Информационная безопасность

В.А. Галатенко
АО "Инфосистемы Джет"
Vladimir.Galatenko@jet.msk.su

Важность проблемы информационной безопасности сейчас, к сожалению, очевидна далеко не для всех. Однако даже небольшого размышления достаточно, чтобы понять ее проблемы и сложность, проистекающие как из сложности и разнородности современных информационных систем, так и из необходимости комплексного подхода к безопасности с привлечением законодательных, административных и программно-технических мер.

Введение

Информационной безопасностью занимаются давно. Первоначально это было прерогативой государственных организаций, имеющих дело с секретной информацией или отвечающих за обеспечение режима секретности. В 1983 году министерство обороны США выпустило книгу в оранжевой обложке с названием "Критерии оценки надежных компьютерных систем" (Trusted Computer Systems Evaluation Criteria, TCSEC) [8], положив тем самым начало систематическому распространению знаний об информационной безопасности за пределами правительственных ведомств. Во второй половине 1980-х годов аналогичные по назначению документы были изданы в ряде европейских стран [9]. В 1992 году в России Гостехкомиссия при Президенте РФ издала серию брошюр, посвященных проблеме защиты от несанкционированного доступа [1-5].

Сегодня в России наблюдается всплеск интереса к информационной безопасности, который объясняется в первую очередь развитием банковского бизнеса (хотя, конечно, в защите нуждаются не только банки). В этих условиях ощущается острая нехватка литературы на русском языке, посвященной данной тематике. Пожалуй, сейчас можно рекомендовать лишь работы [6, 7], в которых превосходно излагаются общие вопросы информационной безопасности. В то же время даже человеку, имеющему практически неограниченный доступ к англоязычной литературе, крайне сложно приобрести навыки, полезные на практике. Как строить безопасные, надежные системы? Как поддерживать режим безопасности? "Оранжевая книга" и издания, следующие в ее фарватере, не дают ответов на эти вопросы, поскольку ориентированы в первую очередь на разработчиков информационных систем, а не на пользователей или-системных администраторов. Конечно, основы знать необходимо, однако от основ до практики - "дистанция огромного размера". Да и оценки важности различных аспектов безопасности в государственных и коммерческих структурах весьма различны.

Все сходятся на том, что защитные мероприятия призваны обеспечить конфиденциальностпь, целостносчпь и доступность информации, однако если для режимных государственных организаций на первом месте стоит конфиденциальность, а целостность понимается исключительно как неизменность информации, то для коммерческих структур, вероятно, важнее всего целостность (актуальность) и доступность данных и услуг по их обработке. По сравнению с государственными, коммерческие организации более открыты и динамичны, поэтому вероятные угрозы для них отличаются и количественно, и качественно.

Данная статья открывает серию публикаций, посвященных информационной безопасности коммерческих систем. В качестве методологической основы для изложения программно-технического аспекта защиты выбран подход клиент/сервер. Это объясняется двумя основными причинами. Во-первых, подход клиент/сервер позволяет провести декомпозицию сложной информационной системы, после чего можно относительно независимо рассматривать вопросы защиты отдельных компонентов (сервисов). Во-вторых, ряд защитных услуг реализуется с помощью серверов в строгом смысле этого слова (пример - сервер аутентификации Kerberos).

Стандарты и рекомендации в области информационной безопасности

Существуют разные мнения по поводу практической применимости классического подхода к информационной безопасности, однако в любом случае необходимо владеть базовыми понятиями, введенными по большей части в работах, выполненных по заказу министерства обороны США.

Знание критериев оценки информационной безопасности способно помочь при выборе и комплектовании аппаратно-программной конфигурации. Кроме того, в своей повседневной работе администратор по безопасности вынужден хотя бы до некоторой степени повторять действия сертифицирующих органов, поскольку обслуживаемая система, скорее всего, время от времени претерпевает изменения и нужно, во-первых, оценивать целесообразность модификаций и их последствия, а во-вторых, соответствующим образом корректировать повседневную практику пользования и администрирования. Если знать, на что обращают внимание при сертификации, то можно сконцентрироваться на анализе критически важных аспектов, экономя время и силы и повышая качество защиты.

Критерии оценки надежных компьютерных систем

"Оранжевая книга" министерства обороны США, называемая так по цвету обложки, была впервые опубликована в августе 1983 года. Само название заслуживает комментария - речь идет не о безопасных, а о надежных системах, причем слово "надежный" трактуется так же, как в сочетании "надежный человек" - человек, которому можно доверять.

"Оранжевая книга" поясняет понятие безопасной системы, которая "управляет, посредством соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, писать, создавать и удалять информацию". Очевидно, однако, что абсолютно безопасных систем не существует, что это абстракция. Любую систему можно "взломать", если располагать достаточно большими материальными и временными ресурсами. Есть смысл оценивать лишь степень доверия, которое разумно оказать той или иной системе.

Основные понятия

В "Оранжевой книге" надежная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Степень доверия, или *надежность* систем, оценивается по двум основным критериям:

- *Политика безопасности* - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь имеет право оперировать с определенными наборами данных. Чем надежнее система, тем строже и-многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Политика безопасности - это активный компонент защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

- *Гарантированность* - мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность может проистекать как из тестирования, так и из проверки (формальной или нет) общего замысла и исполнения системы в целом и ее компонентов. Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. Гарантированность можно считать пассивным компонентом защиты, надзирающим за самими защитниками.

Важным средством обеспечения безопасности является механизм *подотчетности* или *протоколирования.* Надежная система должна фиксировать все события, касающиеся

безопасности, а ведение протоколов дополняется аудитом - анализом регистрационной информации.

Концепция надежной вычислительной базы является центральной при оценке степени гарантированности, с которой систему можно считать надежной. *Надежная вычислительная база* - это совокупность защитных механизмов компьютерной системы в целом, отвечающих за проведение в жизнь политики безопасности. Надежность вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, вводимых административным персоналом. Вообще говоря, компоненты вне вычислительной базы могут не быть надежными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки надежности компьютерной системы достаточно рассмотреть только ее вычислительную базу, которая, как можно надеяться, достаточно компактна.

Основное назначение надежной вычислительной базы - выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами определенных операций над объектами. Монитор проверяет каждое обращение пользователя к программам или данным на предмет их согласованности со списком допустимых действий.

От монитора обращений требуется выполнение трех свойств:

- Изолированность. Монитор должен быть защищен от отслеживания своей работы.

- Полнота. Монитор вызывается при каждом обращении, причем не должно быть способов его обхода.

- Верифицируемость. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, при наличии, конечно, уверенности в полноте тестирования.

Реализация монитора обращений называется *ядром безопасности,* который является основой построения всех защитных механизмов. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Границу надежной вычислительной базы называют *периметром безопасности.* Как уже указывалось, от компонентов, лежащих вне периметра безопасности, вообще говоря, не требуется надежности. С развитием распределенных систем понятию "периметр безопасности" все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что внутри владений, считается надежным, а то, что вне - нет. Связь между внутренним и внешним мирами осуществляют посредством шлюзовой системы, которая по идее способна противостоять потенциально ненадежному или даже враждебному окружению.

Основные элементы политики безопасности

Согласно "Оранжевой книге", политика безопасности должна включать в себя по крайней мере следующие элементы:

- Добровольное управление доступом.
- Безопасность повторного использования объектов.
- Метки безопасности.
- Принудительное управление доступом.

Рассмотрим перечисленные элементы более подробно.

Добровольное управление доступом. Добровольное управление доступом - это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Добровольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту.

С концептуальной точки зрения текущее состояние прав доступа при добровольном управлении описывается матрицей, в строках которой перечислены субъекты, а в столбцах - объекты. В клетках, расположенных на пересечении строк и столбцов, записываются способы доступа, допустимые для субъекта по отношению к объекту - например: чтение, запись, выполнение, возможность передачи прав другим субъектам и т. п.

Очевидно, прямолинейное представление подобной матрицы вследствие ее больших размеров невозможно, да и не нужно, поскольку она разрежена и большинство клеток в ней пусты. В операционных системах более компактное представление матрицы доступа основывается или на структурировании совокупности субъектов (владелец/группа/прочие как в ОС UNIX), или на механизме списков управления доступом, когда матрица представляется по столбцам и для каждого объекта перечисляются субъекты вместе с их правами доступа. За счет использования метасимволов можно компактно описывать группы субъектов, удерживая тем самым размеры списков управления доступом в разумных пределах.

Большинство операционных систем и СУБД реализуют именно добровольное управление доступом. Главное его достоинство - гибкость, главные недостатки - рассредоточенность управления и сложность централизованного контроля, а также оторванность прав доступа от данных, что позволяет копировать секретную информацию в общедоступные файлы.

Безопасность повторного использования объектов. Безопасность повторного использования объектов - важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения секретной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом.

Важно обратить внимание на следующий момент. Поскольку информация о субъектах также представляет собой объект, необходимо позаботиться о безопасности "повторного использования субъектов". Когда пользователь покидает организацию, следует не только лишить его возможности входа в систему, но и запретить доступ ко всем объектам. В противном случае, новый сотрудник может получить ранее использовавшийся идентификатор, а с ним и все права своего предшественника.

Современные интеллектуальные периферийные устройства усложняют обеспечение безопасности повторного использования объектов. Действительно, принтер может буферизовать несколько страниц документа, которые останутся в памяти даже после окончания печати. Необходимо предпринять специальные меры, чтобы "вытолкнуть" их оттуда. Впрочем, иногда организации защищаются от повторного использования слишком ревностно - путем уничтожения магнитных носителей. На практике заведомо достаточно троекратной записи случайных последовательностей бит.

Метки безопасности. Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, метка объекта - степень закрытости содержащейся в нем информации.

Согласно "Оранжевой книге", метки безопасности состоят из двух частей - уровня секретности и списка категорий. Уровни секретности, поддерживаемые системой, образуют упорядоченное множество, которое может выглядеть, например, так:

- совершенно секретно;
- секретно;
- конфиденциально;
- несекретно.

Впрочем, для разных систем набор уровней секретности может различаться.

Категории образуют неупорядоченный набор. Их назначение - описать предметную область, к которой относятся данные. В военном окружении каждая категория может соответствовать, например, определенному виду вооружений. Механизм категорий позволяет разделить информацию по отсекам, что способствует лучшей защищенности. В последующем мы подробно рассмотрим правила принудительного управления доступом, пока же отметим, что субъект не может получить доступ к "чужим" категориям, даже если его уровень благонадежности "совершенно секретно". Специалист по танкам не узнает тактико-технические данные самолетов.

Главная проблема, которую необходимо решать в связи с метками, это обеспечение их целостности. Во-первых, не должно быть непомеченных субъектов и объектов, иначе в меточной безопасности появятся легко используемые бреши. Во-вторых, при любых операциях с данными метки должны оставаться правильными. В особенности это относится к экспорту и импорту данных. Например, печатный документ должен открываться заголовком, содержащим текстовое и/или графическое представление метки безопасности. Аналогично при передаче файла по каналу связи должна передаваться и ассоциированная с ним метка, причем в таком виде, чтобы удаленная система могла ее разобрать, несмотря на возможные различия в уровнях секретности и наборе категорий.

Одним из средств обеспечения целостности меток безопасности является разделение устройств на многоуровневые и одноуровневые. На многоуровневых устройствах может храниться информация разного уровня секретности (точнее, лежащая в определенном диапазоне уровней). Одноуровневое устройство можно рассматривать как вырожденный случай многоуровневого, когда допустимый диапазон состоит из одного уровня. Зная уровень устройства, система может решить, допустимо ли записывать на него информацию с определенной меткой. Например, попытка напечатать совершенно секретную информацию на принтере общего пользования с уровнем "несекретно" потерпит неудачу.

Метки безопасности, ассоциируемые с субъектами, более подвижны, чем метки объектов. Субъект может в течение сеанса работы с системой изменять свою метку, естественно, не выходя за предопределенные для него рамки. Иными словами, он может сознательно занижать свой уровень благонадежности, чтобы уменьшить вероятность непреднамеренной ошибки. Вообще, принцип минимизации привилегий - весьма разумное средство защиты.

Принудительное управление доступом. Принудительное управление доступом основано на сопоставлении меток безопасности субъекта и объекта.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен - читать можно только то, что положено.

Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может писать в секретные файлы, но не может - в несекретные (разумеется, должны также выполняться ограничения на набор категорий). На первый взгляд подобное ограничение может показаться странным, однако оно вполне разумно.Ни при каких операциях уровень секретности информации не должен понижаться, хотя обратный процесс вполне возможен. Посторонний человек может случайно узнать секретные сведения и сообщить их куда следует, однако лицо, допущенное к работе с секретными документами, не имеет права раскрывать их содержание простому смертному.

Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов, на месте которых могут оказаться даже системные администраторы. После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа. В терминах принудительного управления нельзя выразить предложение "разрешить доступ к объекту X еще и для пользователя Y". Конечно, можно изменить метку безопасности пользователя Y, но тогда он скорее всего получит доступ ко многим дополнительным объектам, а не толькок X.

Принудительное управление доступом реализовано во многих вариантах операционных систем и СУБД, отличающихся повышенными мерами безопасности. В частности, такие варианты существуют для SunOS и СУБД Ingres. Независимо от практического использования принципы принудительного управления являются удобным методологическим базисом для начальной классификации информации и распределения прав доступа. Удобнее мыслить в терминах уровней секретности и категорий, чем заполнять

неструктурированную матрицу доступа. Впрочем, в реальной жизни добровольное и принудительное управление доступом сочетается в рамках одной системы, что позволяет использовать сильные стороны обоих подходов.

Подотчетность

Если понимать политику безопасности узко, то есть как правила разграничения доступа, то механизм подотчетности является дополнением подобной политики. Цель подотчетности - в каждый момент времени знать, кто работает в системе и что он делает. Средства подотчетности делятся на три категории:

- идентификация и аутентификация;
- предоставление надежного пути;
- анализ регистрационной информации.

Идентификация и аутентификация. Каждый пользователь, прежде чем получить право совершать какиелибо действия в системе, должен идентифицировать себя. Обычный способ идентификации - ввод имени пользователя при входе в систему. В свою очередь, система должна проверить подлинность личности пользователя, то есть что он является именно тем, за кого себя выдает. Стандартное средство проверки подлинности (аутентификации) - пароль, хотя в принципе могут использоваться также разного рода личные карточки, биометрические устройства (сканирование радужной оболочки глаза или отпечатков пальцев) или их комбинация.

Идентификация и аутентификация - первый и важнейший программно-технический рубеж информационной безопасности. Если не составляет проблемы получить доступ к системе под любым именем, то другие механизмы безопасности, например, управление доступом, очевидно, теряют смысл. Очевидно и то, что без идентификации пользователей невозможно протоколирование их действий. В силу перечисленных причин проверке подлинности должно придаваться первостепенное значение, Существует целая серия публикаций правительственных ведомств США, разъясняющих вопросы аутентификации и, в частности, проблемы, связанные с паролями. Например, декларируется, что пользователю должно быть позволено менять свой пароль, что пароли, как правило, должны генерироваться компьютером, что пользователю должна предоставляться некоторая регистрационная информация (дата и время последнего входа в систему и т.п.).

Предоставление надежного пути. Надежный путь связывает пользователя непосредственно с надежной вычислительной базой, минуя другие, потенциально опасные компоненты системы. Цель предоставления надежного пути - дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Относительно несложно реализовать надежный путь, если используется неинтеллектуальный терминал - достаточно иметь зарезервированную управляющую последовательность, конечно при условии защищенности линии связи между терминалом и системой. В случае общения пользователя с интеллектуальным терминалом, ПК или рабочей станцией задача обеспечения надежного пути становится чрезвычайно сложной, если вообще разрешимой. Как гарантировать, что пользователь взаимодействует с подлинной программой login, а не с "Троянским конем"? Возможно, по этой причине о предоставлении надежного пути упоминают редко, хотя на практике данный аспект весьма важен.

Анализ регистрационной информации. Аудит имеет дело с действиями, событиями, так или иначе затрагивающими безопасность системы. К числу таких событий относятся:

- вход в систему (успешный или нет);
- выход из системы;
- обращение к удаленной системе;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.).

Можно назвать и другие события - например, смену набора регистрируемых действий. Полный перечень событий, потенциально подлежащих регистрации, зависит от избранной политики безопасности и от специфики системы.

Если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. "Оранжевая книга" предусматривает наличие средств выборочного протоколирования, как в отношении пользователей, когда слежение осуществляется только за подозрительными личностями, так и в отношении событий.

Протоколирование помогает следить за пользователями и реконструировать прошедшие события. Слежка важна в первую очередь как профилактическое средство. Можно надеяться, что многие воздержатся от нарушений безопасности, зная, что их действия фиксируются. Реконструкция событий позволяет проанализировать случаи нарушений, понять, почему они стали возможны, оценить размеры ущерба и принять меры по исключению подобных нарушений в будущем.

При протоколировании события записывается по крайней мере следующая информация:

- дата и время события;
- уникальный идентификатор пользователя - инициатора действия;
- тип события;
- результат действия (успех или неудача);
- источник запроса (например, имя терминала);
- имена затронутых объектов (например, открываемых или удаляемых файлов);
- описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта);
- метки безопасности субъектов и объектов события.

Необходимо подчеркнуть важность не только сбора информации, но и ее регулярного и целенаправленного анализа. В плане анализа выгодное положение занимают средства аудита СУБД, поскольку к регистрационной информации могут естественным образом применяться произвольные SQL-запросы. Следовательно, появляется возможность для выявления подозрительных действий применять сложные эвристики.

Гарантированность

Гарантированность - это мера уверенности, с которой можно утверждать, что для проведения в жизнь сформулированной политики безопасности выбран подходящий набор средств и что каждое из этих средств правильно исполняет отведенную ему роль.

В "Оранжевой книге" рассматривается два вида гарантированности - операционная и технологическая. Первая относится к архитектурным и реализационным аспектам системы, а вторая - к методам построения и сопровождения.

Операционная гарантированность включает в себя проверку следующих элементов:

- архитектура системы;
- целостность системы;
- анализ тайных каналов передачи информации;
- надежное администрирование;
- надежное восстановление после сбоев.

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно проводят в жизнь избранную политику безопасности.

Архитектура системы должна способствовать реализации мер безопасности или прямо поддерживать их. Примеры подобных архитектурных решений в рамках аппаратуры и операционной системы - разделение команд по уровням привилегированности, защита различных процессов от взаимного влияния за счет выделения каждому своего виртуального пространства, особая защита ядра ОС.

В принципе меры безопасности не обязательно должны быть заранее встроены в систему - достаточно принципиальной возможности дополнительной установки защитных продуктов. Так, сугубо ненадежная система MS-DOS может быть улучшена за счет средств проверки паролей доступа к компьютеру и/или жесткому диску, за счет борьбы с вирусами путем отслеживания попыток записи в загрузочный сектор CMOS-средствами и т.п. Тем не менее, по-настоящему надежная система должна изначально проектироваться с акцентом на механизмы безопасности.

Среди архитектурных решений, предусматриваемых "Оранжевой книгой", упомянем следующие:

- деление аппаратных и системных функций по уровням привилегированности и контроль обмена информацией между уровнями;
- защита различных процессов от взаимного влияния за счет механизма виртуальной памяти;
- наличие средств управления доступом;
- структурированность системы, явное выделение надежной вычислительной базы, обеспечение компактности этой базы;
- следование принципу минимизации привилегий - каждому компоненту дается ровно столько привилегий, сколько необходимо для выполнения им своих функций;
- сегментация (в частности, сегментация адресного пространства процессов) как средство повышения надежности компонентов.

Целостность системы в данном контексте означает, что аппаратные и программные компоненты надежной вычислительной базы работают должным образом и что имеется аппаратное и программное обеспечение для периодической проверки целостности.

Анализ тайных каналов передачи информации - тема, специфичная для режимных систем, когда главное - обеспечить конфиденциальность информации. Тайным называется канал передачи информации, не предназначенный для обычного использования. Шпионская аналогия - горшок с геранью в окне как сигнал опасности. Различают тайные каналы с памятью и временные (ударение на "ы"). Тайные каналы с памятью используют изменения хранимых объектов. Тайным знаком может быть размер файла, имя файла (составленное, например, из входного имени и пароля атакуемого субъекта), число пробелов между словами и т.д. Тайный канал считается быстрым, если с его помощью можно передавать 100 или более бит в секунду.

Временные каналы передают информацию за счет изменения временных характеристик процессов - времени обработки запроса, например. Когда-то давно мой товарищ, Андрей Ходулев, написал программу, угадывавшую мысли. Точнее, она отгадывала задуманное число (от 1 до 4). Человеку предлагалось в уме проделать определенные вычисления, естественно, не сообщая программе ответ. "Соль" программы состояла в том, что для разных чисел некоторые вычисления проделать легко, а для других - трудно. Анализируя распределение времени, затраченного на вычисления, программа угадывала задуманное число. Человек, сам того не ведая, передавал программе информацию по тайному временному каналу.

Обычно тайные каналы используются не столько для передачи информации от одного злоумышленника другому, сколько для получения злоумышленником сведений от внедренного в систему "Троянского коня".

Не очень понятно, как на практике, в распределенной системе, выявлять тайные каналы (хотя, после выявления пропускную способность оценить можно). Как следует из предыдущего рассмотрения, тайным каналом может служить почти все что угодно, а скорости современных процессоров и периферийных устройств делают опасными даже прямолинейные способы передачи. Вероятно, только для статичной конфигурации можно с разумной полнотой описать возможные тайные каналы передачи информации.

Надежное администрирование в трактовке "Оранжевой книги" означает всего лишь, что должны быть логически выделены три роли: системного администратора, системного

оператора и администратора безопасности. Физически эти обязанности может выполнять один человек, но, в соответствии с принципом минимизации привилегий, в каждый момент времени он должен выполнять только одну из трех ролей. Конкретный набор обязанностей администраторов и оператора зависит от специфики организации.

Надежное восстановление после сбоев - вещь необходимая, однако ее реализация может быть сопряжена с серьезными техническими трудностями. Прежде всего должна быть сохранена целостность информации и, в частности, целостность меток безопасности. В принципе возможна ситуация, когда сбой приходится на момент записи нового файла с совершенно секретной информацией. Если файл окажется с неправильной меткой, информация может быть скомпрометирована. Далее, на период восстановления система не должна оставаться беззащитной. Нельзя допускать промежуточных состояний, когда защитные механизмы полностью или частично отключены, а доступ пользователей разрешен.

Вообще говоря, надежное восстановление включает в себя два вида деятельности: подготовку к сбою (отказу) и собственно восстановление. Подготовка к сбою - это и регулярное выполнение резервного копирования, и выработка планов действий в экстренных случаях, и поддержание запаса резервных компонентов. Восстановление, вероятно, связано с перезагрузкой системы и выполнением ремонтных и/или административных процедур.

Технологическая гарантированность охватывает весь жизненный цикл системы, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы обезопаситься от утечки информации и нелегальных "закладок".

Первое, на что обычно обращают внимание, это тестирование. Изготовитель или поставщик выполняет набор тестов, документирует его и предоставляет на рассмотрение аттестационной комиссии, которая проверяет полноту набора и, быть может, выполняет свои тесты. Вообще говоря, тестированию подлежат как собственно механизмы безопасности, так и пользовательский интерфейс к ним. Тесты должны показать, что защитные механизмы функционируют в соответствии со своим описанием и не существует очевидных способов обхода или разрушения защиты. Тесты должны продемонстрировать действенность средств управления доступом, защищенность регистрационной и аутентификационной информации. Должна быть уверенность, что надежную вычислительную базу нельзя привести в состояние, когда она перестанет обслуживать пользовательские запросы (пожалуй, это единственное упоминание в "Оранжевой книге" такого аспекта информационной безопасности, как доступность или обслуживаемость). Верификация описания архитектуры - это выполненное автоматически формальное доказательство того, что архитектура системы соответствует сформулированной политике безопасности. Национальный центр компьютерной безопасности США располагает двумя системами для проведения подобных формальных доказательств - Gypsy Verification Environment (GVE) компании Computational Logic, Inc. и Formal Development Methodology (FDM) корпорации UNISYS.

Средства конфигурационного управления защищают надежную систему в процессе проектирования, реализации и сопровождения. Конфигурационное управление включает в себя идентификацию, протоколирование и анализ всех изменений, вносимых в надежную вычислительную базу независимо от того, идет ли речь об аппаратуре или программах, а также, что прямо следует из названия, управление процессом внесения изменений.

Конфигурационное управление давно и широко используется разработчиками программного обеспечения отнюдь не только и не столько по соображениям безопасности. Специфика подхода "Оранжевой книги" - в тотальном контроле за изменениями и в строгой дисциплине их проведения.

Надежное распределение защищает систему в процессе ее передачи от поставщика клиенту. Оно включает в себя два комплекса мер - по защите и по проверке. Защитная часть работает на пути от поставщика к клиенту. Она позволяет поставщику утверждать - клиент получил именно то, что поставщик отгрузил; что передана нужная версия, содержащая все

последние изменения, и что по дороге система не была вскрыта и в нее не были внесены коррективы. Среди защитных механизмов - надежная упаковка, предохраняющая от вредного воздействия окружающей среды, надежная транспортировка и, наконец, надежная инсталляция аппаратуры и программ.

Проверочные меры применяются клиентом, чтобы убедиться, что он получил именно то, что заказал, и система не подверглась нелегальным изменениям. Клиент должен убедиться, что полученный им продукт - точная копия эталонного варианта, имеющегося у поставщика. Для этого существует целый спектр методов, начиная от проверок серийных номеров аппаратных компонентов и кончая верификацией контрольных сумм программ и данных. Следует отметить, что современная практика поставки программного обеспечения на CD-ROM существенно затрудняет, по сравнению, например, с поставкой на дискетах, внесение нелегальных изменений.

Документация

Документация - необходимое условие гарантированной надежности системы и, одновременно, инструмент проведения политики безопасности. Без документации люди не будут знать, какой политике следовать и что для этого нужно делать.

Согласно "Оранжевой книге", в комплект документации надежной системы должны входить следующие тома:

- руководство пользователя по средствам безопасности;
- руководство администратора по средствам безопасности;
- тестовая документация;
- описание архитектуры.

Разумеется, на практике требуется еще по крайней мере одна книга - письменное изложение политики безопасности данной организации.

Руководство пользователя по средствам безопасности предназначено для обычных людей, не имеющих каких-либо привилегий доступа к системе. Оно должно содержать сведения о механизмах безопасности и способах их использования. Руководство должно давать ответы, по крайней мере, на следующие вопросы:

- Как входить в систему? Как вводить имя и пароль? Как менять пароль? Как часто это нужно делать? Как выбирать новый пароль?
- Как защищать файлы и другую информацию? Как задавать права доступа к файлам? Из каких соображений это нужно делать?
- Как импортировать и экспортировать информацию, не нарушая правил безопасности?
- Как уживаться с системными ограничениями? Почему эти ограничения необходимы? Какой стиль работы сделает ограничения необременительными?

Руководство администратора по средствам безопасности предназначено и для системного администратора,и для администратора безопасности. В Руководстве освещаются вопросы начального конфигурирования системы, перечисляются текущие обязанности администратора, анализируется соотношения между безопасностью и эффективностью функционирования.

Типичное оглавление Руководства администратора включает в себя следующие пункты:

- Каковы основные защитные механизмы?
- Как администрировать средства идентификации и аутентификации? В частности, как заводить новых пользователей и удалять старых?
- Как администрировать средства добровольного управления доступом? Как защищать системную информацию? Как обнаруживать слабые места?
- Как администрировать средства протоколирования и аудита? Как выбирать регистрируемые события? Как анализировать результаты?
- Как администрировать средства принудительного управления доступом? Какие уровни секретности и категории выбрать? Как назначать и менять метки безопасности?

- Как генерировать новую, переконфигурированную надежную вычислительную базу?

- Как безопасно запускать систему и восстанавливать ее после сбоев и отказов? Как организовать резервное копирование?

- Как разделить обязанности системного администратора и оператора?

Тестовая документация содержит описания тестов и их результаты. По идее она проста, но зачастую весьма пространна. Кроме того (точнее, перед тем), тестовая документация должна содержать план тестирования и требования, предъявляемые к тестовому окружению.

Описание архитектуры в данном контексте должно включать в себя по крайней мере сведения о внутреннем устройстве надежной вычислительной базы. Вообще говоря, это описание должно быть формальным, допускающим автоматическое сопоставление с политикой безопасности на предмет соответствия требованиям последней. Объем описания архитектуры может оказаться сопоставимым с объемом исходных текстов программной реализации системы.

Классы безопасности

"Критерии" министерства обороны США открыли путь к ранжированию информационных систем по степени надежности. В "Оранжевой книге" определяется четыре уровня безопасности - **D** , **C** , **B** и **A** . Уровень D предназначен для систем, признанных неудовлетворительными. В настоящее время он пуст и ситуация едва ли когда-нибудь изменится. По мере перехода от уровня С до А к надежности систем предъявляются все более жесткие требования. Уровни С и В подразделяются на классы (**C1, C2, B1, B2, B 3**) с постепенным возрастанием надежности. Таким образом, всего имеется шесть классов безопасности - C1, C2, B1, B2, B3, A1. Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять оговоренным требованиям.

В данной статье мы не будем останавливаться на подробном описании требований к классам безопасности, а сделаем это позднее, при изложении Руководящих документов Гостехкомиссии при Президенте РФ. Пока отметим лишь, что в "младших" классах политика довольно быстро ужесточается, по существу достигая пика к классу Bl. Напротив, меры гарантированности отнесены в основном в "старшие" классы, начиная с B2. Это подтверждает независимость двух основных групп критериев надежности и методологическую целесообразность их разделения по Европейскому образцу [7].

Распределение требований по классам вызывает ряд конкретных возражений. Неоправданно далеко отодвинуты такие очевидные требования, как извещение о нарушении защиты, конфигурационное управление, безопасный запуск и восстановление после сбоев. Возможно, это оправдано в физически защищенной военной среде, но никак не в коммерческой, когда постоянное слежение за перемещениями сотрудников может быть очень дорогим удовольствием.

Некоторые комментарии

В представленном виде "Критерии" полностью игнорируют коммуникационный аспект, присущий современным распределенным системам. Далее мы покажем, сколь специфична эта область, сколько потенциальных угроз безопасности она содержит, какие новые защитные механизмы следует использовать. Примечательно, что изданные позднее толкования "Критериев" для сетевых конфигураций примерно в три раза толще самой "Оранжевой книги".

Очень важный методологический недостаток "Оранжевой книги" - явная ориентация на производителя и оценщика, а не на покупателя систем. Она не дает ответ на вопрос, как безопасным образом строить систему, как наращивать отдельные компоненты и конфигурацию в целом. "Критерии" рассчитаны на статичные, замкнутые системы, которые, вероятно, доминируют в военной среде, но крайне редки в среде коммерческой. Покупателям нужны более динамичные и структурированные критерии.

Тем не менее следует подчеркнуть, что публикация "Оранжевой книги" без всякого преувеличения стала эпохальным событием в области защиты коммерческих информационных систем. Появился общепризнанный понятийный базис, без которого даже обсуждение проблем безопасности было бы затруднительным. Именно в этом видится главная ценность "Критериев оценки надежных компьютерных систем" министерства обороны США.

Литература

[1] Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. - Москва, 1992.

[2] Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. - Москва, 1992.

[3] Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - Москва, 1992.

[4] 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. - Москва, 1992.

[5] Гостпехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. - Москва, 1992.

[6] Гайкович В., Першин А. Безопасность электронных банковских систем. - Москва, "Единая Европа", 1994.

[7] Левин В.К. Защита информации в информационно-вычислительных системах и сетях. // "Программирование", М 5, 1994, с. 5-16.

[8] Department of Defense Trusted Computer System Evaliation Criteria. - DoD 5200.28-STD, 1993.

[9] lnformation Technology Security Evaluation Criteria (ITSEC). Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom. - Department of Trade and Industry, London, 1991.

Продолжая начатое изложение по основам информационной безопасности остановимся сегодня на версии 1.2 гармонизированных критериев оценки безопасности информационных технологий Information Technology Security Evaluation Criteria, ITSEC), принятые Европейскими странами и опубликованных в июне 1991 года от имени соответствующих органов четырех стран - Франции, Германии, Нидерландов и Великобритании. Далее рассмотрим руководящие документы по защите от несанкционированного доступа, подготовленные Гостехкомиссией при Преэиденте РФ.

Следуя по пути интеграции, европейские страны приняли согласованные критерии оценки безопасности информационных технологий (Information Technology Security Evaluation Criteria, ITSEC). Выгода от использования согласованных критериев очевидна для всех - и для производителей, и для потребителей, и для самих органов сертификации. Принципиально важной чертой "Европейских Критериев" является отсутствие априорных требований к условиям, в которых должна работать информационная система. (Напомним, что в "Критериях" министерства обороны США очевидна привязка к условиям правительственной системы, обрабатывающей секретную информацию.) Так называемый спонсор или организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации - оценить, насколько полно достигаются поставленные цели: корректность и эффективность

архитектуры, а также реализации механизмов безопасности в описанных спонсором условиях. Таким образом, в терминологии "Оранжевой книги", "Европейские Критерии" относятся к гарантированности безопасной работы системы. Требования к политике безопасности и к наличию защитных механизмов не являются составной частью "Критериев". Впрочем, чтобы облегчить формулировку цели оценки, "Критерии" содержат в качестве приложения описание десяти примерных классов функциональности, типичных для правительственных и коммерческих систем.

Гармонизированные критерии Европейских стран. Основные понятия

"Европейские Критерии" рассматривают следующие составляющие информационной безопасности:

- *конфиденциальность* - защита от несанкционированного получения информации;
- *целостность* - защита от несанкционированного изменения информации;
- *доступность* - защита от несанкционированного удержания информации и ресурсов.

В "Критериях" дается определение различия между системами и продуктами. *Система* - это конкретная аппаратнопрограммная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. *Продукт* - это аппаратно-программный "пакет", который можно купить и по своему усмотрению встроить в ту или иную систему. Таким образом, с точки зрения информационной безопасности, основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях. Угрозы безопасности системы носят вполне конкретный и реальный характер, а относительно угроз продукту можно лишь строить предположения. Разработчик имеет возможность специфицировать условия, пригодные для функционирования продукта; дело покупателя обеспечить выполнение этих условий.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем - например, чтобы облегчить и удешевить оценку системы, составленной из ранее сертифицированных продуктов. В этой связи для систем и продуктов вводится единый термин - объект оценки. В соответствующих местах делаются оговорки, какие требования относятся исключительно к системам, а какие - только к продуктам.

Каждая система и/или продукт предъявляет свои требования к обеспечению конфиденциальности, целостности и доступности. Чтобы удовлетворить эти требования, необходимо предоставить соответствующий набор функций или сервисов безопасности, таких как идентификация и аутентификация, управление доступом или восстановление после сбоев. Сервисы безопасности реализуются посредством конкретных механизмов. Например, для реализации функции идентификации и аутентификации можно использовать такой механизм, как сервер аутентификации Kerberos.

Чтобы объект оценки можно было признать надежным, необходима определенная степень уверенности в наборе функций и механизмов безопасности. Степень уверенности будем называть гарантированностью, которая может быть большей или меньшей в зависимости от тщательности проведения оценки.

Гарантированность затрагивает два аспекта - эффективность и корректность средств безопасности. При проверке *эффективности* анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Точнее говоря, рассматриваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных слабых мест защиты. Кроме того, в понятие эффективности входит способность механизмов защиты противостоять прямым атакам (мощность механизма). Определяется три градации мощности - *базовая, средняя и высокая.*

Под *корректностью* понимается правильность реализации функций и механизмов безопасности. В "Критериях" определяется семь возможных уровней гарантированности

корректности в порядке возрастания - от E0 до E6. Уровень E0 обозначает отсутствие гарантированности - аналог уровня D "Оранжевой книги" [1]. При проверке корректности анализируется весь жизненный цикл объекта оценки - от проектирования до эксплуатации и сопровождения.

Общая оценка системы складывается из минимальной мощности механизмов безопасности и уровня гарантированности корректности. Теоретически эти два аспекта независимы, хотя на практике нет смысла проверять правильность реализации "по высшему разряду", если механизмы безопасности не обладают даже средней мощностью.

Функциональность

В "Европейских Критериях" средства, имеющие отношение к информационной безопасности, рассматриваются на трех уровнях детализации. Наиболее абстрактный уровень соответствует общему взгляду только на цели безопасности. На этом уровне дается ответ на вопрос, зачем нужны функции безопасности. Второй уровень содержит спецификации функций безопасности, из которых можно узнать, какая функциональность на самом деле обеспечивается. Наконец, на третьем уровне содержится информация о механизмах безопасности и где уже видно, как реализуется декларированная функциональность.

Спецификации функций безопасности - важнейшая часть описания объекта оценки. "Критерии" рекомендуют выделить в этих спецификациях разделы со следующими заголовками:

- Идентификация и аутентификация.
- Управление доступом.
- Подотчетность.
- Аудит.
- Повторное использование объектов.
- Точность информации.
- Надежность обслуживания.
- Обмен данными.

Большинство из перечисленных тем были рассмотрены при анализе "Оранжевой книги". Сейчас остановимся лишь на моментах, специфичных для "Европейских Критериев".

Под *идентификацией* и *аутентификацией* понимается не только проверка подлинности пользователей в узком смысле, но и функции для регистрации новых пользователей и удаления старых, а также функции для генерации,изменения и проверки аутентификационной информации, в том числе средства контроля целостности. Сюда же относятся функции для ограничения числа повторных попыток аутентификации.

Средства управления доступом также трактуются Европейскими Критериями достаточно широко. В этот раздел помимо прочих попадают функции, обеспечивающие временное ограничение доступа к совместно используемым объектам с целью поддержания целостности этих объектов - мера, типичная для систем управления базами данных. В этом же разделе имеются функции для управления распространением прав доступа и для контроля за получением информации путем логического вывода и агрегирования данных, что также типично для СУБД.

Под *точностью* в "Критериях" понимается поддержание определенного соответствия между различными частями данных (точность связей) и обеспечение неизменности данных при передаче между процессами (точность коммуникаций). Точность выступает как один из аспектов целостности информации.

Функции *надежности обслуживания* должны гарантировать, что действия, критичные по времени, будут выполнены ровно тогда, когда нужно - не раньше и не позже, и что некритичные действия нельзя перевести в разряд критичных. Далее, должна быть гарантия, что авторизованные пользователи за разумное время получат запрашиваемые ресурсы. Сюда же относятся функции обнаружения и нейтрализации ошибок, необходимые

для минимизации простоев, а также функции планирования, позволяющие гарантировать время реакции на внешние события.

К области *обмена данными* относятся функции, обеспечивающие коммуникационную безопасность данных, передаваемых по каналам связи. Здесь" Европейские Критерии" следуют в фарватере рекомендаций X.800, предлагая следующие подзаголовки:

- Аутентификация.
- Управление доступом.
- Конфиденциальность данных.
- Целостность данных.
- Невозможность отказаться от совершенных действий.

Набор функций безопасности может специфицироваться с использованием ссылок на заранее определенные классы функциональности. В "Европейских Критериях" таких классов десять - пять из них (**F-C1, F-C2, F-B1, F-B2, F-B3**) соответствуют классам безопасности "Оранжевой книги".

Класс **F-IN** предназначается для объектов оценки с высокими потребностями по обеспечению целостности данных и программ, что типично для СУБД. При описании класса F-IN вводится понятие роли и выдвигается требование по предоставлению доступа к определенным объектам только с помощью предопределенных процессов. Должны различаться следующие виды доступа: чтение, запись, добавление, удаление, переименование (для всех объектов), выполнение, удаление, переименование (для выполняемых объектов), создание и удаление объектов.

Класс **F-AV** характеризуется повышенными требованиями к доступности. Это существенно, например, для систем управления технологическими процессами. В разделе "Надежность обслуживания" описание этого класса специфицируется следующим образом: объект оценки должен восстанавливаться после отказа отдельного аппаратного компонента таким образом, чтобы все критически важные функции оставались постоянно доступными. То же должно быть верно для вставки отремонтированного компонента, причем после этого объект оценки возвращается в состояние, устойчивое к одиночным отказам. Независимо от уровня загрузки должно гарантироваться время реакции на определенные события и отсутствие тупиков.

Класс **F-DI** характеризуется повышенными требованиями к целостности передаваемых данных. Перед началом общения стороны должны быть в состоянии проверить подлинность друг друга. При получении данных необходима возможность проверки подлинности источника. При обмене данными должны предоставляться средства контроля ошибок и их исправления. В частности, должны обнаруживаться все повреждения или намеренные искажения адресной и пользовательской информации. Знание алгоритма обнаружения искажений должно исключать возможность производить нелегальную модификацию. Попытки воспроизведения ранее переданных сообщений должны обнаруживаться и трактоваться как ошибки.

Класс **F-DC** характеризуется повышенными требованиями к конфиденциальности передаваемой информации. Перед поступлением данных в каналы связи должно автоматически выполняться шифрование с использованием сертифицированных средств. На приемном конце также автоматически производится расшифровка, ключи которой должны быть защищены от несанкционированного доступа.

Класс **F-DX** характеризуется повышенными требованиями и к целостности, и к конфиденциальности информации. Его можно рассматривать как объединение классов F-DI и F-DC с дополнительными возможностями шифрования, действующими из конца в конец, и с защитой от анализа трафика по определенным каналам. Должен быть ограничен доступ к ранее переданной информации, которая в принципе может способствовать нелегальной расшифровке.

Гарантированность эффективности

Для получения гарантий эффективности средств безопасности рассматриваются следующие вопросы:

- Соответствие набора функций безопасности провозглашенным целям, то есть их пригодность для противодействия угрозам, перечисленным в описании объекта оценки;
- Взаимная согласованность различных функций и механизмов безопасности;
- Способность механизмов безопасности противостоять прямым атакам;
- Возможность практического использования слабостей в архитектуре объекта оценки, то есть наличие способов отключения, обхода, повреждения и обмана функций безопасности;
- Возможность небезопасного конфигурирования или использования объекта оценки при условии, что администраторы и/или пользователи имеют основание считать ситуацию безопасной;
- Возможность практического использования слабостей в функционировании объекта оценки.

Важнейшей частью проверки эффективности является анализ слабых мест в защите объекта оценки. Цель анализа - найти все возможности отключения, обхода, повреждения, обмана средств защиты. Оценивается также способность всех критически важных защитных механизмов противостоять прямым атакам - мощность механизмов. Защищенность системы или продукта не может быть выше мощности самого слабого из критически важных механизмов, поэтому в "Критериях" имеется в виду минимальная гарантированная мощность. Для нее определены три уровня: *базовый, средний и высокий.* Мощность можно считать базовой, если механизм способен противостоять отдельным случайным атакам. Мощность можно считать средней, если механизм способен противостоять злоумышленникам с ограниченными ресурсами и возможностями. Наконец, мощность можно считать высокой, если есть уверенность, что механизм может быть побежден только злоумышленником с высокой квалификацией, набор возможностей и ресурсов которого выходит за пределы обыденной практичности.

Важной характеристикой является простота использования продукта или системы. Должны существовать средства, информирующие персонал о переходе объекта в небезопасное состояние (что может случиться в результате сбоя, ошибок администратора или пользователя). Ситуации, когда в процессе функционирования объекта оценки появляются слабости, допускающие практическое использование, в то время как администратор об этом не знает, должны быть исключены. Эффективность защиты признается неудовлетворительной, если выявляются такие слабые места, и они не исправляются до окончания процесса оценки. В таком случае объекту присваивается уровень гарантированности **E0**.

Обратим внимание на то, что анализ слабых мест производится в контексте целей, декларируемых для объекта оценки. Например, можно примириться с наличием тайных каналов передачи информации, если отсутствуют требования к конфиденциальности. Далее, слабость конкретного защитного механизма может не иметь значения, если она компенсируется другими средствами обеспечения безопасности, то есть если механизм не является критически важным.

Гарантированность корректности

При проверке корректности объекта оценки применяются две группы критериев. Первая группа относится к конструированию и разработке системы или продукта, вторая - к эксплуатации. Оцениваются следующие аспекты:

- *Процесс разработки:* требования к объекту оценки; общая архитектура; детализированная архитектура; реализация.
- *Среда разработки:* средства конфигурационного управления; используемые языки программирования и компиляторы; безопасность среды разработки (ее физическая защищенность, методы подбора персонала и т.п.).

- *Эксплуатационная документация:* руководство пользователя; руководство администратора.

- *Операционное окружение:* доставка и конфигурирование системы или продукта; запуск и эксплуатация.

Уровни корректности от **E1** до **E6** выстроены по нарастанию требований к тщательности оценки. Так, на уровне E1 анализируется лишь общая архитектура объекта - вся остальная уверенность может быть следствием функционального тестирования. На уровне E3 к анализу привлекаются исходные тексты программ и схемы аппаратуры. На уровне E6 требуется формальное описание функций безопасности, общей архитектуры, а также модели политики безопасности. В общем случае распределение требований по уровням гарантированности в "Европейских Критериях" соответствует аналогичному распределению для классов безопасности C1-A1 из "Оранжевой книги".

Руководящие документы по защите от несанкционированного доступа Гостехкомиссии при Президенте РФ

В 1992 году Гостехкомиссия при Президенте РФ опубликовала "Руководящих документов", посвященных проблеме защиты от несанкционированного доступа (НСД) к информации, обрабатываемой средствами вычислительной техники (СВТ) и автоматизированными системами (АС) [2-6]. Рассмотрим важнейшие из них.

Концепция защиты от несанкционированного доступа к информации

Идейной основой набора "Руководящих документов" является "Концепция защиты СВТ и АС от НСД к информации". Концепция "излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от НСД, являющейся частью общей проблемы безопасности информации".

Мы позволим себе многостраничное цитирование Руководящих документов по двум причинам. Во-первых, данные требования, несомненно, важны с практической точки зрения. Лица, отвечающие за информационную безопасность, должны сопоставлять свои действия с Руководящими указаниями, чтобы обеспечить систематичность защитных мер. Во-вторых, брошюры Гостехкомиссии при Президенте РФ являются библиографической редкостью, и ознакомиться с ними в подлиннике затруднительно.

В "Концепции" различаются понятия средств вычислительной техники и автоматизированной системы, аналогично тому, как в "Европейских Критериях" проводится деление на продукты и системы. Более точно, "Концепция предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от НСД. Это - направление, связанное с СВТ, и направление, связанное с АС. Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации.

Помимо пользовательской информации при создании автоматизированных систем появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации."

Существуют различные способы покушения на информационную безопасность: радиотехнические, акустические, программные и т.п. Среди них НСД выделяется как "доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС."

В "Концепции" формулируются следующие основные принципы защиты от НСД к информации:

"...Защита СВТ обеспечивается комплексом программно-технических средств.

Защита АС обеспечивается комплексом программнотехнических средств и поддерживающих их организационных мер.... Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта,включая технические решения и практическую реализацию средств защиты.

Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами."

"Концепция" ориентируется на физически защищенную среду, проникновение в которую посторонних лиц считается невозможным, поэтому нарушитель определяется как "субъект, имеющий доступ к работе с штатными средствами АС и СВТ как части АС.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей.

Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС - запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

В своем уровне нарушитель является специалистом высшей квалификации, знает все о АС и, в частности, о системе и средствах ее защиты."

В качестве главного средства защиты от НСД к информации в "Концепции" рассматривается система разграничения доступа (СРД) субъектов к объектам доступа. Основными функциями СРД являются:

- "реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;
- реализация ПРД субъектов и их процессов к устройствам создания твердых копий;
- изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
- управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;
- реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам."

Кроме того, "Концепция" предусматривает наличие обеспечивающих средств для СРД, которые выполняют следующие функции:

- "идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
- регистрацию действий субъекта и его процесса;

- предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;

- реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;

- тестирование;

- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;

- учет выходных печатных и графических форм и твердых копий в АС;

- контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств."

Видно, что функции системы разграничения доступа и обеспечивающих средств, предлагаемые в "Концепции", по своей сути близки к аналогичным положениям "Оранжевой книги". Это вполне естественно, поскольку близки и исходные посылки - защита от несанкционированного доступа к информации в условиях физически безопасного окружения.

Технические средства защиты от НСД, согласно "Концепции", должны оцениваться по следующим основным параметрам:

- "степень полноты охвата ПРД реализованной СРД и ее качество;

- состав и качество обеспечивающих средств для СРД;

- гарантии правильности функционирования СРД и обеспечивающих ее средств."

Здесь просматривается аналогия с гарантированностью эффективности и корректности в европейских гармонизированных критериях, что можно только приветствовать.

Классификация СВТ по уровню защищенности от НСД

Переходя к рассмотрению предлагаемой Гостехкомиссией при Президенте РФ классификации средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации, отметим ее близость к классификации "Оранжевой книги". Процитируем соответствующий "Руководящий документ".

"...устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс - седьмой, самый высокий - первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;

- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

- четвертая группа характеризуется верифицированной защитой и содержит только первый класс."

Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, однако при оценке защищенность СВТ оказалась ниже уровня требований шестого класса. В таблице 1 приведены распределения показателей защищенности по шести классам СВТ.

Таблица 1. Распределение показателей защищенности по шести классам СВТ.

Наименование показателя	**Класс защищенности**					
	6	**5**	**4**	**3**	**2**	**1**
1. Дискреционный принцип контроля доступа	+	+	+	=	+	=
2. Мандатный принцип контроля доступа	-	-	+	=	=	=
3. Очистка памяти	-	+	+	+	=	=
4. Изоляция модулей	-	-	+	=	+	=

5. Маркировка документов	-	-	+	=	=	=
6. Защита ввода и вывода еа отчуждаемый физический носитель информации	-	-	+	=	=	=
7. Сопоставление пользователя с утройством	-	-	+	=	=	=
8. Идентификация и аутентификация	+	=	+	=	=	=
9. Гарантии проектирования	-	+	+	+	+	+
10. Регистрация	-	+	+	+	+	+
11. Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
12. Надежное восстановление	-	-	-	+	=	=
13. Целостность КСЗ	-	+	+	+	=	=
14. Контроль модификации	-	-	-	-	+	=
15. Контроль дистрибуции	-	-	-	-	+	=
16. Гарантии архитектуры	-	-	-	-	-	+
17. Тестирование	+	+	+	+	+	=
18. Руководство пользователя	+	=	=	=	=	=
19. Руководство по КСЗ	+	+	=	+	+	=
20. Тестовая документация	+	+	+	+	+	=
21. Конструкторская (проектная) документация	+	+	+	+	+	+

Обозначения:
"-" - нет требований к данному классу; "+" - новые или дополнительные требования; "=" - требования совпадают с требованиями к СВТ предыдущего класса; "КСЗ" - комплекс средств защиты.

Классификация автоматизированных систем по уровню защищенности от НСД

Классификация автоматизированных систем устроена иначе. Снова обратимся к соответствующему "Руководящему документу".

"...устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

... Третья группа классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А." В таблице 2 собраны требования ко всем девяти классам защищенности АС.

Таблица 2.
Требования к защищенности автоматизированных систем.

Классы	**Подсистемы и требования**								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
1. Подсистема управления доступом									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:									

в систему;	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-	+	+	+	+
к программам;	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей.	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации.	-	-	-	+	-	-	+	+	+
2. Подсистема регистрации и учета									
2.1. Регистрация и учет:									
входа/выхода субъектов доступа в/из системы (узла сети);	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов;	-	+	-	+	-	+	+	+	+
запуска/завершения программ и процессов (заданий, задач);	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая из создания и удаления, передачу по линиям и каналам связи;	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа.	-	-	-	+	-	-	+	+	+
2.2. Учет носителей информации.	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты.	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема									
3.1. Шифрование конфиденциалной информации.	-	-	-	+	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.	-	-	-	-	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств.	-	-	-	+	-	-	-	+	+
4. Подсистема обеспечения целостности									
4.1. Обеспечения целостности программных средств и обрабатываемой информации.	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС.	-	-	-	+	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты.	-	+	-	+	-	-	+	+	+

Обозначения:

"- " - нет требований к данному классу; "+" - есть требования к данному классу; "СЗИ НСД" - система защиты информации от несанкционированного доступа.

На врезке слева приведено подробное изложение требований к достаточно представительному классу защищенности - 1В.

По существу, перед нами - минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность защищаемой информации.

Литература

[1] Владимир Галатенко. Информационная безопасность // "Открытые системы", # 4, 1995.

[2] Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. - Москва, 1992.

[3] Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. - Москва, 1992.

[4] Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - Москва, 1992.

[5] 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. - Москва, 1992.

[6] Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. - Москва, 1992.

ТРЕБОВАНИЯ К КЛАССУ ЗАЩИЩЕННОСТИ 1В

Подсистема управления доступом:

- должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и/или адресам;
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Подсистема регистрации и учета:

- должна осуществляться регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова;
- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию;
- должна осуществляться регистрация запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;
- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;
- должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа;
- должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;
- должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки;
- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двухкратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;

- должна осуществляться сигнализация попыток нарушения защиты.

Подсистема обеспечения целостности:

- должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды, при этом:
- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ,
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке и (или) хранении защищаемой информации;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
- должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминами и необходимые средства оперативного контроля и воздействия на безопасность АС;
- должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в год;
- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НОД и их периодическое обновление и контроль работоспособности;
- должны использоваться сертифицированные средства защиты."

Термины и определения из Руководящего документа Гостехкомиссии России "Защита от несанкционированного доступа к информации"

Порядок следования и нумерация терминов соответствует официальному документу.

1. Доступ к информации, Доступ, Access to information - Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации

2. Правила разграничения доступа (ПРД), Security policy - Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

3. Санкционированный доступ к информации, Authorized access to information - Доступ к информации, не нарушающий правила разграничения доступа

4. Несанкционированный доступ к информации (НСД), Unauthorized access to information - Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами, Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем

5. Защита от несанкционированного доступа, Защита от НСД, Protection from unauthorized access - Предотвращение или существенное затруднение несанкционированного доступа

6. Субъект доступа, Субъект, Access subject - Лицо или процесс, действия которых регламентируются правилами разграничения доступа

7. Объект доступа, Объект, Access object - Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами

8. Матрица доступа, Access matrix - Таблица, отображающая правила разграничения доступа

9. Уровень полномочий, Subject privilege - Совокупность прав доступа субъекта субъекта доступа доступа

10. Нарушитель правил разграничения доступа, Нарушитель ПРД, Security policy violator - Субъект доступа, осуществляющий несанкционированный доступ к информации

11. Модель нарушителя правил разграничения доступа, Модель нарушителя ПРД, Security policy violater's model - Абстрактное (формализированное или неформализованное) описание нарушителя правил разграничения доступа

12. Комплекс средств защиты КСЗ, Trusted computing base - Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации

13. Система разграничения доступа (СРД), Security poticy realization - Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах

15. Идентификация, Identification - Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов

16. Пароль, Password - Идентификатор субъекта доступа, который является его (субъекта) секретом

17. Аутентификация, Authentication - Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности

20, Модель защиты, Protection model - Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и/или организационных мер защиты от несанкционированного доступа

21. Безопасность информации, Information security - Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз

22. Целостность информации, Information integrity - Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения {разрушения)

23. Конфиденциальная информация, Sensitive information - Информация, требующая защиты

24. Дискреционное управление доступом, Discretionary access control - Разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту

25. Мандатное управление доступом, Mandatory access control - Разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности

26. Многоуровневая защита, Multilevel secure - Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности

27. Концепция диспетчера доступа, Reference monitor concept - Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам

28. Диспетчер доступа, Security kernel - Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа; ядро защиты

35. Система защиты информации от несанкционированного доступа (СЗИ НСД), System of protection from unauthorized access to information - Комплекс организационных мер и программно технических (в том числе криптографических) средств зашиты от несанкционированного доступа к информации в автоматизированных системах

36. Средство криптографической защиты информации (СКЗИ), Cryptographic information protection facility - Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности

"Оранжевая книга" Министерства обороны США и Руководящие документы Гостеккомиссии при Президенте РФ создавались в расчете на централизованные конфигурации, основу которых составляют большие машины. Распределенная организация современных информационных систем требует внесения существенных изменений и дополнений как в политику безопасности, так и в способы проведения ее в жизнь. Для противодействия новым угрозам безопасности нужны и новые функции и механизмы защиты. Продолжая начатое в предыдущих номерах журнала [1,2] изложение по основам информационной безопасности остановимся сегодня на особенностях безопасной работы с компьютерными сетями. Основополагающим документом в области защиты распределенных систем стали Рекомендации X.800 [3]. В данном разделе мы рассмотрим эту работу, а также интерпретацию "Критериев" Министерства обороны США для сетевых конфигураций [4].

Рекомендации X.800

Рекомендации X.800 - документ довольно обширный, поэтому сосредоточим внимание только на специфических сетевых функциях или сервисах безопасности и на необходимых для их реализации защитных механизмах. Одновременно имеет смысл познакомится с основными понятиями данной области информационной безопасности.

Чтобы почувствовать специфику распределенных систем, достаточно рассмотреть такое стандартное средство защиты, как подотчетность. Помимо других целей, записи в регистрационном журнале могут служить доказательством того, что определенный пользователь совершил то или иное действие (точнее, действие было совершено от его имени). В результате пользователь не может отказаться от содеянного и в некоторых случаях несет за это наказание. В распределенных системах действие порой совершается на нескольких компьютерах, и, вообще говоря, не исключено, что их регистрационные журналы противоречат друг другу. Так бывает, когда злоумышленнику удается подделать сетевой адрес и имя другого пользователя - значит, нужны иные средства обеспечения "неотказуемости" (невозможности отказаться) от совершенных действий.

Функции безопасности

Перечислим функции безопасности, характерные для распределенных систем, и роли, которые они могут играть.

Аутентификация. Данная функция обеспечивает аутентификацию партнеров по общению и аутентификацию источника данных.

Аутентификация партнеров по общению используется при установлении соединения или иногда периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи.

Аутентификация источника данных - это подтверждение подлинности источника отдельной порции данных. Функция не обеспечивает защиты против повторной передачи данных.

Управление доступом. Управление доступом обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

Конфиденциальность данных. Данная функция обеспечивает защиту от несанкционированного получения информации. Различают следующие виды конфиденциальности:

- конфиденциальность данных при общении с установлением соединения (в этом и следующем случаях защищаются вся пользовательская информация);
- конфиденциальность данных при общении без установления соединения;
- конфиденциальность отдельных полей данных (избирательная конфиденциальность);
- конфиденциальность трафика (защита информации, которую можно получить, анализируя трафик).

Целостность данных. Данная функция подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры - с установлением соединения или без такового, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

Неотказуемость. Данная функция невозможности отказаться от совершенных действий обеспечивает два вида услуг:

- неотказуемость с подтверждением подлинности источника данных;
- неотказуемость с подтверждением доставки.

Побочным продуктом неотказуемости является аутентификация источника данных.

В таблице 1 указаны уровни эталонной семиуровневой модели OSI, на которых могут быть реализованы функции безопасности. Отметим, что прикладные процессы в принципе могут взять на себя поддержку всех защитных сервисов.

Таблица 1.

Распределение функций безопасности по уровням эталонной семиуровневой модели OSI.

Функции безопасности	**Уровень**						
	1	2	3	4	5	6	7
Аутентификация	-	-	+	+	-	-	+
Управление доступом	-	-	+	+	-	-	+
Конфиденциальность соединения	+	+	+	+	-	+	+
Конфиденциальность вне соединений	-	+	+	+	-	+	+
Избирательная конфиденциальность	-	-	-	-	-	+	+
Конфиденциальность трафика	+	-	+	-	-	-	+
Целостность с восстановлением	-	-	-	+	-	-	+
Целосность без восстановления	-	-	+	+	-	-	+
Избирательная целостность	-	-	-	-	-	-	+
Целостность вне соединения	-	-	+	+	-	-	+
Неотказуемость	-	-	-	-	-	-	+

Обозначени: "+" - данный уровень может предоставить функцию безопасности; "-" - уровень не подходит для предоставления функции безопасности.

Механизмы безопасности

Для реализации функций безопасности могут использоваться следующие механизмы и их комбинации.

Шифрование. Шифрование подразделяется на симметричное с секретным ключом, когда знание ключа шифрования влечет знание ключа расшифровки, и асимметричное с открытым ключом, когда знание ключа шифрования не позволяет узнать ключ расшифровки.

Различают также обратимое и необратимое шифрование. Последнее может использоваться для вычисления криптографических контрольных сумм (хэш-функций, дайджестов, имитовставок).

Электронная подпись. Механизм электронной подписи включает в себя две процедуры:

- выработку подписи;
- проверку подписанной порции данных.

Процедура выработки подписи использует информацию, известную только лицу, визирующему порцию данных. Процедура проверки подписи является общедоступной, она не должна позволять найти секретный ключ подписывающего.

Механизмы управления доступом. При принятии решений о предоставлении запрашиваемого типа доступа могут использоваться следующие виды и источники информации:

- Базы данных управления доступом. В такой базе, поддерживаемой централизованно, или на оконечных системах могут храниться списки управления доступом или структуры аналогичного назначения.
- Пароли или иная аутентификационная информация.
- Токены, билеты или иные удостоверения, предъявление которых свидетельствует о наличии прав доступа.
- Метки безопасности, ассоциированные с субъектами и объектами доступа.
- Время запрашиваемого доступа.
- Маршрут запрашиваемого доступа.
- Длительность запрашиваемого доступа.

Механизмы управления доступом могут располагаться у любой из общающихся сторон или в промежуточной точке. В промежуточных точках целесообразно проверять права доступа к коммуникационным ресурсам. Очевидно, что требования механизма, расположенного на приемном конце, должны быть известны заранее, до начала общения.

Механизмы контроля целостности данных. Различают два аспекта целостности: целостность отдельного сообщения, или поля информации, и целостность потока сообщений, или полей информации. Вообще говоря, контроль двух видов целостности осуществляется различными механизмами, хотя контролировать целостность потока, не проверяя отдельные сообщения, едва ли имеет смысл.

Процедура контроля целостности отдельного сообщения, или поля, включает в себя два процесса: один на передающей стороне, другой - на приемной. На передающей стороне к сообщению добавляется избыточная информация, которая является функцией от сообщения (та или иная разновидность контрольной суммы). На приемной стороне независимо генерируется контрольная сумма полученного сообщения с последующим сравнением результатов. Данный механизм сам по себе не защищает от дублирования сообщений.

Для проверки целостности потока сообщений: защиты от кражи, переупорядочивания, дублирования и вставки сообщений - используются порядковые номера, временные штампы, криптографическое связывание, при котором результат шифрования очередного сообщения зависит от предыдущего, или иные аналогичные приемы.

При общении в режиме без установления соединения использование временных штампов может обеспечить ограниченную форму защиты от дублирования сообщений.

Механизмы аутентификации. Аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов - когда демонстрируется знание секретного ключа, устройств измерения и анализа биометрических характеристик.

Аутентификация бывает односторонней, когда клиент обычно доказывает свою подлинность серверу, и двусторонней, или взаимной. Пример односторонней аутентификации - процедура входа пользователя в систему.

Для защиты от дублирования аутентификационной информации могут использоваться временные штампы и синхронизация часов в узлах сети.

Механизмы дополнения трафика. Механизмы дополнения трафика эффективны, разумеется, только в сочетании со средствами обеспечения конфиденциальности, поскольку в противном случае злоумышленнику будет очевиден фиктивный характер дополнительных сообщений.

Механизмы управления маршрутизацией. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными.

Механизмы нотаризации. Механизм нотаризации служит для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, которая обладает

достаточной информацией, чтобы ее подтверждению можно было доверять. Обычно нотаризация опирается на механизм электронной подписи.

В таблице 2 сведены функции и механизмы безопасности, а также показано, какие отдельные механизмы или их комбинации с другими могут использоваться для реализации той или иной функции.

Таблица 2. Взаимосвязь функций и механизмов безопасности.

Механизмы/Функции безопасности	**Шифрование подписи**	**Электронный трафик**	**Управление доступом**	**Целостность**	**Аутентификация**	**Дополнение**	**Управление маршрутизацией**	**Нотаризация**
Аутентификация партнеров	+	+	-	-	+	-	-	-
Аутентификация источника	+	+	-	-	-	-	-	-
Управление доступом	-	-	+	-	-	-	-	-
Конфиденциальность	+	-	-	-	-	-	+	-
Избирательная конфиденциальность	+	-	-	-	-	-	-	-
Конфиденциальность трафика	+	-	-	-	-	+	+	-
Целостность соединения	+	-	-	+	-	-	-	-
Целостность вне соединения	+	+	-	+	-	-	-	-
Неотказуемость	-	+	-	+	-	-	-	+

Обозначения: "+" - механизм пригоден для реализации данной функции безопасности; "-" - механизм не предназначен для реализации данной функции безопасности.

Администрирование средств безопасности

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы функций и механизмов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение криптографических ключей, установка значений параметров защиты, ведение регистрационного журнала и т.п.

Концептуальной основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое, распределенное хранилище, но каждая из оконечных систем должна располагать информацией, необходимой для проведения в жизнь избранной политики безопасности.

Усилия администратора средств безопасности должны распределяться по трем направлениям:

- администрирование системы в целом;
- администрирование функций безопасности;

- администрирование механизмов безопасности.

Среди действий, относящихся к системе в целом, отметим поддержание актуальности политики безопасности, взаимодействие с другими административными службами, реагирование на происходящие события, аудит и безопасное восстановление.

Администрирование функций безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для реализации функции безопасности, взаимодействие с другими администраторами для обеспечения согласованной работы.

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов. Типичный список имеет следующий вид:

- Управление ключами (генерация и распределение). Вероятно, многие аспекты управления ключами, например их доставка, выходят за пределы среды OSI.
- Управление шифрованием: установка и синхронизация криптографических параметров. К управлению шифрованием можно отнести и администрирование механизмов электронной подписи. Управление целостностью, если оно обеспечивается криптографическими средствами, также тяготеет к данному направлению.
- Администрирование управления доступом (распределение информации, необходимой для управления - пароли, списки доступа и т. п.).
- Управление аутентификацией (распределение информации, необходимой для аутентификации - паролей, ключей и т. п.).
- Управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений - частоту отправки, размер и т. п.). Характеристики могут варьироваться по заданному закону в зависимости от даты и времени.
- Управление маршрутизацией (выделение надежных путей).
- Управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Мы видим, что администрирование средств безопасности в распределенной среде имеет много особенностей по сравнению с централизованными системами.

Интерпретация "Оранжевой книги" для сетевых конфигураций

В 1987 году Национальный центр компьютерной безопасности США выпустил в свет интерпретацию "Оранжевой книги" для сетевых конфигураций [4]. Данный документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

Интерпретация

В первой части вводится минимум новых понятий. Важнейшее из них - сетевая надежная вычислительная база, распределенный аналог надежной вычислительной базы изолированных систем. Сетевая надежная вычислительная база формируется из всех частей всех компонентов сети, обеспечивающих информационную безопасность. Надежная сетевая система должна обеспечивать такое распределение защитных механизмов, чтобы общая политика безопасности проводилась в жизнь несмотря на уязвимость коммуникационных путей и параллельную, асинхронную работу компонентов.

Не существует прямой зависимости между вычислительными базами компонентов, рассматриваемых как изолированные системы, и фрагментами сетевой вычислительной базы. Более того, нет прямой зависимости и между уровнями безопасности отдельных компонентов и уровнем безопасности всей сетевой конфигурации. Например, в результате объединения двух систем класса B1, обладающих несовместимыми правилами кодирования меток безопасности, получается сеть, не удовлетворяющая требованию обеспечения целостности меток. В качестве противоположного примера рассмотрим объединение двух компонентов, один из которых не обеспечивает сам протоколирование действий пользователя, но передает необходимую информацию другому компоненту, который и ведет

протокол. В таком случае сеть в целом, несмотря на слабость компонента, удовлетворяет требованию подотчетности.

Чтобы понять суть положений, вошедших в первую часть, рассмотрим интерпретацию требований к классу безопасности С2. Первое требование - это поддержка добровольного управления доступом. "Интерпретация" предусматривает различные варианты распределения сетевой надежной вычислительной базы по компонентам и, соответственно, различные варианты распределения механизмов управления доступом. В частности, некоторые компоненты, закрытые от прямого доступа пользователей (например, коммутаторы пакетов, оперирующие на третьем уровне семиуровневой модели OSI), могут вообще не содержать подобных механизмов.

Пользователь осуществляет доступ к удаленному ресурсу посредством суррогатного процесса, выполняющегося на удаленной системе от его имени. Данный процесс подвергается стандартным локальным процедурам контроля доступа. "Интерпретация" предусматривает различные способы ассоциирования идентификатора пользователя с суррогатным процессом. Может существовать единая идентификационная база данных, доступная каждому компоненту; могут быть реализованы лишь локальные базы, и тогда суррогатный процесс выполняется от имени незарегистрированного пользователя или по некоторым правилам получает идентификатор кого-либо из локальных пользователей.

Идентификация групп пользователей может строиться на основе сетевых адресов хостов или подсетей. В то же время регистрационный журнал должен содержать достаточно информации для ассоциирования действий с конкретным пользователем. Сетевой адрес может являться частью глобального идентификатора пользователя.

В принципе возможен централизованный контроль доступа, когда решения принимает специальный сервер авторизации. Возможен и смешанный вариант, когда сервер авторизации разрешает соединение двух хостов, а дальше в дело вступают локальные механизмы хоста, содержащего объект доступа.

Аналогично, идентификация и аутентификация пользователей может производиться как централизованно (соответствующим сервером), так и локально - той системой, с которой пользователь непосредственно взаимодействует. Возможна передача идентификационной и аутентификационной информации между хостами, чтобы избавить пользователя от многократной аутентификации. При передаче аутентификационная информация должна быть защищена не слабее, чем на каждом из компонентов сетевой конфигурации.

В идентификации и аутентификации могут нуждаться не только пользователи, но и компоненты сети, такие как хосты.

Регистрационная информация в сетевом случае может включать в себя записи новых видов, например, сведения об установлении и разрыве соединений, о потенциальном нарушении целостности данных, например, в ввиду неправильной маршрутизации датаграмм, об изменениях в конфигурации сети. "Адресное пространство пользователей" становится распределенным, а в число регистрируемых событий попадают действия с удаленными объектами (открытие, переименование и т.п.).

При ведении регистрационного журнала могут использоваться локальные или глобальные синхронизированные часы.

Регистрационные журналы разных компонентов сети должны быть согласованы между собой; должны предоставляться средства для комплексного анализа совокупности регистрационных журналов с целью глобального отслеживания деятельности пользователей.

Возможно выделение в сети одного или нескольких серверов протоколирования и аудита, обслуживающих другие компоненты, которые не имеют ресурсов или по иным причинам не желают вести протоколирование самостоятельно.

Переходя к рассмотрению вопросов гарантированности, отметим, что каждая часть сетевой надежной вычислительной базы, расположенная на отдельном компоненте, должна поддерживать отдельную область для собственного выполнения, защищенную от внешних воздействий.

"Интерпретация" отличается от самих "Критериев" учетом динамичности сетевых конфигураций. Предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами живучести и корректности функционирования друг друга, доступность средств оповещения администратора о неполадках в сети. Сетевая конфигурация должна быть устойчива к отказам отдельных компонентов или коммуникационных путей.

Динамичность, согласно "Интерпретации", должна найти отражение в Руководстве администратора по средствам безопасности. Помимо прочих, это Руководство обязано освещать такие темы, как аппаратное конфигурирование сети, учет последствий подключения новых компонентов или отключения старых.

В качестве еще одного отличительного момента "Интерпретации" отметим повышенное внимание к целостности информации вообще и меток безопасности в частности. Здесь уже речь идет о некоторых аспектах принудительного управления доступом, характерного для уровня безопасности "B". Для контроля целостности меток и для их защиты от нелегального изменения в "Интерпретации" рекомендуется широкое использование криптографических методов. Далее, чтобы принудительное управление доступом в распределенной конфигурации имело смысл, совокупность уровней секретности и категорий должна поддерживаться централизованно. В этом одно из принципиальных отличий от добровольного управления доступом.

В целом следует отметить довольно очевидный характер первой части "Интерпретации", что, впрочем, является прямым следствием выбранного методологического подхода. Описание существенно новых сервисов и механизмов вынесено во вторую часть документа. Если первая часть посвящена в основном управлению доступом к информации, то во второй нашли отражение все основные аспекты безопасности: конфиденциальность, целостность и доступность.

Новые сервисы безопасности и защитные механизмы

Рассматриваемый документ создавался примерно в то же время, что и Рекомендации X.800. Естественно, что две рабочие группы обменивались информацией, поэтому во многих отношениях их подходы схожи. Имеются, однако, и важные различия. "Интерпретация" не замыкается на эталонной семиуровневой модели, ее цель - оценка безопасности всей распределенной конфигурации, а не только чисто сетевых аспектов. Рекомендации X.800 в основном имеют дело с функциональностью (с сервисами безопасности) и в меньшей степени - с защитными механизмами. В части 2 "Интерпретации" анализируется еще одна важнейшая характеристика - гарантированность.

Основой функционирования сетей вообще и коммуникационной безопасности в частности являются сетевые протоколы. Многие защитные механизмы встраиваются в протоколы. От протоколов зависит защита системы от тупиков и иных обстоятельств, способных повлиять на доступность сервисов, а также наличие средств обнаружения ситуаций недоступности. Протоколы влияют и на возможность поддержания целостности данных.

Среди защитных механизмов в сетевых конфигурациях на первом месте стоит криптография, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость реализации механизмов управления ключами.

Для поддержания целостности (в аспектах, относящихся к коммуникациям) используются аутентификация, контроль целостности полей и механизмы обеспечения неотказуемости. Этот сервис подробно рассматривался в связи с Рекомендациями X.800.

Новым, по сравнению с X.800, является подход к вопросу доступности. Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии

обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей. Надежная система должна быть в состоянии обнаруживать ситуации недоступности, уметь возвращаться к нормальной работе и противостоять атакам на доступность.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

- Внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.).
- Наличие средств реконфигурирования для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность.
- Рассредоточенность сетевого управления, отсутствие единой точки отказа.
- Наличие средств нейтрализации отказов (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов).
- Выделение подсетей и изоляция групп пользователей друг от друга.

С точки зрения оценки надежности систем, критерии части 2 дополняют "Оранжевую книгу". Каждый сервис безопасности рассматривается независимо и может получить одну из трех положительных оценок. Таким образом, общая оценка сетевой конфигурации выглядит примерно так: класс безопасности С2, сервис_1 - удовлетворительно, сервис_2 - хорошо и т.д. Заказчик, зная свои потребности, в состоянии принять решение о пригодности той или иной конфигурации.

Оценка надежностн сетевой конфигурации на основе оценки компонентов

В части 1 "Интерпретации" излагается подход к оценке надежности сетевой конфигурации как единого целого. В то же время имеет право на существование и другой взгляд, когда сеть составляется из предварительно проверенных компонентов, а общая оценка по определенным правилам выводится из их "рейтинга". Подобная точка зрения является предметом рассмотрения приложений к "Интерпретации", где анализируются три главных вопроса:

- Как следует структурировать сеть, чтобы оценка компонентов помогала получить общую оценку?
- Какие критерии следует применять к компонентам?
- Как получать общую оценку?

Предварительным условием надежности сетевой конфигурации является наличие единой политики безопасности, с которой должны быть согласованы поведение каждого компонента и характер связей между ними. В "Интерпретации" рассматриваются следующие аспекты политики безопасности:

- добровольное управление доступом;
- принудительное управление доступом;
- идентификация и аутентификация;
- протоколирование и аудит.

Одним из важнейших в "Оранжевой книге" является понятие монитора обращений, а применительно к структурированию сетевой конфигурации можно сформулировать следующее утверждение, дающее достаточное условие корректности фрагментирования монитора обращений.

Утверждение 1. Пусть каждый субъект, в качестве которого выступает процесс, действующий от имени какого-либо пользователя, заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Пусть, далее, каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа и все мониторы проводят в жизнь согласованную политику безопасности. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации.

Истинность этого утверждения непосредственно следует из определения монитора обращений.

Отметим разумность структурирования на компоненты, содержащие собственные мониторы обращений. Обычно каждый такой компонент предоставляет законченный набор услуг, а значит, его выделение естественно и целесообразно не только с точки зрения безопасности, но и с функциональной точки зрения.

Таким образом, сетевые конфигурации рекомендуется структурировать на компоненты, предоставляющие определенные виды сервиса и отслеживающие обращения к своим объектам, и на коммуникационные каналы, защищенные надежными сетевыми сервисами, использующими, как правило, криптографические механизмы.

Оценка компонентов производится по обычным критериям "Оранжевой книги" с одной важной оговоркой, а именно: каждый компонент, вообще говоря, не обязан поддерживать все перечисленные выше аспекты политики безопасности. В таком случае к нему нужно применять соответствующее подмножество критериев. Компоненты, поддерживающие лишь часть аспектов политики безопасности, должны обладать программными и/или протокольными интерфейсами, чтобы получить недостающие им сервисы от других компонентов (предоставляющих такую возможность).

При оценке сетевой конфигурации принимается во внимание тип компонентов и присвоенный им класс безопасности. Комбинируя четыре аспекта политики безопасности, каждый из которых может независимо поддерживаться или не поддерживаться, получим 15 типов компонентов и их комбинаций (случай, когда не поддерживается ни один аспект, не рассматривается). Как правило, условия корректности комбинаций и итоговый класс безопасности очевидным образом следуют из обычных критериев. Так, при объединении двух компонентов, поддерживающих добровольное управление доступом, необходимо, чтобы был определен протокол передачи идентификационной информации, на которой основываются решения о предоставлении запрашиваемого вида доступа. Политика безопасности каждого компонента и их объединения должна быть согласована с общей политикой. Итоговый класс безопасности объединения равен минимальному из классов, присвоенных компонентам.

При объединении компонента с добровольным управлением доступом и компонента, поддерживающего идентификацию и аутентификацию, должны сохраниться возможности обоих компонентов и, кроме того, для классов C2 и выше необходимо наличие интерфейса к компонентам протоколирования и аудита. Если компонент идентификации отнесен к классу безопасности C2, то итоговый класс объединения совпадает с классом компонента с добровольным управлением доступом.

Литература

[1] В. Галатенко. Информационная безопасность, "Открытые системы", # 4, 1995.

[2] В. Галатенко. Информационная безопасность, "Открытые системы", # 5, 1995.

[3] Security Architecture for Open Systems lnterconnection for CCITT Applications. Recommendation X.800. - CCITT, Geneva, 1991.

[4] National Computer Security Center. Trusted Network Interpretation. - NCSC-TG-005, 1987.