**Понятие информационной безопасности**

Словосочетание "информационная безопасность" в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин "информационная безопасность" используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Законе РФ "Об участии в международном информационном обмене" (закон утратил силу, в настоящее время действует "Об информации, информационных технологиях и о защите информации") информационная безопасность определяется аналогичным образом – как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

В данном случае внимание будет сосредоточено на хранении, обработке и передаче информации вне зависимости от того, на каком языке (русском или каком-либо ином) она закодирована, кто или что является ее источником и какое психологическое воздействие она оказывает на людей. Поэтому термин "информационная безопасность" будет использоваться в узком смысле, так, как это принято, например, в англоязычной литературе.

**Основные понятия**

* **Информация** — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
* **Носитель информации** — физическое лицо или материальный объект, в том числе физическое поле, в которых информация находит своё отображение в виде символов, образов, сигналов, технических решений и процессов.
* **Собственник информации** — субъект, в полном объёме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.
* **Владелец информации** — субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.
* **Пользователь (потребитель) информации**— субъект, пользующийся информацией, полученной от её собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.
* **Информационной безопасностью** мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Таким образом, правильный с методологической точки зрения подход к проблемам ИБ начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Из этого довольно очевидного положения можно вывести два важных следствия:

**1)** Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные военные организации и учреждения образования. В первом случае «пусть лучше всё сломается, чем враг узнает хоть один секретный бит», во втором — «да нет у нас никаких секретов, лишь бы всё работало».

**2)** Информационная безопасность не сводится исключительно к защите от несанкционированного доступа (НСД) к информации. Субъект информационных отношений может пострадать (понести убытки) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в обслуживании клиентов. Более того, для многих открытых организаций (например, учебных) собственно защита от НСД стоит по важности отнюдь не на первом месте.

**Понятие об информации**

Как упоминалось выше

**Информация** — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информация есть характеристика не сообщения, а соотношения между со­общением и его потребителем. Без наличия потребителя, хотя бы потенциального, говорить об информации бессмысленно.

В случаях, когда говорят об автоматизированной работе с информацией посредством каких-либо технических устройств, обыч­но в первую очередь интересуются не содержанием сообщения, а тем, сколько символов это сообщение содержит.

Применительно к компьютерной обработке данных под информацией понима­ют некоторую последовательность символических обозначений (букв, цифр, закодиро­ванных графических образов и звуков и т. п.), несущую смысловую нагрузку и пред­ставленную в понятном компьютеру виде. Каждый новый символ в такой последовательности символов увеличивает информационный объем сообщения.

Информация может существовать в виде:

* текстов, рисунков, чертежей, фотографий;
* световых или звуковых сигналов;
* радиоволн;
* электрических и нервных импульсов;
* магнитных записей;
* жестов и мимики;
* запахов и вкусовых ощущений;
* хромосом, посредством которых передаются по наследству признаки и свойства организмов, и т. д.

Предметы, процессы, явления материального или нематери­ального свойства, рассматриваемые с точки зрения их информацион­ных свойств, называются информационными объектами.

На свойства информации влияют как свойства данных, так и свойства методов её обработки.

1. **Объективность информации.**Понятие объективности информации относительно. Более объективной является та информация, в которую методы обработки вносят меньше субъективности. Например, в результате наблюдения фотоснимка природного объекта образуется более объективная информация, чем при наблюдении рисунка того же объекта. В ходе информационного процесса объективность информации всегда понижается.
2. **Полнота информации.**Полнота информации характеризует достаточность данных для принятия решения. Чем полнее данные, тем шире диапазон используемых методов их обработки и тем проще подобрать метод, вносящий минимум погрешности в информационный процесс.
3. **Адекватность информации.**Это степень её соответствия реальному состоянию дел. Неадекватная информация может образовываться при создании новой информации на основе неполных или недостоверных данных. Однако полные и достоверные данные могут приводить к созданию неадекватной информации в случае применения к ним неадекватных методов.
4. **Доступность информации.**Это мера возможности получить информацию. Отсутствие доступа к данным или отсутствие адекватных методов их обработки приводят к тому, что информация оказывается недоступной.
5. **Актуальность информации.**Это степень соответствия информации текущему моменту времени. Поскольку информационные процессы растянуты во времени, то достоверная и адекватная, но устаревшая информация может приводить к ошибочным решениям. Необходимость поиска или разработки адекватного метода обработки данных может приводить к такой задержке в получении информации, что она становится ненужной.

**Необходимость и цели защиты информации**

Практически любой пользователь персонального компьютера так или иначе сталкивался с угрозой. Угрозу для информации могут представлять вредоносные компьютерные программы (вирусы, троянцы), сбои в работе полезного программного обеспечения, непосредственно ошибки самого пользователя, перебои с электроэнергией и т.п. факторы. Соответственно, защита компьютерной информации является одной из важнейших областей всей сферы информационных технологий.

Средства и методы защиты компьютерной информации

Методы, способы и средства по защите компьютерной информации можно разделить по типам угроз, против которых они призваны бороться, хотя во многом различные средства могут пересекаться между собой:

* Защита от воздействия вредоносных программ, повреждающих или похищающих информацию с компьютера, в основном строится на использовании ПО, предупреждающего и блокирующего деятельность таких вредителей — антивирусы, антитрояны, фаервалы. Чаще всего современное решение по защите информации будет включать в себя все эти компоненты. Антивирус призван не допустить уничтожения информации, антитрояны и фаервалы — не дать ее похитить. Важно помнить, что и на мобильных устройствах следует использовать [мобильный антивирус](http://dimio.org/avg-vypustila-antivirus-dlya-os-android.html).
* Основной метод защиты информации от ошибок ПО, неверных действий пользователя или перебоев в подаче электроэнергии остается неизменным много лет — это резервное копирование. Иметь резервную копию важных данных полезно в любом случае, поскольку такой метод защиты позволит безболезненно пережить и вирусную атаку, и разрушительные действия злоумышленника. Важно следовать двум правилам — резервные копии необходимо делать регулярно и хранить их следует на отдельном независимом носителе.
* Шифрование компьютерных данных также относится к комплексному методу их защиты — позволяет предотвратить негативные последствия в случае преднамеренной или случайной утечки данных, может помешать работе программ-вредителей (например троянцев, настроенных на кражу паролей или номеров кредитных карт). Применение шифрования вместе с резервным копированием дает все основания не беспокоиться за сохранность информации.

**Цель** – это желаемый результат построения системы защиты, задачи – то, что надо сделать для достижения цели. Целью защиты информации является обеспечение информационной безопасности. Понятие информационной безопасности не менее многогранно, чем понятие самой информации, и зависит от контекста, в котором применяется.

Более детально цели защиты информации перечислены в Федеральном законе "Об информации, информатизации и о защите информации":

* предотвращение утечки, хищения, утраты, искажения, подделки информации;
* предотвращение угроз безопасности личности, общества, государства;
* предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
* предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
* защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
* сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
* обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения

Важно понимать, что система защиты информации не может обеспечить стопроцентную защиту. Задается определенный уровень информационной безопасности, который отображает допустимый риск ее хищения, уничтожения или изменения.

Все меры защиты информации по способам осуществления подразделяются на:

* правовые (законодательные);
* морально-этические;
* технологические;
* организационные (административные и процедурные);
* физические;
* технические (аппаратурные и программные).

Среди перечисленных видов защиты базовыми являются правовая, организационная и техническая защита информации.

**Правовая защита** - защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением. К правовым мерам защиты относятся законы РФ, указы и другие нормативно-правовые акты.

К **морально-этическим мерам** относятся устоявшиеся в обществе нормы поведения. В отдельных случаях они могут быть оформлены в письменном виде, например, уставом или кодексом чести организации. Соблюдение морально-этических норм не является обязательным и носит скорее профилактический характер.

**Организационные меры защиты** – меры организационного характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой. Среди базовых организационных мер по защите информации можно выделить следующее:

* Формирование политики безопасности;
* Регламентация доступа в помещения;
* Регламентация допуска сотрудников к использованию ресурсов информационной системы и др.
* Определение ответственности в случае несоблюдения требований информационной безопасности.

**Физическая защита** представляет собой совокупность средств, препятствующих физическому проникновению потенциального злоумышленника в контролируемую зону. Ими могут быть механические, электро- или электронно-механические устройства различного типа.

**Техническая защита информации** - защита информации, заключающаяся в обеспечении не криптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств. Важно обратить внимание, что техническая защита – это не только защита от утечки информации по техническим каналам утечки, но и защита от НСД, от математического воздействия, от вредоносных программ и т.п.