**Угрозы доступности**

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих ИС. Иногда такие ошибки являются собственно угрозами (неправильно введённые данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65 % потерь есть следствие непреднамеренных ошибок. Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе. Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками — максимальная автоматизация и строгий контроль.

Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы:

**Отказ пользователей**

Обычно применительно к пользователям рассматриваются следующие угрозы:

* Нежелание работать с ИС (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
* Невозможность работать с ИС в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т. п.);
* Невозможность работать с ИС в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т. п.).

**Внутренний отказ ИС**

Основными источниками внутрених отказов являются:

* отступление (случайное или умышленное) от установленных правил эксплуатации;
* выход ИС из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчётного числа запросов, чрезмерный объём обрабатываемой информации и т. п.);
* ошибки при (пере)конфигурировании ИС;
* отказы программного и аппаратного обеспечения;
* разрушение данных;
* разрушение или повреждение оборудования.

**Отказ поддерживающей инфраструктуры**

По отношению к поддерживающей инфраструктуре выделяют следующие угрозы:

* нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
* разрушение или повреждение помещений;
* невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т. п.).

Помимо этого весьма опасны так называемые « обиженные сотрудники», нынешние и бывшие. Как правило, они стремятся нанести вред предприятию-обидчику, например:

* испортить оборудование;
* встроить логическую бомбу, которая со временем разрушит программы и/или данные;
* удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия, — пожары, наводнения, землетрясения, ураганы. По статистике, на долю огня, воды и тому подобных «злоумышленников» (среди которых самый опасный — нарушение электропитания) приходится 13 % потерь, нанесённых информационным системам.

Рассмотрим некоторые угрозы доступности более подробно:

**Повреждение и разрушение оборудования**

Угрозы доступности могут выглядеть грубо — как повреждение или даже разрушение оборудования, том числе носителей данных. Такое повреждение может вызываться естественными причинами. Чаще всего это грозы: большинство используемых источников бесперебойного питания не защищают от мощных кратковременных импульсов, поэтому случаи выгорания оборудования не редкость.

В принципе, мощный кратковременный импульс, способный разрушить данные на магнитных носителях, можно сгенерировать и искусственным образом — с помощью так называемых высокоэнергетических радиочастотных пушек. Но, наверное, в наших условиях подобную угрозу следует всё же признать надуманной.

В реальной жизни более опасны протечки водопровода и отопительной системы. Часто организации, чтобы сэкономить на арендной плате, снимают помещения в домах старой постройки, делают косметический ремонт, но не меняют ветхие трубы.

Летом, в сильную жару, норовят сломаться кондиционеры, установленные в серверных залах, набитых дорогостоящим оборудованием. В результате значительный ущерб наносится и репутации, и кошельку организации.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если оно выполняется, резервные носители зачастую хранят небрежно, не обеспечивая их защиту от вредного воздействия окружающей среды. И когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

**Агрессивное потребление ресурсов**

В качестве средства вывода ИС из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (обычно это полоса пропускания, вычислительные ресурсы процессора или оперативной памяти). По расположению источника угрозы такое потребление подразделяется на локальное и удалённое. При просчётах в конфигурации ИС локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Удалённое потребление ресурсов в последнее время проявляется в особенно опасной форме — как DoS - и DDoS-атаки ([Distributed] Denial-of-Service, [распределённая] атака на отказ в обслуживании). В последнем случае на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание. Временем начала моды на эти атаки можно считать февраль 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее, владельцы и пользователи этих систем). Если имеет место архитектурный просчёт (пропускная способность сети и производительность сервера разбалансированы), защититься от распредёленных атак на доступность крайне трудно.

**Отказ программного или аппаратного обеспечения**

Для выведения систем из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок. Например, известная ошибка в процессоре Pentium I давала возможность локальному пользователю путём выполнения определённой команды «подвесить» компьютер так, что спасала только аппаратная перезагрузка. А программа Teardrop могла удалённо «подвешивать» компьютеры, эксплуатируя ошибку в сборке фрагментированных IP-пакетов.