Известия Гомельского государственного университета
имени Ф. Скорины, №3(18), 2003

УДК 681.3

Проблемы информационной безопасности в компьютерных сетях

А.Б.Демуськов, Г.И.Большакова, Т.П.Бышик

В конце 80-х годов прошлого века в связи с начавшимся широким распространением компьютерных сетей значительно вырос интерес пользователей и специалистов к защите информации в вычислительных системах. Публикации последних лет отмечают обострение проблемы безопасности компьютеров как объектов, наиболее часто подвергающихся нападению злоумышленников. Интенсивное расширение числа абонентов глобальной сети Internet несёт с собой увеличение уязвимости различного рода автоматизированных систем, а использование современного персонального компьютера даёт в руки злоумышленникам уникальный по своим возможностям инструмент разведки и проникновения в сеть. Одним из стимуляторов разработки программных средств защиты послужило также широкое распространение программ-вирусов, разрушающих данные, носители информации и даже оборудование.

Уязвимость информации, обрабатываемой с помощью ЭВМ, резко увеличилась, когда в конце 80-х годов прошлого века появилось большое число вычислительных машин, открытых для доступа по телефонным линиям и другим каналам связи. Быстрыми темпами растёт в настоящее время количество объединяемых в различного рода сети персональных компьютеров, лавинообразно увеличивается число абонентов глобальной сети Internet. Всё это приводит к существенному расширению инструментария для потенциальных нарушителей целостности информации. Большинство нарушений, как показывает отечественный и зарубежный опыт, связано именно с проникновением в компьютерные сети, что сводит на нет эффективность процедур физического ограничения доступа к ЭВМ. В то же время необходимость в контролируемом использовании данных (защита авторских прав, персональных данных, коммерческой тайны, сохранения секретов) растёт, что обостряет потребность как в программных и аппаратных средствах защиты, так и в организационном обеспечении процесса функционирования сетей, а также и в правовом регулировании информационной сферы в целом.

В распределённой вычислительной сети возникают дополнительные по сравнению с автономными ЭВМ аспекты обеспечения безопасности. Среди них можно выделить:

- широкие возможности абонента-злоумышленника представиться другим абонентом;
- возможность использования некоторой скомпрометированной центральной ЭВМ;
- возможности модификации операционной системы или базы данных одной ЭВМ таким образом, что она распространится на другие ЭВМ (проблемы вирусов и других подобного класса программ);
- возможности нападения на одну систему нескольких других систем;
- неодинаковость защиты данных у каждого из элементов сети;
- отсутствие политик безопасности;
- несоблюдение политики безопасности при монтаже, настройке, расширении и обслуживании.

На сегодняшний день сформулированы три базовых принципа, которые должна обеспечивать информационная безопасность:

- целостность данных – защита от сбоев, ведущих к потере информации, а также защита от неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей.

Степень доверия, или надежность систем, можно оценивать по двум основным критериям: политике безопасности, гарантированности.

Политика безопасности – это набор законов, правил и норм поведения, определяющих, каким образом 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 много образнее 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 – это мера доверия, которая может быть оказана архитектуре и алгоритмам 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 (протоколирования). Надежная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть 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 (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Надежность вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит административный персонал (например, это могут быть данные о степени благонадежности пользователей). 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.

Среди наиболее эффективных путей решения проблемы защиты на сегодня могут быть выделены:

- контроль доступа к ресурсам, который сводится к тому, что все абоненты сети должны быть аутентифицированы до того, как будет установлена связь между абонентом и системой;
- гарантирование требуемого уровня защищённости, реализация контроля и наблюдения за использованием ресурсов сети и целостностью средств обеспечения безопасности;
- полномасштабный контроль использования ресурсов сети.

В целях обеспечения дополнительной защиты от случайной или преднамеренной утечки информации в компьютерных сетях помимо аутентификации для отдельной ЭВМ, входящей в сеть, должна вводится процедура установления подлинности самих ЭВМ. При этом следует иметь в виду, что свидетельства подлинности в условиях сети имеют свойство становиться менее эффективными, так как они проходят цепочку многочисленных узлов и других элементов сети. Поэтому в компьютерной сети целесообразна централизованная проверка и применение средств аутентификации, защищённых от подделок.

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 согласованности со списком действий, допустимых для пользователя.

Исходя из этих особенностей, с технической точки зрения необходимо иметь специальные механизмы, ограничивающие или локализующие нарушения безопасности работы

сети. Причём защита всей сети в целом должна быть независимой от защиты отдельных её элементов.

Согласно "Оранжевой книге" (критериям надёжности компьютерных систем Министерства обороны США) политика безопасности должна включать в себя по крайней мере следующие элементы:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом.

Произвольное управление доступом – это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность 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 произвольном 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 невозможно (поскольку она очень велика), да и не нужно (поскольку она разрежена, то есть большинство клеток в ней пусты). В операционных системах более компактное представление матрицы доступа основывается или на структурировании совокупности субъектов (владелец/ группа/ прочие в ОС UNIX), или на механизме списков управления доступом, то есть на представлении матрицы по столбцам, когда 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 рамках. Большинство операционных систем и систем управления базами данных реализуют именно произвольное 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 – 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 следующую особенность. 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.

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. 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 воспринимать, 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 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 (даже системных администраторов). 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 только к X.

Принудительное управление доступом реализовано во многих вариантах операционных систем и СУБД, отличающихся повышенными мерами безопасности. 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 произвольное и принудительное управление доступом сочетается в рамках одной системы, что позволяет использовать сильные стороны обоих подходов.

Учитывая рассмотренные проблемы информационной безопасности, базовые принципы, критерии политики безопасности и пути решения этих проблем, обозначим некоторые практические задачи обеспечения информационной безопасности.

При переходе к решению практических задач обеспечения безопасности необходимо обратить пристальное внимание на комплексный характер проблемы, необходимость сочетания законодательных, организационных и программно-технических мер. К сожалению, законодательная база отстаёт от потребностей практики. В то же время следует учитывать, что от государства требуется в первую очередь поддержка, организация и координация работ. Следующим после законодательного уровня необходимо рассматривать управленческий уровень. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов. Главное, что должен сделать управленческий уровень, – это выработать политику безопасности, которая задает общее направление работам в данной области. Следующий уровень в практических задачах обеспечения безопасности – это человеческий фактор. На этом уровне необходимо рассматривать меры безопасности, которые ориентированы на людей, а не на технические средства. Имеются в виду способы подбора персонала, его обучения, обеспечения дисциплины. Сюда же относятся меры по физической защите помещений и оборудования и некоторые другие. Именно люди формируют режим информационной безопасности, и они же оказываются главной угрозой, поэтому «человеческий фактор» заслуживает первостепенного внимания. Для поддержания режима информационной безопасности особенно важны и программно-технические меры, поскольку основная угроза компьютерным системам исходит от самих этих систем (сбои оборудования, ошибки программного обеспечения, промахи пользователей и администраторов и т.п.).

Стандарты и прилагаемые к ним рекомендации образуют понятийный базис, на котором строятся все работы по обеспечению информационной безопасности. В то же время эти документы ориентированы в первую очередь на производителей и "оценщиков" систем и в гораздо меньшей степени – на потребителей (пользователей). Информационную безопасность нельзя купить, ее приходится каждодневно поддерживать, взаимодействуя при этом не только и не столько с компьютерами, сколько с людьми. Иными словами, стандарты и рекомендации не дают ответов на два главных (с практической точки зрения) вопроса:

- Как приобретать (комплектовать) информационную систему масштаба предприятия, чтобы ее можно было сделать безопасной?
- Как практически сформировать режим безопасности и поддерживать его в условиях постоянно меняющегося окружения и структуры самой системы?

Таким образом, стандарты и рекомендации являются лишь отправной точкой на длинном и сложном пути защиты информационных систем организаций. С практической точки зрения важны рекомендации, по возможности простые, следование которым дает пусть не оптимальное, но достаточно хорошее решение задачи обеспечения информационной безопасности.

Abstract

There are the problems of computer networks in the field of information safety under consideration in the article. The principles and criteria of ensuring information safety are considered here.

Литература

1. Галатенко В. Информационная безопасность. Jet Info, 1996. – №1-3

2. Герасименко В.А., Малюк А.А. Основы защиты информации Москва, 1997, МИФИ

3. Научная сессия МИФИ-2003. X всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы». Сборник научных трудов. М.: МИФИ, 2003. – 256 с.

4. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. Москва, 1992.

5. Гайкович В., Першин А. Безопасность электронных банковских систем. Москва. Единая Европа, 1994.

Гомельский государственный
университет им.Ф.Скорины

Поступило 06.04.03