Саидов Х.З.
Первый заместитель директора
Департамента безопасности и защиты
инфомации ЦБ РУз

Система безопасности банковской системы Республики Узбекистан.

По мере развития и расширения сферы применения средств вычислительной техники острота проблемы обеспечения безопасности вычислительных систем и защиты хранящейся и обрабатываемой в них информации от различных угроз все более возрастает. Для этого есть целый ряд объективных причин.

Основная причина - возросший уровень применения автоматизированных систем обработки информации. Им доверяют самую ответственную работу, от которой зависит жизнь и благосостояние многих людей. ЭВМ управляет техническими процессами на предприятиях и атомных электростанциях, движениями самолетов и поездов, выполняют финансовые операции, обрабатывают конфиденциальную информацию.

Сегодня проблемы защиты вычислительных систем становятся еще более значительными в связи с развитием и расширением сетей ЭВМ. Распределенные системы и системы с удаленным доступом выдвинули на первый план вопрос защиты обрабатываемой и передаваемой информации.

Доступность средств вычислительной техники, и, прежде всего, персональных ЭВМ. привела к распространению компьютерной грамотности в широких слоях населения. Это, в свою очередь, вызвало многочисленные попытки вмешательства в работу государственных и коммерческих систем, как со злым умыслом, так и из чисто "спортивного" интереса.

Многие из этих попыток имели успех и нанесли значительный урон владельцам информации и вычислительных систем.

Поэтому понятным и естественным выглядит их желание обезопасить себя и свою информацию от подобных угроз.

В немалой степени это касается разных коммерческих структур и организаций, особенно тех, кто по роду своей деятельности хранит и обрабатывает ценную (в денежном выражении) информацию, затрагивающую к тому же интересы большого количества людей.

Надежная защита автоматизированных систем особенно необходима банкам и другим крупным финансовым организациям. Более того, им нужна тщательно спланированная и постоянно поддерживаемая защита. Это обуславливается следующими факторами;

1) хранимая и обрабатываемая в банковских системах информация представляет собой реальные деньги. На основании информации компьютера могут производиться выплаты, выдаваться кредиты, переводиться значительные суммы. Вполне понятно, что незаконное манипулирование такой информацией может привести к серьезным убыткам;

2) информация в банковских системах затрагивает интересы большого количества людей и организаций - клиентов банка. Как правило, она конфиденциальна, и банк несет ответственность за обеспечение требуемой степени секретности перед своими клиентами. Естественно, клиенты вправе ожидать, что банк должен заботиться об их интересах, в противном случае он рискует своей репутацией со всеми вытекающими отсюда последствиями.

Современный банк трудно представить без автоматизированной информационной системы.

Связь компьютеров между собой и с более мощными компьютерами, а также с ЭВМ других банков - также необходимое условие успешной деятельности банка -слишком велико количество операций, которые необходимо выполнять в течении короткого периода времени.

Для того, чтобы эффективно противостоять всем потенциальным угрозам, банки должны иметь стройную концепцию безопасности, четко определяющую основные понятия и ключевые аспекты данной сферы.

I. Цель и задачи банковской безопасности.

Под безопасностью коммерческого банка понимается состояние защищенности интересов владельцев, руководства и клиентов банка, материальных ценностей и информационных ресурсов от внутренних и внешних угроз. Состояние защищенности представляет собой умение и способность кредитной организации надежно противостоять любым попыткам криминальных структур или недобросовестных конкурентов нанести ущерб законным интересам банка.

Очевидно, что обеспечение безопасности информации представляет крайне сложную задачу и требует специфических организационных, охранных и кадровых мероприятий, а порой и значительной поддержки со стороны правоохранительных органов.

В 1994 году Постановлением Кабинета Министров Республики Узбекистан в составе Центрального банка был создан Департамент безопасности и защиты информации. Главной целью департамента является обеспечение устойчивого функционирования банковской системы и предотвращение угроз ее безопасности, защита законных интересов банков от противоправных посягательств, недопущения хищения финансовых и материально-технических средств, уничтожения имущества и ценностей, разглашения, утраты, утечки, искажения и уничтожения служебной информации, нарушения работы технических средств.

Другими целями являются:

- определение путей реализации мероприятий, обеспечивающих необходимый уровень надежной защищенности объектов;
- повышение имиджа банков и роста прибыли за счет обеспечения высокого качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов.

Для достижения вышеизложенных целей в составе коммерческих банков были организованы службы безопасности и защиты информации, деятельность которых координируется Центральным банком.

Основными задачами по обеспечению безопасности коммерческих банков являются:

- прогнозирование и своевременное выявление и устранение угроз безопасности персоналу и ресурсам банка; причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развитию;
- отнесение информации к категории ограниченного доступа (служебной, банковской и коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования), а других ресурсов - к различным уровням уязвимости (опасности) и подлежащих сохранению;
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявление негативных тенденций в функционировании банков;
- эффективное пресечение угроз персоналу и посягательств на ресурсы на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерным действиям физических и юридических лиц, ослабление

негативного влияния последствий нарушения безопасности на достижение стратегических целей банков.

II. Основные объекты и субъекты безопасности, источники угроз банковской информации.

Стабильная деятельность современного банковского учреждения невозможна без надежного обеспечения информационной безопасности. Многие преступления начинаются с утечки информации. Даже безопасность самих банковских работников непосредственно связана со степенью защиты банковской информации. Если банк хорошо охраняется, налажен режим па рабочих местах, введена надежная система защиты информации, то возможность криминального вмешательства в деятельность банка практически исключается.

Основными объектами, подвергающимися угрозам являются.

- персонал, среди которого в первую очередь можно выделить руководящих работников; производственный персонал, имеющий непосредственный доступ к валюте, ценностям, хранилищам, а также осведомленный в сведениях, составляющих банковскую и коммерческую тайну; работники внешнеэкономических служб;
- финансовые средства, валюта, драгоценности, материальные ценности;
- информационные ресурсы с ограниченным доступом, составляющие служебную и коммерческую тайну, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, информативные физические поля различного характера;
- средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии телеграфной, телефонной, факсимильной, радио- и космической связи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы), новейшие технологии;
- материальные средства (здания, сооружения, хранилища, техническое оборудование, транспорт и иные средства);
- технические средства и системы охраны и защиты материальных и информационных ресурсов.

Все объекты, в отношении которых могут быть осуществлены угрозы безопасности или противоправные посягательства, имеют различную потенциальную уязвимость с точки зрения возможного материального или морального ущерба. Исходя из этого они должны быть классифицированы по уровням уязвимости (опасности), степени риска.

При решении проблем безопасности, между собой взаимодействуют следующие субъекты:

- государство - как собственник ресурсов, создаваемых, приобретаемых и накапливаемых за счет средств государственных бюджетов, а также информационных ресурсов, отнесенных к категории государственной тайны;
- Центральный банк, осуществляющий денежно - кредитную политику страны;
- коммерческий банк как юридическое лицо, являющееся собственником финансовых, а также информационных ресурсов, составляющих служебную, коммерческую и банковскую тайну;
- другие юридические и физические лица, в том числе партнеры и клиенты; службы безопасности коммерческих банков.

Наибольшую уязвимость представляют финансовые и валютные средства, особенно в процессе транспортировки, а также информационные ресурсы и некоторые категории персонала.

Основные источники угроз безопасности информации в компьютерных системах - мошенничество, саботаж персонала, действия профессиональных хакеров, ошибки в деятельности человека и сбои оборудования системы.

Злоумышленники разрабатывают множество комбинаций для хищения средств. Наиболее распространенной техникой банковского мошенничества стала схема, получившая за рубежом название "атака салями". Она заключается в аккумулировании остатков денежных сумм, образующихся за счет округления счетов и процентных операций по ним.

Акты саботажа могут возникнуть в результате недовольства работников своим служебным или материальным положением, а также психических расстройств. Своими действиями подобные сотрудники могут уничтожить или исказить информацию, привести к потере способности нормального функционирования компьютерной системы и другим диверсиям.

Анализ состояния защищенности банковской информации в западных странах показал, что эти вопросы американские и европейские банки решили одновременно с вопросами стандартизации систем кодирования банковских операций и финансовых сообщений. Создав в 1973 году общество СВИФТ (SWIFT - Society for Worldwide Interbank Financial Telecommunication), западные банки - члены СВИФТ перешли на международный стандарт использования компьютеров и средств телекоммуникаций в банковском деле, обеспечивающий более надежную, быструю и безопасную систему передачи информации. Средства обеспечения безопасности СВИФТ контролируют процедуры подключения терминалов к сети, обеспечивают регистрацию и шифрование сообщений, контролируют достоверность сообщений и источника информации.

Ряд ведущих западных банков защищают главные компьютеры своих сетей устройствами. Эти устройства, выполняющие роль сетевого контроллера, управляют модемами, проверяют телефонные номера абонентов, подключающихся к сети, регистрируют успешные и безуспешные попытки соединения с центральной электронно-вычислительной машиной.

В 1996 году в Узбекистане была внедрена собственная система электронных платежей (СЭП) (безбумажная технология платежей), участниками которой являются Центральный банк, все коммерческие банки Республики Узбекистан, Главный Центр информатизации и расчетно-кассовые центры Главных территориальных управлений Центрального банка

Система электронных платежей объединяет локальные сети участников посредством Банковской телекоммуникационной сети (БТС). Данная сеть позволяет осуществлять передачу между всеми субъектами банковской системы электронных платежных документов, электронных сообщений и другой информации. Система защиты БТС Центрального банка построена в соответствии с проектом, который предусматривает защиту информации от вторжения из вне (установлено межсетевой экран типа брандмауэр), защиту информации локальной сети от несанкционированных пользователей, строгую аутентификацию (установление подлинности сообщения источника данных) участника СЭП, защиту информации при передаче по каналам связи (шифрация информации), безопасность информации по свойствам конфиденциальности и целостности при передаче посредством проставление электронной цифровой подписи.

Система защиты информации совместно с другими службами операционной системы выполняет следующие функции:

1. Идентификация, аутентификация и авторизация субъектов и объектов системы.

Эти функции необходимы для подтверждения подлинности субъекта, законности его прав на данный объект или на определенные действия, а также для обеспечения работы субъекта в системе;

2. Контроль входа пользователя в систему и управление паролями;

3. Регистрация и протоколирование. Аудит.

Эти функции обеспечивают получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля, а также регистрацию действий, признанных администрацией потенциально опасными для безопасности системы;

4. Контроль доступа.

Контроль осуществляется при доступе к: оперативной памяти; распределяемым устройствам прямого доступа; распределяемым устройствам последовательного доступа; распределяемым программам и подпрограммам; разделяемым наборам данных.

Для защиты информации от несанкционированного доступа во всех компьютерах пользователей системы установлены программно-аппаратные средства Dallas Lock, которые имеют сертификат Государственной технической комиссии при Президенте Российской Федерации и имеет показатели защищенности от несанкционированного доступа к информации по 3 классу защищенности. Кроме того, все компьютерное и телекоммуникационное оборудование соответствует международному сертификату ISO 9000. Используемые маршрутизаторы CISCO имеют международные сертификаты и сертификат соответствия Госстандарта России.

Межсетевой экран WatchGuard FireBox имеет сертификат соответствия Гостехкомиссии России.

Вся система в целом отвечает стандарту:

ISO-17799 - комплексный подход к информационной безопасности. Технические, организационные, административные меры обеспечивающие конфиденциальность, целостность, достоверность и доступность информации. Телекоммуникационная связь:

ISO-7498-2 Взаимосвязь открытых систем. ISO-9735 безопасность обмен данными. ISO\IEC-10745 модель безопасности верхнего уровня. Методы криптографии:

ISO-2382-2-76 обработка данных

ISO-9796-91 цифровая подпись с восстановлением сообщения.

ISO-14888 цифровая подпись с приложением

Оконечное шифрование информации и проставление электронной подписи выполняется аппаратно-программным комплексом (АПК) при помощи устройств TouchMemory DS 1994, объемом памяти 390 байт, вмещающем 5 байт информации. АПК поддерживает способы защиты данных на основе алгоритмов DES (64 бит), RSA (N-5 12 бит и E-256 бит), Г ОСТ (256 бит), Эль-Гамаля, Шамира, а также алгоритм открытого распространения ключей Диффи-Хелмана.

АПК имеет сертификат Республики Беларусь и сертификат соответствия Российской Федерации.

Генерация и замена ключей шифрации и электронно-цифровой подписи выполняется Центром распространения ключей, расположенным в Головном офисе Центрального банка. Периодичность обновления - раз в полгода.

III. Правовые основы системы безопасности

Правовые основы безопасности банковской системы определяют соответствующие положения Конституции Республики Узбекистан, законов «О Центральном банке», «О банках и банковской деятельности», а также ряд нормативных актов Центрального банка.

Правовая защита персонала банков, материальных и экономических интересов банков и их клиентов от преступных посягательств обеспечивается на основе норм уголовного и уголовно-процессуального кодексов.

Защиту имущественных и иных материальных интересов и деловой репутации коммерческих банков призваны обеспечивать также гражданское, гражданско-процессуальное, хозяйственное и хозяйственно-процессуальное законодательство.

Правовую основу безопасности кредитных отношений банков с клиентами составляют законодательные акты, регулирующие возможность применения различных способов обеспечения исполнения обязательств, таких как удержание, залог, поручительство и банковская гарантия.

Обеспечение информационной безопасности в банковской системе регулируется рядом законов, среди которых закон «О банках и банковской деятельности», «Об информатизации», нормативные акты Центрального банка.

В настоящее время Центральным банком Республики Узбекистан разработан проект Закона «Об электронных платежах», целью которого является придание правового статуса электронным платежам. Данный проект определяет основные понятия в сфере электронных платежей, содержит требования, предъявляемые к электронному платежному документу, условия его обработки, требования и правила защиты, службы защиты, а также определяет орган призванный контролировать деятельность по защите электронных платежей и в этом качестве определен Центральный банк Республики Узбекистан. Также необходимо придат законный статус электронной подписи. Для этого надо принимать закон "Об Электронно цифровой подписи". Принятие этих законопроектов позволит заполнить пробел правовой основы информационной безопасности банковской системы в Республике Узбекистан.

Необходимо отметить, что наличие прочной законодательной основы для осуществления всего комплекса мероприятий по обеспечению защиты коммерческих банков является одним из основных факторов, позволяющих государственным и иным правоохранительным и охранным структурам организовывать противостояние противоправным посягательствам на банковскую безопасность в различных ее аспектах.