно решаемой. Помимо этого, при разработке этих механизмов обычно мало внимания уделяется обеспечению устойчивости их к атакам потенциальных нарушителей, что ведет к тому, что они могут считаться надежной защитой только от самых неквалифицированных злоумышленников. Вследствие этого даже имеющиеся средства защиты требуют серьезной модификации или полной замены с учетом принятых для данной системы моделей угроз и нарушителя. Все эти действия должны быть подкреплены комплексом организационно-технических мер, включающих обучение пользователей и администраторов, подбор администраторов безопасности, физическую защиту оборудования и т. д.

2. Проектирование системы в защищенном исполнении

Основными звеньями в средствах защиты информации являются подсистемы управления доступом и контроля целостности. В случае рассматриваемых информационных систем они должны обеспечивать разграничение доступа и неизменяемость не для объектов операционной системы (файлы и т. д.), а для своих объектов, которые могут иметь весьма сложную структуру (электронные документы, различные записи в базе данных, поисковый индекс). Подсистема управления доступом при этом должна быть спроектирована и разработана таким образом, чтобы реализованные правила не противоречили деловой логике всей системы, легко поддавались проверке и соответствовали требованиям нормативных документов.

При проектировании и разработке защищенной информационной системы особое значение имеет определение среды ее работы и хранения данных, поскольку используемые при работе механизмы ОС и СУБД (сетевые протоколы, средства аутентификации и протоколирования событий, защиты файлов, реестра, записей в таблицах) должны выбираться, исходя из требований устойчивости к известным атакам. Так, операционная система Windows-XP сертифицирована по уровню 1Г классификации ФСТЭК (о классификации требований по безопасности информационных систем см. [4–9]), что означает возможность работы с конфиденциальной информацией при условии соблюдения рекомендуемых требований по настройке ее системы безопасности. В частности, указанная операционная система обеспечивает защиту файлов, записей в реестре и системного журнала событий от сетевых атак и неправомерных действий пользователей, разрабатываемые средства защиты информации должны опираться на эти возможности. Однако, устойчивость к атакам на данные, передаваемые по сети, обеспечивают не все сетевые протоколы, входящие в состав Windows-XP.

Хотя речь идет о доработке готовой системы, проектирование ее защищенного варианта мало отличается от проектирования защищенной системы с нуля. В частности, требуется полноценная проработка модели безопасности, призванной ответить на несколько простых вопросов, от ответов на которые зависит архитектура части, связанной с защитой информации. Правильно и точно сформулированная модель безопасности позволяет достаточно точно оценить необходимые средства защиты, а также после реализации СЗИ проверить корректность выполненной работы. Обычно некоторые фрагменты модели безопасности включаются

в Техническое задание на систему или в отдельное ТЗ на СЗИ, в то время как полное ее изложение является частью Технического или Эскизного проекта системы. Основные разделы модели безопасности перечислены ниже.

- Субъекты защиты. Этот раздел характеризует тех, от кого, собственно, защищается информация. Например, это могут быть легальные пользователи системы, которые пытаются получить привилегии, превосходящие их собственные. Кроме того, возможна постановка задачи, когда система защищается от обслуживающего персонала или случайно зашедших в офис организации посетителей. Здесь же целесообразно определить некоторые привилегии пользователей системы, например, привилегию супервизора, который может читать все данные системы, но не может их изменять. Целесообразно определить полномочия администраторов системы, рассмотреть возможность и целесообразность выделения в отдельную системную роль администраторов безопасности.
- Объекты защиты. Это — полный перечень защищаемых информационных объектов. Например, для системы электронного документооборота это могут быть документы, сообщения почтовой системы, информация о поручениях, исполняемых пользователями, личные расписания пользователей, информация о подготавливаемых ими совещаниях и других мероприятиях. Однако, некоторые информационные объекты могут и не входить в перечень объектов защиты, если утечка или искажение информации о них не существенна для заказчика системы (например, график отпусков или перечень выходных и праздничных дней в организации). Естественно, отсутствие объекта в списке объектов защиты не означает, что он может искажаться или уничтожаться произвольным образом. Работа с ним идет по обычным правилам работы в системе, что обеспечивает его сохранность, но специальных мер по линии СЗИ для его защиты не применяется, поскольку его искажение или получение данных по нему посторонними лицами не ведет к существенному ущербу для организации-заказчика информационной системы.
- Допустимые действия субъектов с объектами. Представляет собой список действий с объектами защиты. Обычно это создание, уничтожение, чтение и модификация объекта. Часто отдельно выделяется изменение прав доступа к объекту, например, изменение списка пользователей, которые могут редактировать содержимое объекта.
- Правила определения допустимости действий. Формулировка правил в этом разделе должна быть достаточно ясной для того, чтобы

проверка их выполнения не приводила к разночтениям в трактовке. Например, право чтения документа имеют те пользователи, которые занесены в список «Читатели» для этого документа. Право создания документов и писем имеют все пользователи системы. При этом положения модели безопасности могут отличаться от деловой логики системы, например, право создания документов может быть ограничено для некоторых их категорий (входящие документы могут регистрировать только работники секретариата). Также с точки зрения СЗИ любой пользователь может отправить письмо любому пользователю системы, тогда как с точки зрения алгоритма работы всей системы в целом отправлять письма директору имеют право только руководители структурных подразделений. Это различие не снижает защищенности данных, поскольку реального несанкционированного доступа к ним не происходит, однако простота правил позволяет точно оценить корректность их реализации.

- Перечень протоколируемых событий в системе. Как уже говорилось выше, протоколирование является одним из способов защиты информации, поэтому перечень событий и определение объема протоколируемых данных — одна из существенных частей проектирования СЗИ. Обычно протоколируются события, связанные с входом пользователей в систему и выходом из нее, изменения в базе данных пользователей (регистрация новых пользователей, помещение их в системные группы). Также протоколируются события, связанные с доступом к объектам защиты: их создание и уничтожение, просмотр пользователями, изменение самих объектов и отдельно прав доступа к ним. Для обеспечения нормальной работы системы необходимо протоколировать и внутрисистемные события — аппаратные сбои, искажения или потерю данных. В протоколы заносятся обычно время события, пользователь, выполняющий действие, определение действия.
- Модель нарушителя, т. е. характеристика потенциального нарушителя, включающая в себя его уровень квалификации, должностное положение, имеющиеся возможности в плане воздействия на систему. Этот пункт важен тем, что для нарушителей разной квалификации и с разными техническими возможностями средства защиты могут радикально отличаться. Так, для недобросовестного коллеги, компьютерная грамотность которого ограничивается умением копировать файлы на дискету, достаточно блокировать рабочую станцию и закрыть сетевой доступ к дискам; для профессионала, занимающе-

гося промышленным шпионажем, нужен хороший замок на дверях серверной и шифрование сетевого трафика средней стойкости.

- Модель угроз, т. е. угрозы защищаемым данным и способы их преодоления. С предыдущим пунктом тесно связано описание предполагаемых угроз защищаемым данным [2]. Полный список угроз должен включать не только перехват сетевых пакетов и похищение компьютера, но и вирусные атаки, атаки типа «Отказ в обслуживании», стихийные бедствия. Следует отметить, что способы преодоления могут быть не только программные, но и организационно-административные меры, а также подбор и обучение персонала.

3. Архитектура СЗИ

Типичная архитектура СЗИ информационной системы представлена на рис. (1). Поскольку для встраивания указанных средств защиты в основную часть программного кода может потребоваться его коренная переработка, наиболее целесообразным вариантом действий представляется их разработка в виде отдельного программного модуля — Диспетчера доступа, предусмотренного требованиями ФСТЭК по 4 классу защищенности для СВТ и выше [9]. Этот модуль располагается между клиентскими приложениями и стандартным сервером системы, перехватывая и анализируя приходящие на сервер запросы, а также ответы сервера клиентским приложениям. Основным недостатком такого подхода следует признать возможное дублирование в рамках Диспетчера доступа отдельных функциональных возможностей, уже реализованных в основной части системы.

Однако, как видно из рисунка, не все рассмотренные средства защиты можно разместить в Диспетчере, некоторые из них должны быть размещены на клиентских рабочих местах. Это модули формирования и проверки ЭЦП, а также средства протоколирования таких действий пользователя, которые выполняются только на клиенте (работа с ЭЦП, печать документов, копирование файлов на внешние носители и другие незащищенные области памяти).

При выборе способов реализации механизмов безопасности ИС необходимо учитывать возможность использования средств, входящих в операционную систему, а также внешних программных модулей. Так, защита файлов на серверах и клиентских местах должна всегда осуществляться средствами ОС; СУБД, как правило, представляет собой внешнюю систему по отношению ИС, а модули контроля целостности данных и управления доступа, непосредственно зависящие от специфики ОС, должны разрабатываться как ее составные части. Особняком в этом ряду стоит криптогра-

Рис. 1

фическая подсистема, основной особенностью которой следует признать высокую алгоритмическую сложность модулей этого класса. Вследствие этого наиболее целесообразным представляется использование внешних криптографических пакетов, прошедших сертификацию и рекомендованных к использованию заказчиком системы. В то же время подсистема протоколирования может быть реализована разработчиками системы как полностью самостоятельно, так и с использованием системного журнала событий. Второй способ реализации дает возможность использовать стандартные средства работы с протоколами в части их просмотра, удаления и назначения средствами ОС прав доступа к записям. Аналогично подсистема авторизации может быть сделана самостоятельно с реализацией собственных механизмов хранения информации о пользователях, включая парольную информацию. Использование для этой цели соответствующего механизма операционной системы позволяет использовать настройки ОС, в частности парольную политику, а также упростить работу пользователей системы, исключив набор системного имени и пароля при входе в ИС.

Доработка информационной системы до необходимого уровня защищенности почти всегда требует внесения изменений в основную часть программы. Это связано с несколькими обстоятельствами, одно из которых — необходимость реализации фрагментов СЗИ в рамках клиентского приложения — рассмотрено выше. Помимо этого может потребоваться ограничение основного функционала исходной системы в части, не соответствующей требованиям политики безопасности. Такие ограничения должны быть реализованы как на уровне сервера системы, так и в клиентских приложениях, что позволит сделать это максимально надежно.

Литература

1. *Даниленко А. Ю.* Защита данных в сложных информационных системах // Информационно-аналитические аспекты в задачах управления: Труды ИСА РАН. / Под ред. В. Л. Арлазарова и Н. Е. Емельянова. М.: Издательство ЛКИ/URSS, 2007. С. 49–58.
2. *Вихорев С.*, *Кобцев Р.* Как определить источники угроз // Открытые системы. № 7–8, 2002.
3. *Галатенко В.* Информационная безопасность // Открытые системы. № 4–6, 1995.
4. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М., 1992.
5. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. М., 2002.
6. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. М., 1992.
7. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. М., 1992.
8. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. М., 1992.
9. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. М., 1992.