**Основы информационной безопасности. Виды угроз.**

Безопасность виртуального сервера может быть рассмотрена только непосредственно как **«информационная безопасность»**. Многие слышали это словосочетание, но не все понимают, что же это такое?

**«Информационная безопасность»** — это процесс обеспечения **доступности, целостности и конфиденциальности информации**.

Под **«доступностью»** понимается соответственно обеспечение доступа к информации.

**«Целостность»** — это обеспечение достоверности и полноты информации.

**«Конфиденциальность»** подразумевает под собой обеспечение доступа к информации только авторизованным пользователям.

Исходя из Ваших целей и выполняемых задач на виртуальном сервере, необходимы будут и различные меры и степени защиты, применимые по каждому из этих трех пунктов.

Для примера, если Вы используете виртуальный сервер, только как средство для серфинга в интернете, то из необходимых средств для обеспечения безопасности, в первую очередь будет использование средств антивирусной защиты, а так же соблюдение элементарных правил безопасности при работе в сети интернет.

В другом случае если у Вас размещен на сервере продающий сайт или игровой сервер, то и необходимые меры защиты будут совершенно различными.

Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее оптимальные средства обеспечения безопасности, для этого рассмотрим основные моменты.

Под **«Угрозой»** понимается потенциальная возможность тем или иным способом нарушить информационную безопасность. Попытка реализации угрозы называется **«атакой»**, а тот, кто реализует данную попытку, называется **«злоумышленником»**. Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем.

Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы.

Угрозы информационной безопасности, которые наносят наибольший ущерб

Рассмотрим ниже классификацию видов угроз по различным критериям:

1. Угроза непосредственно информационной безопасности:
	* Доступность
	* Целостность
	* Конфиденциальность
2. Компоненты на которые угрозы нацелены:
	* Данные
	* Программы
	* Аппаратура
	* Поддерживающая инфраструктура
3. По способу осуществления:
	* Случайные или преднамеренные
	* Природного или техногенного характера
4. По расположению источника угрозы бывают:
	* Внутренние
	* Внешние

Как упоминалось в начале понятие «угроза» в разных ситуациях зачастую трактуется по-разному. И необходимые меры безопасности будут разными. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать — вся информация считается общедоступной, однако в большинстве случаев нелегальный доступ представляется серьезной опасностью.

Применимо к виртуальным серверам, угрозы, которые Вам как администратору сервера, необходимо принимать во внимание это — угроза доступности, конфиденциальности и целостность данных. За возможность осуществления угроз направленных на конфиденциальность и целостность данных, не связанные с аппаратной или инфраструктурной составляющей, Вы несете прямую и самостоятельную ответственность. В том числе как и применение необходимых мер защиты, это Ваша непосредственная задача.

На угрозы направленные на уязвимости используемых Вами программ, зачастую Вы как пользователь не сможете повлиять, кроме как не использовать данные программы. Допускается использование данных программ только в случае если реализация угроз используя уязвимости этих программ, либо не целесообразна с точки зрения злоумышленника, либо не имеет для Вас как для пользователя существенных потерь.

Обеспечением необходимых мер безопасности от угроз направленных на аппаратуру, инфраструктуру или угрозы техногенного и природного характера, занимается напрямую та хостинг компания, которую Вы выбрали и в которой арендуете свои сервера. В данном случае необходимо наиболее тщательно подходить к выбору, правильно выбранная хостинг компания на должном уровне обеспечит Вам надежность аппаратной и инфраструктурной составляющей.

Вам как администратору виртуального сервера, данные виды угроз нужно принимать во внимание только в случаях при которых даже кратковременная потеря доступа или частичная или полная остановка в работоспособности сервера по вине хостинг компании могут привести к не соизмеримым проблемам или убыткам. Это случается достаточно редко, но по объективным причинам ни одна хостинг компания не может обеспечить Uptime 100%.

Угрозы непосредственно информационной безопасности

 К основным угрозам доступности можно отнести

1. Внутренний отказ информационной системы;
2. Отказ поддерживающей инфраструктуры.

Основными источниками внутренних отказов являются:

* Нарушение (случайное или умышленное) от установленных правил эксплуатации
* Выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.)
* Ошибки при (пере)конфигурировании системы
* Вредоносное программное обеспечение
* Отказы программного и аппаратного обеспечения
* Разрушение данных
* Разрушение или повреждение аппаратуры

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать 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.).

Основные угрозы целостности

Можно разделить на угрозы статической целостности и угрозы динамической целостности.

Так же стоит разделять на угрозы целостности служебной информации и содержательных данных. Под служебной информацией понимаются пароли для доступа, маршруты передачи данных в локальной сети и подобная информация. Чаще всего и практически во всех случаях злоумышленником осознанно или нет, оказывается сотрудник организации, который знаком с режимом работы и мерами защиты.

С целью нарушения статической целостности злоумышленник может:

* Ввести неверные данные
* Изменить данные

Угрозами динамической целостности являются, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений.

Основные угрозы конфиденциальности

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример — нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Для наглядности данные виды угроз так же схематично представлены ниже на рис 1.

Рис. 1. Классификация видов угроз информационной безопасности

Для применения наиболее оптимальных мер по защите, необходимо провести оценку не только угроз информационной безопасности но и возможного ущерба, для этого используют характеристику приемлемости, таким образом, возможный ущерб определяется как приемлемый или неприемлемым. Для этого полезно утвердить собственные критерии допустимости ущерба в денежной или иной форме.

Каждый кто приступает к организации информационной безопасности, должен ответить на три основных вопроса:

1. Что защищать?
2. От кого защищать, какие виды угроз являются превалирующими: внешние или внутренние?
3. Как защищать, какими методами и средствами?

Принимая все выше сказанное во внимание, Вы можете наиболее полно оценить актуальность, возможность и критичность угроз. Оценив всю необходимую информацию и взвесив все «за» и «против». Вы сможете подобрать наиболее эффективные и оптимальные методы и средства защиты.