

СИСТЕМА ЗАЩИТЫ БАНКОВСКОЙ ИНФОРМАЦИИ

Рассмотрены вопросы обеспечения информационной безопасности банковских информационных систем. Выявлены основные факторы, которые необходимо учитывать при построении систем информационной безопасности в банковской сфере. Определена общая структура системы защиты банковской информации.

С развитием электронных технологий в финансовой сфере для банков наиболее остро встала проблема обеспечения информационной безопасности. В данном случае под информационной безопасностью понимают защищенность банковской системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, модификации или разрушения ее компонентов.

Информационная безопасность обеспечивается конфиденциальностью, целостностью и доступностью данных – АИС-триада (Availability, Integrity, Confidentiality) [1].

Стратегия информационной безопасности банков весьма сильно отличается от аналогичных стратегий других компаний и организаций. Это обусловлено, прежде всего, специфическим характером угроз, а также публичной деятельностью банков:

- Хранимая и обрабатываемая в банковских системах информация представляет собой реальные деньги.
- Информация в банковских системах затрагивает интересы большого количества людей и организаций – клиентов банка.
- Конкурентоспособность банка зависит от того, насколько клиенту удобно работать с банком, а также насколько широк спектр предоставляемых услуг, включая услуги, связанные с удаленным доступом.
- Информационная безопасность банка (в отличие от большинства компаний) должна обеспечивать высокую надежность работы компьютерных систем даже в случае нештатных ситуаций.
- Банк хранит важную информацию о своих клиентах, что расширяет круг лиц, заинтересованных в краже или порче такой информации.

Для обеспечения защиты информации, общим для всех видов информационных систем, являются следующие подсистемы [2]:

- подсистема контроля доступа;
- подсистема регистрации и учета;

- подсистема обеспечения целостности;
- подсистема межсетевой безопасности.

В случае подключения к сети Интернет необходимо дополнительно использовать следующие подсистемы:

- подсистема антивирусной безопасности;
- подсистема обнаружения вторжений;
- подсистема анализа защищенности.



Рис. 1 – Структура системы защиты банковской информации

Необходимо использовать криптографию при передаче данных по незащищенным каналам связи, а также, ЭЦП, для подтверждения подлинности данных.

С каждым годом все больше возрастает количество вирусов, сетевых атак, злоумышленников, возникают угрозы нарушения конфиденциальности информации внутри банка, что приводит к финансовым потерям. Поэтому решение вопросов защиты данных в современных информационных системах является наиболее актуальным и будет успешным только при условии использования комплексного подхода к построению системы защиты информации.

1. Зегжда, Д. П., Ивашко, А. М. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2000. – 452 с.
2. Корт, С.С. Теоретические основы защиты информации / С. С. Корт. – М.: Гелиос АРВ, 2004. – 240 с.

Крюковский Александр Михайлович, студент 5 курса факультета информационных технологий и управления Белорусского государственного университета информатики и радиоэлектроники, alex_krykovsky@mail.ru.

Научный руководитель: Столбанов Николай Андреевич, ассистент кафедры систем управления Белорусского государственного университета, dekitu@bsuir.by.