**Введение**

Защита информации всегда была и остается актуальной ввиду ее важности в различных сферах жизни человека, начиная от желания защитить свои личные тайны, заканчивая необходимостью защиты интересов целого государства.

Одним из первых шифрующих устройств можно считать сциталу, которая появилась в описании древнегреческого поэта Архилоха, жившего в 7 веке до н. э. Сцитала представляет собой устройство, состоящее из двух одинаковых по толщине палок, которые и назывались сциталами и находились у собеседников, желающих защитить свою переписку от посторонних глаз.

Для того чтобы воспользоваться сциталой, необходимо было плотно намотать на нее узкую полосу папируса, а затем нанести на нее текст сообщения. После этого полосу снимали и передавали другому собеседнику, который в свою очередь также наматывал полоску на аналогичную сциталу. Секретным в этом случае считается диаметр сциталы, так как он обеспечивает невозможность прочтения сообщения в обычном виде.

Однако вместе с методами защиты информации параллельно разрабатывались и методы для ее обхода. Так древнегреческий философ Аристотель придумал, как можно обойти защиту сциталы. Он предложил наматывать перехваченный пергамент с зашифрованным сообщением на длинный конус. Таким образом, в определенном месте текст сообщения начинал приобретать смысл, тем самым можно было определить секретный ключ – диаметр сциталы, а значит, и расшифровать секретное послание.

Очевидно, что со временем и уровнем развития технологий способы защиты информации меняются. Большим толчком к этому послужило появление компьютеров. Удобство в использовании и многозадачность этого вида техники привело к тому, что большая часть людей и предприятий предпочитают хранить свою информацию в электронном виде, вследствие чего возникла потребность в защите этой информации.

На сегодняшний день информация может не только помочь, но и навредить. Повсеместное использование локальных компьютерных сетей и объединение их в глобальные сети увеличивает возможности их несанкционированного использования. Все страны мира каждый день сталкиваются с постоянным потоком “компьютерных” преступлений, что требует привлекать больше внимания и сил для организации борьбы с этим видом преступлений. Основываясь на отчетах и прогнозах международной компании “Group-IB”, специализирующейся на предотвращении кибератак можно сделать вывод о том, что существенный размах компьютерные преступления получили в автоматизированных банковских системах.

Повсеместная интеграция компьютеров увеличивает объем хранимой в электронном виде информации. С появлением локальных и глобальных сетей даже отсутствие непосредственного физического доступа к компьютеру не гарантирует сохранность хранящихся на нем ресурсов. Это влечет за собой появление все большего количества специализированных средств защиты информации, которые, как правило, ориентированы на решение только одной задачи обеспечения безопасности системы. Так, организациям, чтобы обеспечить защиту от "компьютерных" преступлений приходится реализовывать большой набор мер. Этот набор в Российской Федерации устанавливают Государственные органы на основании Федеральных законов (ссылка) и подзаконных нормативных правовых актов (ссылки).

Каждый сбой или отклонение в работе компьютерной сети это не только "моральный" ущерб для работников предприятия и сетевых администраторов, но и 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.

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 информацию об инцидентах, передаваемую в рамках рабочего процесса в сети "Интернет", 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.

Рассмотрим пример. В системе произошел критический инцидент: перестали вычитываться заявки на получения кредитов. Исправление, которое необходимо внести 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 произошел инцидент, о котором начальник узнает только когда вернется из магазина и получит доступ к компьютеру, за это время может произойти влияние на клиента (наберется критическая масса нерассмотренных заявок), что повлечет репетиционный и финансовый ущерб для всего банка.

Основной целью выпускной квалификационной работы является нахождение оптимального варианта решения проблемы: передача важной информации в общедоступной сети.

Достижения указанной цели требует решить ряд определенных задач.

Во-первых, проанализировать возможные варианты решения основной цели, во-вторых, исследовать и проанализировать методы и средства защиты информации, и, в-третьих, рассмотреть задачи защиты информации в отдельной корпоративной сети (на примере Публичного акционерного общества "Сбербанк России"). В качестве отправной точки для исследования поставленных задач мною использовались материалы общедоступных публикаций сети "Интернет".

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