Секция «6. Экономическая и информационная безопасность: проблемы»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ФИНАНСОВО-КРЕДИТНЫХ И ДРУГИХ ОРГАНИЗАЦИЯХ

Сидарук Екатерина Константиновна
Студент
Финансовый университет при Правительстве РФ, Факультет финансов и кредита, Москва, Россия
E-mail: katerina.sidaruk@yandex.ru

Научный руководитель
к. ф.-м. н. Савина Светлана Владимировна

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ФИНАНСОВО-КРЕДИТНЫХ И ДРУГИХ ОРГАНИЗАЦИЯХ

Сидарук Е. К.
Финансовый университет при
Правительстве Российской Федерации,
г. Москва
Научный руководитель: к. ф.-м. н. Савина С.В.

Развитие информационных технологий и внедрение их во все сферы деятельности влечет за собой не только повышение качества жизни и ведения бизнеса, но и порождает новые проблемы – проблемы информационной безопасности. С каждым годом увеличивается количество компьютерных преступлений, в том числе трансграничных, возрастают их корыстная направленность, наносимый ими материальный ущерб. Информационные технологии все чаще используются для совершения традиционных преступлений – хищений, вымогательств, мошенничества и террористической деятельности.

Важнейшей частью информационной безопасности любого государства является информационная безопасность в банковской деятельности. Вопросы обеспечения информационной безопасности каждого банка являются жизненно важными в силу ряда причин:

с точки зрения информационной безопасности банк как сосредоточение «живых» денег – организация повышенного риска, незаконное манипулирование с информацией из автоматизированной системы которой может привести к серьезным убыткам;

современный банк предоставляет большое число сервисов, связанных с удаленным доступом к его информационной системе (персональный интернет-банкинг, интернет-доступ к финансовым рынкам, электронный документооборот и многое другое). С этих позиций банк – «точка пересечения» публичных сетей (Интернет) и коммерческих финансовых сетей;

банки обладают сложными информационными системами, которые включают большой набор «бэк-офисных» и «фронт-офисных» приложений, нередко гетерогенных, а управление ими осложняется территориальной распределенностью, наличием у банков филиалов и дополнительных офисов. При этом информационная система современного банка является основой функционирования почти всех его основных бизнес-процессов;

банк хранит персональные данные граждан и конфиденциальную информацию своих клиентов – юридических лиц;

банки выполняют особую роль посредников при расчетах экономических субъектов. Негативные последствия сбоев в работе даже отдельных кредитных организаций в принципе могут привести к развитию кризиса платежной системы страны.

Указанные причины заставляют предъявлять жесткие требования к защите информационной системы современного банка.

Проблема защиты банковской информации и формирования систем информационной безопасности – одна из самых актуальных в настоящее время. Активное участие в развитии указанного направления принимает Банк России, регулярно публикуя стандарты в области информационной безопасности.

Проблемы защиты информации в банке связаны, прежде всего, с обширностью и емкостью информации, с разнообразием и техническими характеристиками используемого аппаратного обеспечения и территориальной удаленностью информационных каналов для пользователей информации.

Проанализировав возможные угрозы надлежащему хранению информации в банке, Ларина И.О. и Мазулина Т.Ю. составили рейтинг (на основе мнения специалистов) значительности угроз:

преднамеренное хищение информации внутри организации;

халатность сотрудников, допустивших утечку информации;

аппаратные и программные сбои;

вредоносные программы;

внешнее финансовое мошенничество;

хакерские атаки;

стихийные бедствия и катаклизмы.

По данным сайта Securitylab.ru, в мире еженедельно регистрируется около 9 крупных утечек информации, совокупный ущерб от которых достигает от сотен тысяч до десятков миллионов долларов. И подобных примеров сотни. До сих пор памятна одна из наиболее крупных утечек информации, произошедшая в 2006 г. и коснувшаяся более 10 крупных российских банков. На нелегальном рынке в продаже появилась база, содержащая данные о 3 миллионах заемщиков. В нее входили информация об отказах по кредитам и стоп-листы банков, а также об имени заемщика, адресе, телефоне, месте работы и причине попадания в базу (просрочка по кредиту, отказ в выдаче кредита и другие строго конфиденциальные данные, например, наличие судимости).

Организационные мероприятия и процедуры, используемые для решения проблемы безопасности переработки информации, необходимо решать на всех этапах проектирования и в процессе эксплуатации автоматизированных информационных технологий (АИТ).

Средства обеспечения безопасности процессов переработки информации, используемые для создания механизма зашиты, подразделяются на формальные и неформальные. Если рассматривать неформальные средства защиты, можно выделить:

– организационные, представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты обработки информации;

– законодательные, которые определяются законодательными актами страны, регламентирующими правила пользования, обработки и передачи информации ограниченного доступа и устанавливающими меры ответственности за нарушение этих правил;

– морально-этические, которые реализуются в виде всевозможных норм и правил.

Также необходимо использование инновационных механизмов контроля доступа, осуществляющего проверку полномочий объектов АИТ (программ и пользователей) на доступ к ресурсам сети. При доступе к ресурсу через соединение контроль выполняется как в точке инициации, так и в промежуточных точках, а также в конечной точке. Механизмы обеспечения целостности данных применяются как к отдельному блоку, так и к потоку данных. Целостность блока является необходимым, но недостаточным условием целостности потока. Целостность блока обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке. Однако описанный механизм не позволяет вскрыть подмену блока в целом. Поэтому необходим контроль целостности потока, который реализуется посредством шифрования с использованием ключей, изменяемых в зависимости от предшествующих блоков. Аутентификация может быть односторонней и взаимной. В первом случае один из взаимодействующих объектов проверяет подлинность другого, тогда как во втором случае проверка является взаимной.

Таким образом, без надлежащей организационной поддержки программно-технических средств защиты переработки информации от несанкционированного доступа и точного выполнения предусмотренных проектной документацией процедур в должной мере не решить проблему обеспечения безопасности переработки информации, какими бы совершенными эти программно - технические средства не были.

Литература

1. Ларина О.И., Мазулина Т.Ю. Некоторые аспекты создания системы информационной безопасности в банке // Деньги и кредит. – 2012. -№7. – С.61-64.

2. Дьяконов Б.П. Информационная безопасность в банках // Банковское дело. – 2008. – 11. – С. 86-88.

3. Лузин А.И. Инновационные способы обеспечения информационной безопасности на предприятии // Теория и практика общественного развития. – 2011. – №2.