**Введение**

Проблема защиты информации уходит корнями в давние времена. Уже тогда люди начали разрабатывать способы защиты информации. Например, в V—IV веках до нашей эры в Греции применялись шифрующие устройства. Такое устройство (по описанию древнегреческого историка Плутарха) состояло из двух палок одинаковой толщины, которые назывались сциталами и находились у двух абонентов, желающих обмениваться секретными сообщениями. На сциталу по спирали наматывалась без зазоров узкая полоска папируса, и в таком состоянии наносились записи. Потом полоску папируса снимали и отправляли другому абоненту, который наматывал ее на свою сциталу и получал возможность прочесть сообщение. Элемент, обеспечивающий секретность в таком шифрующем устройстве - диаметр сциталы.

Но в то же время вместе с техническими методами защиты информации разрабатывались и методы ее обхода. Так древнегреческий философ Аристотель предложил использовать длинный конус, на который наматывалась лента с зашифрованным сообщением. В каком-то месте начинали просматриваться куски сообщения, что и позволяло определить диаметр сциталы и, соответственно, расшифровать все сообщение.

Несомненно, что способы защиты информации со временем меняются, как меняется наше общество и технологии. Появление компьютеров и их распространение привело к тому, что большинство людей и организаций стали хранить информацию в электронном виде. Следовательно, возникла потребность в защите такой информации.

В настоящее время актуальность защиты информации связана с ростом возможностей вычислительной техники, а также требованиями со стороны государственных органов обеспечивать защиту в соответствие с определенными нормами и требованиями. Эти требования в Российской Федерации устанавливают такие нормативные документы как приказы ФСТЭК, постановления правительства России, приказы ФСБ России, Федеральные законы,

В современном обществе информация может быть не только помощником, но и оружием. Распространение компьютерных систем и объединение их в коммуникационные сети усиливает возможности электронного проникновения в них. Во всех странах мира существует проблема компьютерной преступности, что вызывает необходимость привлечения все большего внимания и сил для организации борьбы с данным видом преступлений. Особенно большой размах преступления получили в автоматизированных банковских системах и в электронной коммерции. По зарубежным данным, потери в банках в результате компьютерных преступлений ежегодно составляют многие миллиарды долларов.

В связи с массовым внедрением компьютеров во все сферы деятельности человека объем информации, которая хранится в электронном виде, вырос в тысячи раз, а с появлением компьютерных сетей даже отсутствие физического доступа к компьютеру не дает гарантии сохранности информационных ресурсов. Все больше появляется специализированных средств защиты информации, которые ориентированы на решение, как правило, только одной задачи обеспечения безопасности системы или в редких случаях, некоторого ограниченного набора задач. Так, организациям, чтобы оградить себя от "компьютерных" преступлений приходится реализовывать целый набор мер. Расширение применения современных информационных технологий делает возможным распространение различных злоупотреблений, связанных с использованием вычислительной техники.

Каждый сбой работы компьютерной сети это не только "моральный" ущерб для работников предприятия и сетевых администраторов. По мере развития технологий электронных платежей, "безбумажного" документооборота и других, серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем на сегодняшний день.

Для уменьшения ущерба нужно грамотно выбирать меры и средства обеспечения защиты информации от кражи, умышленного разрушения, несанкционированного доступа, порчи, чтения и копирования. Необходимо знание основных законодательных положений в этой области, экономических, организационных и иных мер.

Технологии компьютерных систем и сетей развиваются очень быстро и, соответственно, также быстро появляются новые способы защиты информации.

Актуальность темы моей выпускной квалификационной работы «Методы и средства защиты информации в сетях» не вызывает никаких сомнений, так как без знания и квалифицированного применения методов и средств защиты информации нельзя достигнуть необходимого уровня информационной безопасности компьютерных систем и сетей.

Объект исследования - информация, передаваемая по телекоммуникационным сетям.

Предмет исследования - информационная безопасность сетей.

Основной целью выпускной квалификационной работы является изучение и анализ методов и средств защиты информации в сетях.

Для достижения указанной цели требуется решить ряд задач.

Во-первых, анализ потенциальных угроз в компьютерных сетях при реализации программных злоупотреблений, во-вторых, исследование и анализ методов и средств защиты информации, и, в-третьих, особенности защиты информации в отдельной корпоративной сети (на примере Государственного учреждения - Управления пенсионного фонда по Кстовскому району (ГУ-УПФР)). В качестве отправной точки для исследования выделенных задач мною использовались материалы открытых публикаций Internet, а также работы: Биячуева Т.А., Ясенева В.Н., Безбогова А.А., Исаева А.Б., Лукашина В. И., Родичева Ю.А., Хорева П. Б., Шаньгина В.Ф. и др.

При написании второй главы мною была использована работа, написанная во время прохождения практики в ГУ-УПФР.