1-лекция.

Введение. Цель и задачи дисциплины

Целью дисциплины является раскрытие сущности и значения информационной безопасности и защиты информации в телекоммуникационных системах, их классификация и характеристика, а также ознакомление с основами теории кодирования и передачи информации, криптографии, методами и средствами защиты информации.

Основные задачи:

- раскрытие базовых положений и методологии информационной безопасности и защиты информации в телекоммуникационных системах;
- ознакомление с основными видами и источниками атак на информацию;
- определение целей и принципов защиты информации, установление и раскрытие сущности компонентов защиты информации;
- освоение методов и средств защиты информации в телекоммуникационных системах;
- освоение основ криптологии.

В настоящее время над проблемой защищенности передаваемой по сетям информации работает большое количество специалистов практически во всех экономически развитых странах мира. Можно сказать, что информационная безопасность сформировалась в отдельную быстро развивающуюся дисциплину. Однако, несмотря на усилия многочисленных организаций, занимающихся защитой информации, обеспечение информационной безопасности продолжает оставаться чрезвычайно острой проблемой. Насколько остро стоит сейчас проблема обеспечения безопасности в сетях говорит тот факт, что американские специалисты пришли в настоящее время к выводу: преступления в системах обработки и передачи данных превратились в национальное бедствие. Необходимо отметить, что "электронный грабеж" приобрёл организованную форму и международный характер: "хаккеры" (киберпреступники) во многих странах (например, в Германии и Японии) уже имеют свои клубы, выпускают свои собственные журналы, в которых ведётся обмен опытом по преодолению защиты компьютерных систем. Существенную опасность для систем обработки и передачи информации представляют специальные программы, получившие название "компьютерного вируса", внедрение которых как непосредственно в компьютерную сеть, так и по каналам телекоммуникаций, позволяет решать практически все задачи "электронного бандитизма", связанные с несанкционированным получением информации, ее физическим уничтожением, модификацией программного обеспечения.

Особо широкий размах получили преступления в системах телекоммуникаций, обслуживающих банковские и торговые учреждения. По оценкам специалистов в США, например, убытки от несанкционированного проникновения в эти системы оцениваются в десятки миллионов долларов, причем, цена каждого такого проникновения составляет от 100 тыс. до 1,5 млн. долларов. Участились случаи хищения программных средств. Эти хищения приняли характер эпидемии, т.к. на каждую законную копию, имеющую сколько-нибудь широкое распространение, в настоящее время существует по меньшей мере четыре (по некоторым оценкам более десяти), полученные незаконным путем. Зарубежные журналисты приводят в

последнее время многочисленные факты преступлений, связанных с несанкционированным доступом к системам обработки и передачи информации. Так, например, агенство "Рейтер" в марте 1987 г. сообщило, что со счетов автомобильной компании Volkswagen бесследно исчезли 260 млн. долларов. По словам представителя компании, преступникам удалось обеспечить доступ к компьютерному центру и внести коррективы в программы, осуществляющие расчеты доходов и расходов компании.

Опасность несанкционированных злоумышленных действий в системах обработки и передачи информации является весьма реальной, а проблема обеспечения безопасности в каналах телекоммуникации становится все более значимой и актуальной.

Достижения последних лет в области вычислительной техники, электроники и связи позволяют сегодня по-новому подойти к проблеме безопасности в каналах телекоммуникаций, обеспечив широкое внедрение технологии защиты информации и популяризацию знаний в вопросах технического закрытия информации.

Проблемы защиты информации и несанкционированного доступа к ней приняли антагонистический характер в постановке, известной из теории игр. Применительно к проблеме защиты информации это означает, что для ее решения требуется не просто разработка частных механизмов защиты, а организация целого комплекса мер теоретического и практического характера по защите в широком понимании этого понятия, т.е. создание и использование комплекса специальных средств, методов и мероприятий с целью предотвращения потери информации, находящейся в КС и в каналах телекоммуникаций.

В этом смысле сегодня рождается новое научное направление и новая современная технология - технология защиты информации, обрабатываемой в КС и передаваемой по каналам телекоммуникаций, в область влияния которой попадают не только каналы связи, но и центры коммутации, периферийные устройства, терминалы, администраторы связи и т.п.

Однако, несмотря на большой интерес со стороны потенциальных пользователей, специфические особенности проблемы обеспечения безопасности и высокая стоимость технических средств защиты долгое время ограничивали коммерческое внедрение и широкую публикацию в отечественной печати.

Теоретической основой решения вопросов безопасности в каналах связи является **информатика** - отрасль науки, *изучающая законы, методы и средства сбора, хранения, обработки и передачи информации с помощью компьютеров*.

Необходимо отметить, что понятие "информация" в информатике рассматривается в узком, практическом аспекте, а именно - *под информацией понимаются все сведения, являющиеся объектом хранения, преобразования и передачи*.

В то же время нельзя забывать о том, что **информатика** является лишь обеспечивающим звеном в общей системе научных основ управления, которые опираются на теоретический фундамент **кибернетики**.

В свою очередь теоретическим базисом информатики является **теория информации**, которая входит на правах самостоятельного раздела в кибернетику и включает *методы математического описания и исследования информационных процессов различной природы, методы передачи, обработки, хранения, извлечения и классификации информации в различных областях деятельности*.

Создание любой КС невозможно без разработки и оптимизации алгоритмического обеспечения.

Основой алгоритмического обеспечения в КС является **теория алгоритмов** - раздел математики, изучающий *процедуры (алгоритмы) вычислений и математические объекты, которые могут быть определены на базе методов теорий множеств, отношений и функционалов*.

Причем, наиболее важными для решений проблем КС являются такие разделы этой теории, как **теория вычислительных процедур** и **теория сложности алгоритмов.**

Эти две теории послужили основой создания в рамках информатики раздела, именуемого **прикладной теорией алгоритмов** и *изучающего математические модели дискретных систем*, входящих в состав систем управления.

Построение сложных территориально распределенных КС предполагает необходимость *исследования не только методов и алгоритмов обработки, накопления и хранения информации, но и методов ее передачи между отдельными элементами системы*.

Это обстоятельство обуславливает использование при исследовании и разработке КС методов **теории передачи информации, теории кодирования** и **криптологии.**

Теория передачи информации является разделом теории информации, изучающим методы оценивания качества и оптимизации систем связи и систем передачи данных.

Теория кодирования является разделом теории информации, изучающим вероятностные и сложностные аспекты кодирования информации.

Криптология является разделом теории информации, который изучает методы преобразования информации для обеспечения ее секретности и методы анализа засекреченной информации.

Совокупность этих теорий, хотя и охватывает различные области организации скрытной передачи данных в КС, тем не менее *не позволяет структурировать проблему обеспечения безопасности информации и проводить анализ процессов во всех аспектах функционирования системы* (морфологическом, функциональном, информационном и прагматическом).

Следовательно, *возникает необходимость формирования нового прикладного научного направления* – ***основ теории безопасности и защиты КС,*** интегрирующей основные научные положения прикладной теории алгоритмов, теории передачи информации, теории кодирования, криптологии и *с единых системных позиций изучающей методы предотвращения случайного или преднамеренного раскрытия, искажения или уничтожения хранимой, обрабатываемой и передаваемой информации в КС, функционирующих на базе средств вычислительной техники*.

В связи с тем, что *новое научное направление* строится на основе синтеза методов нескольких разделов кибернетики и информатики, исследует информационные процессы, протекающие в КС, и ориентирована, прежде всего, на средства автоматизированной обработки и передачи данных, то по своему содержанию оно *должно входить в информатику в качестве самостоятельного раздела с четко обозначенной предметной областью*, которая, в качестве основных направлений, должна охватывать: теоретические основы безопасности и защиты КС,

- методы и средства обеспечения безопасности КС,
- методы и средства обеспечения безопасности телекоммуникаций в КС, а

также ряд сопутствующих направлений, таких, например, как вопросы стандартизации и сертификации методов и средств защиты и др.