**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.

Сегодня 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.

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. Этот набор мер в Российской Федерации устанавливают такие нормативные документы как приказы ФСТЭК, приказы ФСБ России, Федеральные законы и другие.

Каждый сбой или отклонение в работе компьютерной сети это не только "моральный" ущерб для работников предприятия и сетевых администраторов, но угроза прекращения функционирования целых сегментов банковских систем, что может привести к ощутимым материальным потерям.

Для уменьшения ущерба нужно грамотно выбирать меры и средства обеспечения защиты информации от кражи, умышленного разрушения, несанкционированного доступа, порчи, чтения и копирования.

Так, например, перехваченное сообщение о сбое или отклонении в работе системы может быть использовано злоумышленниками с целью нанесения вреда предприятию или получению собственной выгоды.

Актуальность темы моей выпускной квалификационной работы обусловлена необходимостью защитить технологическую информацию, передаваемую в рамках рабочего процесса в общедоступных сетях, ввиду важности быстроты реакции на нее, по каналам связи с повышенным риском из-за возможности ее перехвата. Не смотря на то, что защита технологической информации не закреплена ни в одном нормативном документе, использование ее лицами, для которых она не предназначена, влечет за собой как репутационные, так и потенциальные финансовые риски.

**Пример?**

Ситуация 1. В системе произошло критическое отклонение, исправление которого требует согласование с начальником отдела сопровождения. Из-за того, что важная информация не может быть передана безопасно на личный телефон, приходится использовать рабочий или домашний компьютер, на котором организовано удаленное подключение. Доступ к этим устройствам начальник имеет далеко не всегда. Допустим, он отошел в магазин, за это время произошло отклонение, о котором начальник узнает только когда вернется из магазина и получит доступ к компьютеру, за это время может произойти влияние на клиента, что повлечет ущерб для всего банка.

Объект исследования - информация, передаваемая по телекоммуникационным сетям.

Предмет исследования - информационная безопасность сетей.

**Основной целью** выпускной квалификационной работы является разработка программного комплекса для защиты информации при ее передачи.

Для достижения указанной цели требуется решить ряд задач.

Во-первых, анализ возможных вариантов решения основной цели, во-вторых, исследование и анализ методов и средств защиты информации, и, в-третьих, особенности защиты информации в отдельной корпоративной сети (на примере Публичного акционерного общества "Сбербанк России"). В качестве отправной точки для исследования выделенных задач мною использовались материалы открытых публикаций Internet, а также работы: … каких то людей.

При написании второй главы мною была использована работа, написанная во время прохождения практики в ПАО “Сбербанк”.