Проблемы защиты информации.

Широкое применение компьютерных технологий в автоматизированных системах обработки информации и управления привело к обострению проблемы защиты информации, циркулирующей в компьютерных системах, от несанкционированного доступа. Защита информации в компьютерных системах обладает рядом специфических особенностей, связанных с тем, что информация не является жёстко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Известно очень большое число угроз информации, которые могут быть реализованы как со стороны внешних нарушителей, так и со стороны внутренних нарушителей. Проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на три основных типа: **·**перехват информации – целостность информации  сохраняется, но её конфиденциальность нарушена; **·** модификация информации – исходное сообщение изменяется  либо полностью подменяется другим и отсылается адресату; **·**подмена авторства информации. Данная проблема может иметь серьёзные последствия. Например, кто-то может послать письмо от вашего имени или Web – сервер может притворяться электронным магазином, принимать заказы, номера кредитных карт, но не высылать никаких товаров. Исследования практики функционирования систем обработки данных и вычислительных систем показали, что существует достаточно много возможных направлений утечки информации и путей несанкционированного доступа в системах и сетях. В их числе: **·** чтение остаточной информации в памяти системы после выполнения санкционированных запросов; **·**копирование носителей информации и файлов информации с преодолением мер защиты; **·** маскировка под зарегистрированного пользователя; **·** маскировка под запрос системы; **·** использование программных ловушек; **·** использование недостатков операционной системы; **·** незаконное подключение к аппаратуре и линиям связи; **·** злоумышленный вывод из строя механизмов защиты; **·** внедрение и использование компьютерных вирусов.

***Информационная безопасность*** - защищенность информации и *поддерживающей инфраструктуры* от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб* субъектам информационных отношений. В вычислительной технике понятие безопасности подразумевает и надежность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в неё изменений неуполномоченными лицами, и сохранение тайны переписки при электронной связи.

***Защита информации*** – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Угрозы *информационной безопасности* – это оборотная сторона использования информационных технологий.

Информационная безопасность, зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

*составляющие информационной безопасности:****доступность****,****целостность****и****конфиденциальность*** информационных ресурсов и *поддерживающей инфраструктуры*.

***Доступность*** – это возможность за приемлемое время получить требуемую информационную услугу. Особенно ярко ведущая роль доступности проявляется в системах управления – производством, транспортом и т.п. Неприятные последствия может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Под ***целостностью*** подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

***Конфиденциальность*** – это защита от несанкционированного доступа к информации.

**Основные определения и критерии классификации угроз**

***Угроза*** - это потенциальная возможность определенным образом нарушить информационную безопасность.

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 - перебой электропитания) приходится 13% потерь, нанесенных информационным системам.

Одним из опаснейших способов проведения *атак* является внедрение в *атакуемые* системы *вредоносного программного обеспечения*.

По механизму распространения различают:

* ***вирусы*** - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
* ***"черви"*** - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации *вируса* требуется запуск зараженной программы).

На втором месте по размерам ущерба (после *непреднамеренных ошибок* и упущений) стоят *кражи* и *подлоги*.

Информационные сообщения и (или) материалы средства массовой информации, распространяемые через сеть Интернет, должны будут иметь гиперссылку на первоисточник информации или на средство массовой информации, ранее разместившее эти информационные сообщения и (или) материалы. Указ впервые регламентирует механизм ограничения доступа к информации по требованию пользователя интернет-услуг. Например, по запросу пользователя интернет-услуг поставщик обязан ограничить доступ принадлежащего этому пользователю абонентского устройства к информации, содержание которой направлено на распространение порнографических материалов, пропаганду насилия, жестокости и других деяний, запрещенных законодательством.

Несмотря на то, что на страже безопасности граждан стоят законы, надежность работы компьютерных систем во многом опирается на меры самозащиты.

Для защиты информации от вирусов используются общие и программные средства.

*К общим средствам*, помогающим предотвратить заражение и его разрушительные последствия, относят:

резервное копирование информации (создание копий файлов и системных областей жестких дисков);

входной контроль программных средств. Чаще всего вирусы распространяются вместе с компьютерными программами, очень часто полученными по Internet. Не следует запускать непроверенные файлы;

перезагрузка компьютера перед началом работы, если за этим компьютером работали другие пользователи;

ограничение доступа к информации, например, физическая защита дискеты во время копирования файлов с неё.

*К программным средствам* защиты относят разные антивирусные программы (антивирусы).

**Антивирус** – это программа, выявляющая и обезвреживающая компьютерные вирусы. Антивирусные программы могут выявлять и уничтожать лишь известные вирусы, при появлении нового компьютерного вируса защиты от него не существует до тех пор, пока для него не будет разработан свой антивирус.

Решение проблем защиты электронной информации базируется в основном на использовании криптографических методов. Притом современные методы криптографического преобразования сохраняют исходную производительность автоматизированной системы, что является немаловажным. Это является наиболее эффективным способом, обеспечивающим конфиденциальность данных, их целостность и подлинность. Использование криптографических методов в совокупности с техническими и организационными мероприятиями обеспечивают надежную защиту от широкого спектра угроз.

Основные проблемы защиты информации при работе в компьютерных сетях, можно условно разделить на три типа: перехват информации (нарушение конфиденциальности информации), модификация информации (искажение исходного сообщения или замена другой информацией), подмена авторства (кража информации и нарушение авторского права).

Сегодня защита компьютерных систем от несанкционированного доступа характеризуется возрастанием роли программных и криптографических механизмов по сравнению с аппаратными. Новые проблемы в области защиты информации уже требуют использования протоколов и механизмов со сравнительно высокой вычислительной сложностью.

В результате общедоступности информации в сети internet, выявляется слабость традиционных механизмов и отставание применения современных методов защиты. Криптография расширяет возможности защиты информации и обеспечивает её безопасность в сети. Стратегически правильным решением проблемы защиты информации, является использование достижений криптографии.

Отсутствие достаточного количества средств защиты информации на внутреннем рынке долгое время не позволяло осуществлять мероприятия по защите данных в необходимых масштабах. Усугублялась ситуация и отсутствием достаточного количества специалистов в области защиты информации, поскольку их подготовка велась с учетом требований специальных организаций.

В заключение можно сделать вывод: важной особенностью использования информационных технологий является необходимость эффективных решений проблемы защиты информационного ресурса, что предполагает рассредоточение мероприятий по защите данных среди пользователей. Основными направлениями защиты информации должно быть обеспечение защиты помещения от несанкционированных доступов и утечки от персонала входящие в состав организации, у которых есть доступ в зп и утечки по техническим каналам. Это самый рациональный и эффективный принцип защиты интересов организаций, что является первичной ячейкой на пути решения проблемы защиты информации и интересов государства в целом.