# ВОПРОСЫ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

*Студент* **Хакимова Е.Р., Лыскова Л.А.**
*(науч. руководитель* **ассист. Шопенская Т.В.)**

В данный момент, к сожалению, в Украине актуальна проблема безопасности электронных платежей. Так в Киеве были зафиксированы случаи незаконного снятия денежных средств по средствам банкомата. Поэтому остро стоит проблема обеспечения безопасности совершения электронных платежей.

Для определения общих проблем защиты систем Обмена Электронными Данными (ОЭД) рассмотрим прохождение документа при ОЭД.

Можно выделить три основных этапа:

1. подготовка документа к отправке;
2. передача документа по каналу связи;
3. прием документа и его обратное преобразование.

Одно из наиболее уязвимых мест в системе ОЭД - пересылка платежных и других сообщений между банками, или между банком и банкоматом, или между банком и клиентом.

При пересылке платежных и других сообщений возникают следующие проблемы:

1. внутренние системы организаций Получателя и Отправителя должны быть приспособлены к получению/отправке электронных документов и обеспечивать необходимую защиту при их обработке внутри организации;
2. взаимодействие Получателя и Отправителя документа осуществляется опосредованно- через канал связи.

Это порождает три типа проблем:

1) взаимного опознавания абонентов;
2) защиты документов, передаваемых по каналам связи;
3) защиты самого процесса обмена документами.

С технической точки зрения эти проблемы решаются с помощью нескольких механизмов, отвечающих за обеспечение адекватной безопасности электронных банковских систем. Работа большинства этих механизмов обеспечивается службами сети с

расширенным набором услуг (Value-Added Network, VAN). Службы, реализующие ОЭД, должны выполнять следующие функции:

1. обеспечить защиту от случайных и умышленных ошибок;
2. обеспечить адаптацию к частым изменениям количества пользователей, типов оборудования, способов доступа, объемов трафика, топологии.
3. полнота решения рассмотренных выше проблем сильно зависит от правильного выбора системы шифрования. Система шифрования (или криптосистема) представляет собой совокупность алгоритмов шифрования и методов распространения ключей.

Правильный выбор системы шифрования помогает:

1. скрыть содержание документа от посторонних лиц (обеспечение конфиденциальности документа) путем шифрования его содержимого;
2. обеспечить совместное использование документа группой пользователей системы ОЭД путем криптографического разделения информации и соответствующего протокола распределения ключей. При этом для лиц, не входящих в группу, документ недоступен;
3. в настоящее время в мире существует большое количество систем электронных платежей. Наиболее известная из них: Безопасность в системе S.W.I.F.T. (The Society for Worldwide Inter-bank Financial Telecommunication) обеспечивается применением организационных, программных и технических мер.

В системе SWIFT существует строгое разделение ответственности за поддержание безопасности системы. Так банк, подключенный к системе, отвечает за правильную эксплуатацию и физическую защиту терминалов, модемов и линий связи до регионального процессора, за правильное оформление сообщения при передаче его в сеть и наличие работоспособных терминалов.

SWIFT- бесприбыльное кооперативное международное сообщество, целью которого является организация межбанковских расчетов по всему миру.

Так как в Украине программа SWIFT используется не так широко как на международном уровне, мы предлагаем банкам постепенно переходить на данную программу, так как в реализации защиты SWIFT отражены основные подходы, которые применяются при организации системы электронных платежей в целом.