ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СЕТЯХ ЭВМ

Шония Отар, Цомая Нино
Грузинский Технический Университет

Резюме

Рассматривается информационная безопасность, ее базовые принципы, основные задачи, виды защиты информации и выявляются основные объекты, нуждающиеся в защите, и объекты угроз безопасности. Определяются средства физической и программной защиты.

Ключевые слова: информационная безопасность. Конфиденциальность информации. Целостность данных. Сетевые ресурсы. Физическая защита. Программные средства контроля. Компьютерные вирусы. Устройства контроля доступа. Классы защищенности.

1. Введение

Защита данных в компьютерных сетях становится одной из самых открытых проблем в современных информационно-вычислительных системах. На сегодняшний день сформулировано три базовых принципа информационной безопасности, задачей которой является обеспечение:

- целостности данных - защита от сбоев, ведущих к потере информации или ее уничтожения;
- конфиденциальности информации;
- доступности информации для авторизованных пользователей.

Однако обеспечение безопасности включает в себя 3 основные задачи (рис.1):

- **Предотвращение** – создание защитных процедур и защищенной среды, предотвращающей попытки вторжения злоумышленников и снижающей потенциальный риск или потери.
- **Обнаружение** – отслеживание действий, выполняемых в интернете, для немедленного выявления изменений в событиях, связанных с безопасностью.
- **Реагирование** – выполнение мероприятий по контролю или пресечению вредоносных
- действий при обнаружении атаки или вторжения.

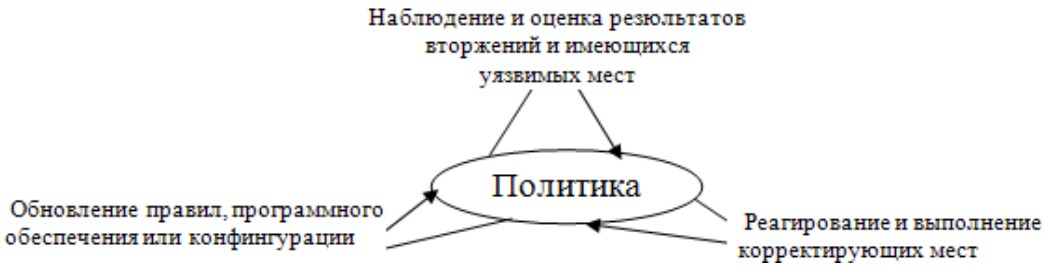

Рис.1. Система обеспечения безопасности информации

2. Основная часть

Рассматривая проблемы, связанные с защитой данных в сети, возникает вопрос о классификации сбоев и несанкционированности доступа, что ведет к потере или нежелательному изменению данных. Это могут быть сбои оборудования (кабельной системы, дисковых систем, серверов, рабочих станций и т.д.), потери информации (из-за инфицирования компьютерными вирусами, неправильного хранения архивных данных, нарушений прав доступа к данным), некорректная работа пользователей и обслуживающего персонала. Перечисленные нарушения работы в сети вызвали необходимость создания различных видов защиты информации. Условно их можно разделить на три класса:

- средства физической защиты;

-программные средства (антивирусные программы, системы разграничения полномочий, программные средства контроля доступа);

-административные меры защиты (доступ в помещения, разработка стратегий безопасности фирмы и т.д.).

Основными объектами информационной безопасности нуждающимися в защите в компаниях являются следующие компаненты, представленные на рисунке 2:

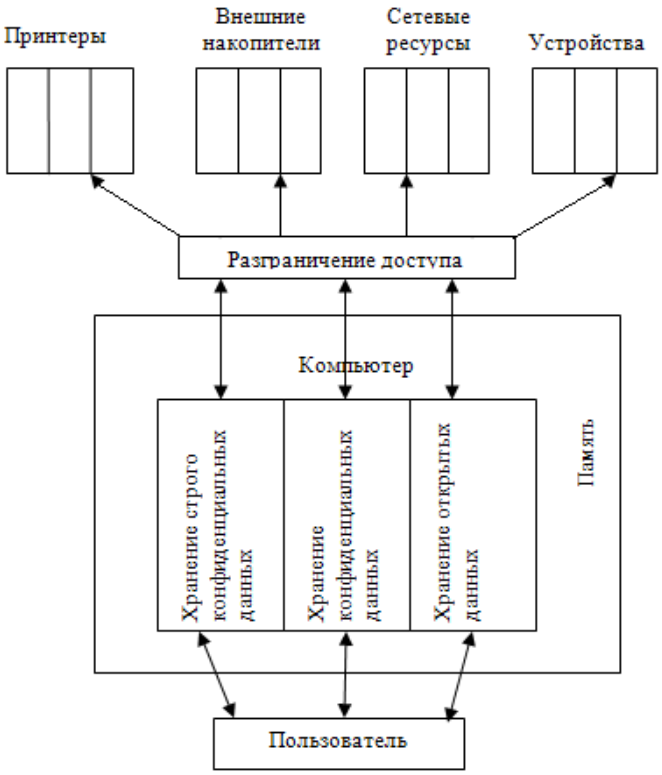

Рис.2. Объекты защиты

А основными объектами угроз безопасности в компаниях являются объекты, представленные на рисунке 3.

Одним из средств физической защиты являются системы архивирования и дублирования информации. В локальных сетях, где установлены один-два сервера, чаще всего система устанавливается непосредственно в свободные слоты серверов. В крупных корпоративных сетях предпочтение отдается выделенному специализированному архивационному серверу, который автоматически архивирует информацию с жестких дисков серверов и рабочих станций в определенное время, установленное администратором сети, выдавая отчет о проведенном резервном копировании. Наиболее распространенными моделями архивированных серверов являются Storage Express System корпорации Intel ARCserve for Windows.

Для борьбы с компьютерными вирусами наиболее часто применяются антивирусные программы, реже - аппаратные средства защиты. Однако, в последнее время наблюдается тенденция к сочетанию программных и аппаратных методов защиты. Среди аппаратных устройств используются специальные антивирусные платы, вставленные в стандартные слоты расширения компьютера. Корпорация Intel предложила перспективную технологию защиты от вирусов в сетях, суть которой заключается в сканировании систем компьютеров еще до их загрузки.

Кроме антивирусных программ, проблема защиты информации в компьютерных сетях решается введением контроля доступа и разграничением полномочий пользователя. Для этого используются встроенные средства сетевых операционных систем, крупнейшим производителем которых является корпорация Novell. В системе, например, NetWare, кроме стандартных средств ограничения доступа (смена паролей, разграничение полномочий), предусмотрена возможность кодирования данных по принципу "открытого ключа" с формированием электронной подписи для передаваемых по сети пакетов.

Однако, такая система защиты слабомощна, т.к. уровень доступа и возможность входа в систему определяются паролем, который легко подсмотреть или подобрать. Для исключения неавторизованного проникновения в компьютерную сеть используется комбинированный подход - пароль + идентификация пользователя по персональному "ключу". "Ключ" представляет собой пластиковую карту (магнитная или со встроенной микросхемой - смарт-карта) или различные устройства для идентификации личности по биометрической информации - по радужной оболочке глаза, отпечаткам пальцев, размерам кисти руки и т.д. Серверы и сетевые рабочие станции, оснащенные устройствами чтения смарт-карт и специальным программным обеспечением, значительно повышают степень защиты от несанкционированного доступа.

Смарт-карты управления доступом позволяют реализовать такие функции, как контроль входа, доступ к устройствам ПК, к программам, файлам и командам. Одним из удачных примеров создания комплексного решения для контроля доступа в открытых системах, основанного как на программных, так и на аппаратных средствах защиты, стала система Kerberos, в основу которой входят три компонента:

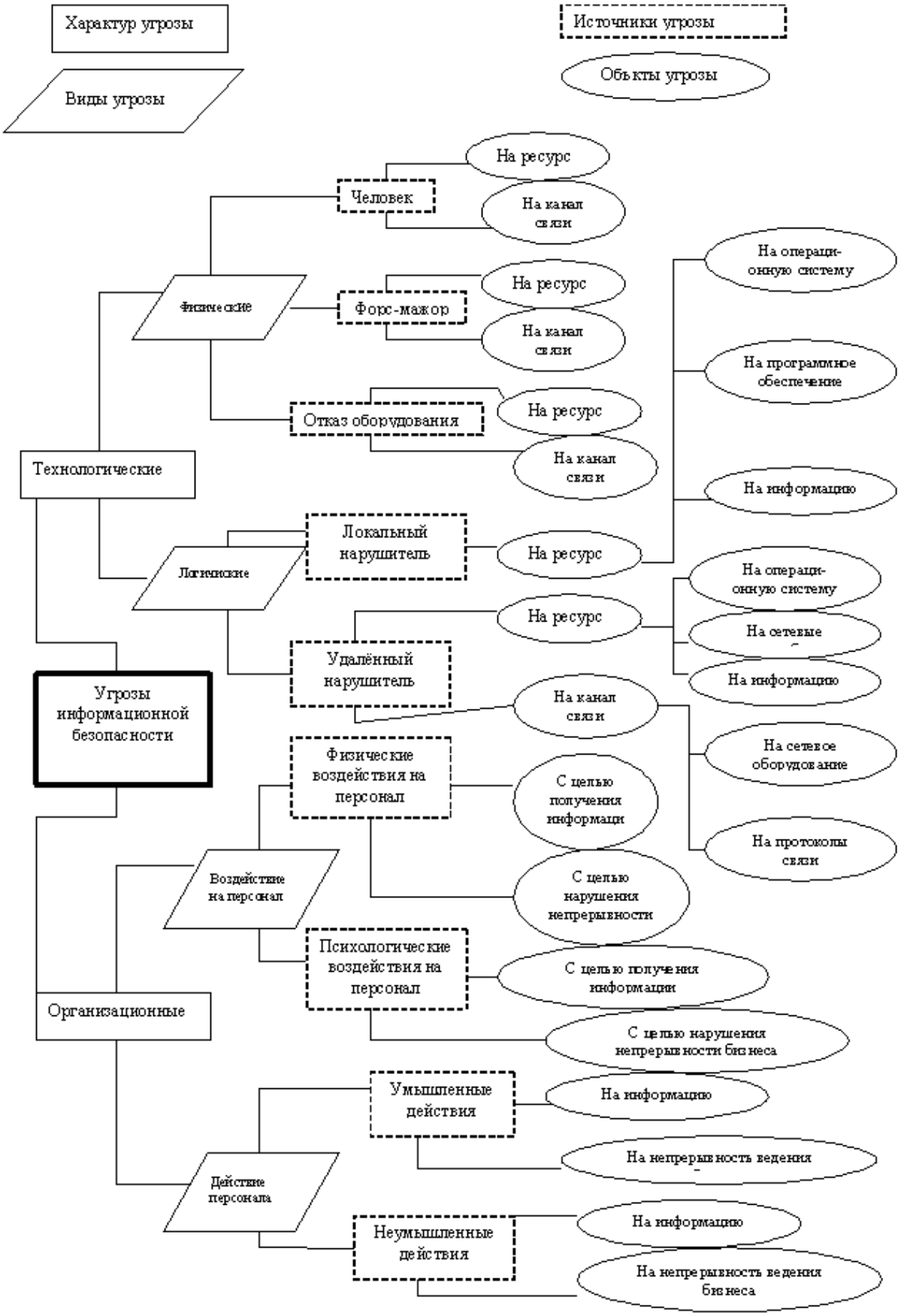

Рис.3. Объекты угроз

- база данных, которая содержит информацию по всем сетевым ресурсам, пользователям, паролям, информационным ключам и т.д.;

- авторизационный сервер (authentication server), задачей которого является обработка запросов пользователей на предоставление того или иного вида сетевых услуг. Получая запрос, он обращается к базе данных и определяет полномочия пользователя на совершение определенной операции. Пароли пользователей по сети не передаются, тем самым, повышая степень защиты информации;

-Ticket-granting server (сервер выдачи разрешений) получает от авторизационного сервера "пропуск" с именем пользователя и его сетевым адресом, временем запроса, а также уникальный "ключ". Пакет, содержащий "пропуск", передается также в зашифрованном виде. Сервер выдачи разрешений после получения и расшифровки "пропуска" проверяет запрос, сравнивает "ключи" и при тождественности дает "добро" на использование сетевой аппаратуры или программ.

По мере расширения деятельности предприятий, роста численности абонентов и появления новых филиалов, возникает необходимость организации доступа удаленных пользователей (групп пользователей) к вычислительным или информационным ресурсам к центрам компаний. Для организации удаленного доступа чаще всего используются кабельные линии и радиоканалы. В связи с этим защита информации, передаваемой по каналам удаленного доступа, требует особого подхода. В мостах и маршрутизаторах удаленного доступа применяется сегментация пакетов - их разделение и передача параллельно по двум линиям, - что делает невозможным "перехват" данных при незаконном подключении "хакера" к одной из линий. Используемая при передаче данных процедура сжатия передаваемых пакетов гарантирует невозможность расшифровки "перехваченных" данных. Мосты и маршрутизаторы удаленного доступа могут быть запрограммированы таким образом, что удаленным пользователям не все ресурсы центра компании могут быть доступны.

В настоящее время разработаны специальные устройства контроля доступа к вычислительным сетям по коммутируемым линиям. Примером может служить, разработанный фирмой AT&T модуль Remote Port Securiti Device (PRSD), состоящий из двух блоков размером с обычный модем: RPSD Lock (замок), устанавливаемый в центральном офисе, и RPSD Key (ключ), подключаемый к модему удаленного пользователя. RPSD Key и Lock позволяют устанавливать несколько уровней защиты и контроля доступа:

- шифрование данных, передаваемых по линии при помощи генерируемых цифровых ключей;

- контроль доступа с учетом дня недели или времени суток.

Прямое отношение к теме безопасности имеет стратегия создания резервных копий и восстановления баз данных. Обычно эти операции выполняются в нерабочее время в пакетном режиме. В большинстве СУБД резервное копирование и восстановление данных разрешаются только пользователям с широкими полномочиями (права доступа на уровне системного администратора, либо владельца БД), указывать столь ответственные пароли непосредственно в файлах пакетной обработки нежелательно. Чтобы не хранить пароль в явном виде, рекомендуется написать простенькую прикладную программу, которая сама бы вызывала утилиты копирования/восстановления. В таком случае системный пароль должен быть "зашит" в код указанного приложения. Недостатком данного метода является то, что всякий раз при смене пароля эту программу следует перекомпилировать.

Применительно к средствам защиты от НСД определены семь классов защищенности (1-7) средств вычислительной техники (СВТ) и девять классов (1А,1Б,1В,1Г,1Д,2А,2Б,3А,3Б) автоматизированных систем (АС). Для СВТ самым низким является седьмой класс, а для АС - 3Б.

Рассмотрим более подробно приведенные сертифицированные системы защиты от НСД.

Система "КОБРА" соответствует требованиям 4-ого класса защищенности (для СВТ), реализует идентификацию и разграничение полномочий пользователей и криптографическое закрытие информации, фиксирует искажения эталонного состояния рабочей среды ПК (вызванные вирусами, ошибками пользователей, техническими сбоями и т.д.) и автоматически восстанавливает основные компоненты операционной среды терминала.

Подсистема разграничения полномочий защищает информацию на уровне логических дисков. Пользователь получает доступ к определенным дискам A,B,C,...,Z. Все абоненты разделены на 4 категории:

- суперпользователь (доступны все действия в системе);

-администратор (доступны все действия в системе, за исключением изменения имени, статуса и полномочий суперпользователя, ввода или исключения его из списка пользователей);

- программисты (может изменять личный пароль);

-коллега (имеет право на доступ к ресурсам, установленным ему суперпользователем).

Помимо санкционирования и разграничения доступа к логическим дискам, администратор устанавливает каждому пользователю полномочия доступа к последовательному и параллельному портам. Если последовательный порт закрыт, то невозможна передача информации с одного компьютера на другой. При отсутствии доступа к параллельному порту, невозможен вывод на принтер.

3. Заключение

Подведем итог. Основными принципами — метауровнем — защиты информации являются: авторизация, адекватная защита информации в целом, предотвращение потери данных, обнаружение нарушенной защиты, возможность восстановления по резервной копии и принцип избыточной защиты в узловых (не рабочих) точках. Если соблюдать все эти простые принципы, то вероятность потери информации с компьютера значительно снизится.

Литература:

1. Безопасность сетей. Полное руководство. Серия: справочник профессионалы Брэгг Р. Изд-во: Эком.

2. გოგიჩაიშვილი გ., ოდიშარია კ., შონია ო. ინფორმაციის დაცვის ავტომატიზებული სისტემები. სტუ, თბ., 2008

3. Джонс К. Анти-хакер. Средство защиты компьютерных сетей. Изд-во: Эком

4. Шербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. 2009

5. შონია ო., შონია დ., ცომაია ნ., გოგოხია ი. კომპიუტერულ დანაშაულებათა მასშტაბები და აქედან მომდინარე საფრთხეები. საერთ.სამეც. ჟურნ. „ინტელექტუალი” №5, 2007.

6. Мэйволд Э. Безопасность сетей. Самоучитель. Изд-во ЭКОМ. 2005.

INFORMATION SAFETY IN COMPUTER NETWORKS

Shonia Otar, Tsomaia Nino
Georgian Technical University

Summary

The article reveals the information security, its basic principles, major tasks, the types of informational security and identifies the main sites requiring the protection and real security threats. The means of physical and software protection are also defined.

ინფორმაციული უსაფრთხოება კომპიუტერულ ქსელებში

ოთარ შონია, ნინო ცომაია
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილული ინფორმაციული უსაფრთხოება, მისი ძირითადი პრინციპები, მთავარი ამოცანები, ინფორმაციული დაცვის სახეობები და ასევე განიხილება ძირითადი ობიექტები, რომლებსაც ჭირდება დაცვა, და უსაფრთხოების საშიშროებები. განსაზღვრულია ფიზიკური და პროგრამული დაცვის ხერხები.