В. М. Бакулин

ОСНОВНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье рассматривается понятие информационной безопасности, характеристика средств и методов защиты информации от различных видов угроз.

Ключевые слова: информация, угроза, авторизация, криптография, электронная цифровая подпись, межсетевой экран.

V. M. Bakulin

GENERAL ISSUES OF INFORMATION SECURITY

In the article the author focuses on the notion of information security and characteristics of means and methods of protecting information from various kinds of threat.

Keywords: information, threat, authorization, cryptography, electronic digital signature, firewall.

Последние десятилетия знаменуются бурным развитием информационных технологий во всех сферах общественной жизни. Информация все в большей мере становится стратегическим ресурсом государства и востребованным товаром. Подобно любым другим существующим товарам, информация также нуждается в своей сохранности и надежной защите.

Уязвимость информации в компьютерных системах обусловлена большой концентрацией вычислительных ресурсов, их территориальной рассредоточенностью, долговременным хранением больших объемов данных, одновременным доступом к ресурсам компьютерных систем многочисленных пользователей. Каждый день появляются все новые и новые угрозы, поэтому острота проблемы информационной безопасности с течением времени приобретает все большую актуальность.

Создание всеобщего информационного пространства и практически повсеместное применение персональных компьютеров, внедрение компьютерных систем породило необходимость решения комплексной проблемы защиты информации.

В связи с этим в различных учебных заведениях высшего и профессионального образования проводятся курсы, в которых рассматриваются вопросы информационной безопасности. Содержание и подход к преподаванию этих курсов в каждом учебном заведении различен и зависит от специальности и уровня подготовленности обучаемых.

Учитывая гуманитарную направленность обучения курсантов в Волгоградской академии МВД России, необходимо определить степень подробности изучаемой дисциплины. Решая подобную задачу, нужно учитывать не только состояние дел в данной области на сегодняшний день, но и практическую целесообразность. Так, к примеру, следователи постоянно работают с конфиденциальными данными, однако углубление в технические подробности защиты информации для них нецелесообразно, так как это выходит за рамки их служебной деятельности.

В данной статье предлагаются основные понятия, которые следует изучать курсантам и слушателям образовательных учреждений системы МВД РФ не технических специальностей. Даны краткие определения и перечислены

основные методы защиты информации, которые не требуют специальной подготовки.

Защита информации в компьютерных системах — это регулярное использование средств и методов, принятие мер и осуществление мероприятий в целях системного обеспечения требуемой надежности информации, хранимой и обрабатываемой с использованием средств вычислительной техники [1, с. 79]. Объектом защиты является информация, или носитель, а также информационный процесс, в отношении которого необходимо обеспечить защиту в соответствии с поставленной целью защиты информации.

Под информационной безопасностью понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности [4, с. 27]. Информационная безопасность достигается обеспечением сохранности основных свойств информации: конфиденциальности, целостности, достоверности и доступности.

Конфиденциальность — это свойство, указывающее на необходимость введения ограничения доступа к данной информации для определенного круга лиц [2, 8]. Другими словами, это гарантия того, что в процессе передачи данные могут быть известны только легальным пользователям.

Целостность — это свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения в неискаженном виде по отношению к некоторому фиксированному состоянию. Информацию может создавать, изменять или уничтожать только авторизованное лицо (законный, имеющий право доступа пользователь).

Достоверность — это свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята.

Доступность — это свойство информации, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к необходимой информации.

Противодействие многочисленным угрозам информационной безопасности предусматривает комплексное использование различных способов и мероприятий организационного, правового, инженерно-технического, программно-аппаратного, криптографического характера и т. п.

Организационные мероприятия по защите включают в себя совокупность действий по подбору и проверке персонала, участвующего в подготовке и эксплуатации программ и информации, строгое регламентирование процесса разработки и функционирования компьютерных систем.

К правовым мерам и средствам защиты относятся действующие в стране законы, нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушение.

Инженерно-технические средства защиты достаточно многообразны и включают в себя физико-технические, аппаратные, технологические, программные, криптографические и другие средства. Данные средства обеспечивают следующие рубежи защиты: контролируемая территория, здание, помещение, отдельные устройства вместе с носителями информации.

Программно-аппаратные средства защиты непосредственно применяются в компьютерах и компьютерных сетях, содержат различные встраиваемые в КС электронные, электромеханические устройства. Специальные пакеты программ или отдельные программы реализуют такие функции защиты, как разграничение и контроль доступа к ресурсам, регистрация и анализ протекающих процессов, событий, пользователей, предотвращение возможных разрушительных воздействий на ресурсы и другие [3, с. 87].

Суть криптографической защиты заключается в приведении (преобразовании) информации к неявному виду с помощью специальных алгоритмов либо аппаратных средств и соответствующих кодовых ключей.

Рассмотрим основные программные методы защиты информации от наиболее часто встречаемых угроз: несанкционированный доступ, копирование, вредоносные программы (вирусы).

Основным способом защиты компьютерных систем от несанкционированного вмешательства злоумышленников считается использование так называемых средств ЗА (аутентификация, авторизация, администрирование).

Авторизация (санкционирование, разрешение) — процедура, по которой пользователь при входе в систему опознается и получает права доступа, разрешенные системным администратором, к вычислительным ресурсам (компьютерам, дискам, папкам, периферийным устройствам) [4, с. 302]. Авторизация выполняется программой и включает в себя идентификацию и аутентификацию.

Идентификация — предоставление идентификатора, которым может являться несекретное имя, слово, число, для регистрации пользователя. Субъект указывает имя пользователя, предъявленный идентификатор сравнивается с перечнем идентификаторов. Пользователь, у которого идентификатор зарегистрирован в системе, расценивается как правомочный (легальный). Синонимом идентификатора является логин — набор букв и цифр, уникальный для данной системы.

Аутентификация — проверка подлинности, то есть того, что предъявленный идентификатор действительно принадлежит субъекту доступа. Выполняется на основе сопоставления имени пользователя и пароля. После аутентификации субъекту разрешается доступ к ресурсам системы на основе разрешенных ему полномочий.

Наиболее часто применяемыми методами авторизации являются методы, основанные на использовании паролей (секретных последовательностей символов). Пароль можно установить на запуск программы, отдельные действия на компьютере или в сети. Кроме паролей, для подтверждения подлинности могут использоваться пластиковые карточки и смарт-карты.

Администрирование — это регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. Для своевременного пресечения несанкционированных действий, для контроля за соблюдением установленных правил доступа необходимо обеспечить регулярный сбор, фиксацию и выдачу по запросам сведений о всех обращениях к защищаемым компьютерным ресурсам. Основной формой регистрации является программное ведение специальных регистрационных журналов, представляющих собой файлы на внешних носителях информации.

Несанкционированное копирование информации может быть заблокировано различными методами:

1. Методами, затрудняющими считывание скопированной информации. Основаны на создании в процессе записи информации на соответствующие накопители таких особенностей (нестандартная разметка, форматирование носителя информации, установка электронного ключа), которые не позволяют считывать полученную копию на других накопителях, не входящих в состав защищаемой системы. Другими словами, эти методы направлены на обеспечение совместимости нако-пителей только внутри данной компьютерной системы.

2. Методами, препятствующими использованию информации. Затрудняют использование полученных копированием программ и данных. Наиболее эффективным в этом отношении средством защиты является хранение информации в преобразованном криптографическими методами виде. Другим методом противодействия несанкционированному выполнению скопированных программ является использование блока контроля среды размещения программы. Он создается при инсталляции программы и включает характеристики среды, в которой размещается программа, а также средства сравнения этих характеристик. В качестве характеристик используются характеристики ЭВМ или носителя информации.

Для защиты компьютерных систем от разнообразных вредительских программ (вирусов) разрабатываются специальные антивирусные средства. Антивирусная программа обнаруживает вирусы, предлагая вылечить файлы, а при

невозможнос-ти — удалить. Существует несколько разновидностей антивирусных программ:

1) сканеры или программы-фаги — это программы поиска в файлах, памяти, загрузочных секторах дисков сигнатур вирусов (уникального программного кода именно этого вируса), проверяют и лечат файлы;

2) мониторы (разновидность сканеров) — проверяют оперативную память при загрузке операционной системы, автоматически проверяют все файлы в момент их открытия и закрытия, чтобы не допустить открытия и запись файла, зараженного вирусом; блокирует вирусы;

3) иммунизаторы — предотвращают заражение файлов, обнаруживают подозрительные действия при работе компьютера, характерные для вируса на ранней стадии (до размножения), и посылают пользователю соответствующее сообщение;

4) ревизоры — запоминают исходное состояние программ, каталогов до заражения и периодически (или по желанию пользователя) сравнивают текущее состояние с исходным;

5) доктора — не только находят зараженные вирусами файлы, ни и «лечат» их, то есть удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние;

6) блокировщики — отслеживают события и перехватывают подозрительные действия (производимые вредоносной программой), запрещают действие или запрашивают разрешение пользователя.

Эффективным средством противодействия различным угрозам информационной безопасности является закрытие информации методами криптографического (от греч. *kryptos* — тайный) преобразования. В результате такого преобразования защищаемая информация становится недоступной для ознакомления и непосредственного использования лицами, не имеющими на это полномочий. По виду воздействия на исходную информацию криптографические методы разделены на следующие виды:

1. Шифрование — процесс маскирования сообщений или данных в целях скрытия их содержания, ограничения доступа к содержанию других лиц. Заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов. Для шифрования используются алгоритм преобразования и ключ.

2. Стеганография — метод защиты компьютерных данных, передаваемых по каналам телекоммуникаций, путем скрытия сообщения среди открытого текста, изображения или звука в файле-контейнере. Позволяет скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. Скрытый файл может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы.

3. Кодирование — замена смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари, хранящиеся в секрете. Кодирование широко используется для защиты информации от искажений в каналах связи.

4. Сжатие информации — сокращение объемов информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Поэтому сжатые файлы подвергаются последующему шифрованию.

5. Рассечение-разнесение заключается в том, что массив защищаемых данных делится (рассекается) на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации. Выделенные таким образом элементы данных разносятся по разным зонам ЗУ или располагаются на различных носителях.

6. Электронная цифровая подпись представляет собой строку данных, которая зависит от некоторого секретного параметра (ключа), известного только подписывающему лицу, и от содержания подписываемого сообщения, представленного в цифровом виде. Используется для подтверждения целостности и авторства данных, нельзя изменить документ без нарушения целостности подписи [1, с. 496].

Для блокирования угроз, исходящих из общедоступной системы, используется специальное программное или аппаратно-программное средство, которое получило название межсетевой экран или fire wall. Межсетевой экран позволяет разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Иногда сетевая защита полностью блокирует трафик снаружи внутрь, но разрешает внутренним пользователям свободно связываться с внешним миром. Обычно межсетевой экран защищает внутреннюю сеть предприятия от вторжений из глобальной сети Интернет. Межсетевой экран выполняет четыре основные функции:

1) фильтрация данных на разных уровнях;

2) использование экранирующих агентов (proxy-серверы), которые являются программами-посредниками и обеспечивают соединение между субъектом и объектом доступа, а затем пересылают информацию, осуществляя контроль и регистрацию;

3) трансляция адресов предназначена для скрытия от внешних абонентов истинных внутренних адресов;

4) регистрация событий в специальных журналах. Анализ записей позволяет зафиксировать попытки нарушения установленных правил обмена информацией в сети и выявить злоумышленника.

Актуальность вопросов защиты информации возрастает с каждым годом. Многие считают, что данную проблему можно решить чисто техническими мерами — установкой межсетевых экранов и антивирусных программ. Но для построения надежной защиты в первую очередь необходима информация о существующих угрозах и методах противодействия им. И это относится не только к специалистам, работающим в области информационных технологий, но и ко всем, кто по роду своей деятельности использует различные информационные системы. Известный принцип «предупрежден, значит вооружен» работает и в сфере компьютерной безопасности: вовремя распознав угрозу, можно не допустить неприятного развития событий. Поэтому нужно соблюдать меры защиты во всех точках сети, при любой работе любых субъектов с информацией.

Список библиографических ссылок

1. Гаврилов М. В. Информатика и информационные технологии: учебник. М., 2006.
2. Домарев В. В. Безопасность информационных технологий. Киев, 2004.
3. Коуров Л. В. Информационные технологии. Мн., 2000.
4. Шальгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М., 2008.