Савельева Александра Сергеевна
Белорусский государственный экономический университет

О защите информации в банковских сетях

В современном мире важность проблемы обеспечения безопасности компьютерных систем и защиты хранящейся в них информации растёт день ото дня. Это обусловлено многими причинами, самыми главными из которых являются развитие и распространение информационных технологий, их доступность и популярность. Эти факторы привели к тому, что каждый желающий может попытаться вмешаться в работу вычислительных систем какого-либо предприятия, и чаще всего с преступными намерениями.

Проблема создания надёжной системы защиты информации особенно актуальна для банков и других финансовых организаций. В первую очередь это связано с тем, что на основе информации, хранимой в банковских компьютерах, можно производить платежи, открывать кредиты или переводить большие суммы денежных средств. Другими словами, обрабатываемая в банковских системах информация представляет собой реальные деньги. Её незаконное использование может привести к значительным убыткам. Вторая причина заключается в том, что данная информация затрагивает интересы людей и организаций, банк ответственен за обеспечение её конфиденциальности. Отсутствие защиты приведёт не только к убыткам, но и к потере репутации и доверия со стороны клиентов.

Банки, как основа мировой рыночной экономики, всегда были, есть и будут объектом преступного интереса. И особенно это опасно в век развития высоких технологий, когда при должном оборудовании и навыках совершить вмешательство в работу банковской системы можно не выходя из дома.

В связи с вышеизложенной информацией, в данной работе будет рассмотрено понятие безопасности и её видов, типы наиболее частых угроз банковской информации и основные методы её защиты.

Существует несколько подходов к определению безопасности автоматизированной системы обработки информации (АСОИ). Одно из наиболее полных определений сформулировал один из основателей научно-исследовательского предприятия «Информзащита», Владимир Гайкович: «Безопасность АСОИ есть её свойство, выражающееся в способности противодействовать попыткам нанесения ущерба владельцам и пользователям системы при различных возмущающих воздействиях на неё» [1]. Следует также отметить, что воздействия на систему могут быть совершенно различного рода: стихийные бедствия, ошибки персонала, поломки составных частей системы или злоумышленное проникновение в систему.

Все действия по обеспечению безопасности системы всегда направлены на достижение трёх её базовых принципов: целостности данных, т.е. обеспечения достоверности и защищенности информации, на основе которой принимаются решения, от возможных непреднамеренных или умышленных искажений; конфиденциальности информации, т.е. защиты засекреченных данных от утечки; и доступности нужной информации для авторизованных пользователей для решения нужных задач в нужное время [2].

Безопасность автоматизированных банковских систем традиционно делится на внутреннюю и внешнюю. Внешняя безопасность отвечает за защиту системы от стихийных бедствий (пожаров, землетрясений и т.д.), а так же от проникновения в систему извне с целью хищения информации, нарушения её целостности или вывода системы из строя. Внутренняя безопасность, в свою очередь, отвечает за стабильную отлаженную и корректную работу всей системы и её составных частей.

Умышленное нарушение функционирования системы чаще всего приводит к большим убыткам и значительному урону компьютерной системе, и именно поэтому самые опасные угрозы банковской информации связаны с проникновением в систему третьих лиц. Рассмотрим подробно наиболее распространенные из них [1]:

— *Несанкционированный доступ* (НСД, unauthorized access) – самый популярный вид компьютерных атак, который заключается в получении человеком доступа к информации, на которую у него нет прав.

— *Атака «салями»* (salami attack) – одна из самых опасных атак для банков. Суть её заключается в том, что при обработке счетов используются целые единицы исчисления (один доллар, двадцать центов и т.д.). Злоумышленник проникает в систему и с помощью специальной программы округляет сумму $10,549867 до $10,54, тогда как банковская система округлила бы до $10,55. Таким образом, преступник получает прибыль, равную 1 центу. В крупных банках ежедневно обрабатывается огромное количество счетов, и, соответственно, в таких масштабах размер хищения довольно велик.

— *«Маскарад»* (masquerade) – суть этой атаки заключается в присвоении чужих прав и привилегий, выполнении действий от чужого лица. Так как банковские данные представляют собой реальные деньги, урон может быть весьма ощутимым.

— *«Сборка мусора»* (garbage collecting) – атака направлена на хищение и манипуляцию остаточной информацией, которая так или иначе всегда остаётся в оперативной памяти после окончания работы до её полного уничтожения или перезаписи. Примерами остаточной информации могут служить файлы, отправленные в «Корзину», вместо полного их удаления.

— *Вирус* (computer virus) – программа, обладающая способностью заражения вредоносным кодом других программ. Одним из ярких примеров вирусных программ является «Троянский конь» (Trojan horse), который проникает в компьютер под видом легального программного обеспечения и выполняет дополнительные действия, не предусмотренные и не описанные в соответствующей документации. Ещё одним опасным вирусом является «Червь» (worm), который ищет слабые места и уязвимости системы и направляет свою атаку именно туда. Опасность заключается в том, что «червь» почти не оставляет за собой следов. Главная опасность эти вредоносны программ в том, что вирусы способны к самовоспроизведению и вмешательству в работу системы. Количество существующих сейчас вирусов невозможно оценить, потому что каждый день создаются новые виды и совершенствуются уже имеющиеся.

— *«Захватчики паролей»* (password grabber) – программы, направленные на воровство паролей. Они, к примеру, могут имитировать окно ввода логина и пароля и отсылать данные пользователя злоумышленнику.

Традиционно, меры обеспечения банковской информации делятся на пять видов [2]: правовые, морально-этические, административные, физические и технические.

Правовые (законодательные) меры включают в себя нормативно-правовые акты, законы и указы, регламентирующие правила обращения с информацией и наказание за их нарушение. Таким образом, эти меры являются сдерживающим фактором для правонарушителей.

Под *морально-этическими* методами подразумевают какие-либо нормы поведения, сложившиеся по мере распространения информационных технологий в обществе. Морально-этические нормы бывают неписанными (как нормы честности) или оформленными в какой-либо устав или свод правил. Данные меры не являются обязательными.

Административные нормы являются мерами организационного характера, чья деятельность направлена на предотвращение угроз безопасности. К этим мерам относятся: разработка правил пользования системой; организация скрытого контроля над работой персонала; надёжная пропускная система; мероприятия по набору и подготовке работников; создание системы учёта, хранения, использования и уничтожения конфиденциальной информации.

К *физическим* мерам обеспечения безопасности относят механические, электронные или электронно-механические устройства, призванные создавать препятствия для незаконного проникновения в систему.

Технические (аппаратно-программные) методы включают в себя различные электронные устройства и программы, выполняющие функцию защиты. К ним относят

криптографическое преобразование (шифрование) информации, аутентификацию пользователей, разграничение прав и привилегий, надёжную антивирусную защиту и резервное копирование информации.

Наилучшие результаты достигаются только при комплексном подходе к построению системы защиты, так как все пять методов имеют исключительное значение в обеспечении безопасности системы.

Банки называют кровеносной системой экономики. За счёт своей важности, они привлекают всё увеличивающееся внимание преступников. Надёжная и исправно работающая система защиты невероятно важна для каждого банка, так как на нём лежит огромная ответственность за сохранность конфиденциальности информации о своих клиентах.

Построение адекватной системы защиты банка требует тщательного анализа рисков, планирования, немалых затрат и наличия квалифицированных кадров для её поддержания, так как обеспечение безопасности является непрерывным интерактивным процессом, который не заканчивается до тех пор, пока компьютерная система банка жизнеспособна.

Проблема обеспечения защиты АСОИ особенно остра для стран с развитой инфраструктурой, так как их финансовые организации несут огромные убытки ежедневно.

Основываясь на анализе развития банковской отрасли, можно сделать вывод, что компьютеризация этой сферы продолжает возрастать. Таким образом, в скором времени снизится оборот наличных денег, увеличится количество безналичных расчётов с использованием пластиковых карт и сети Интернет. В связи с этим, обеспечение надёжной защиты станет приоритетным для каждой финансовой организации, а потому индустрия защиты электронной информации продолжит своё динамичное развитие.

Источники литературы

1. Гайкович, Ю.В. Безопасность электронных банковских систем / Ю.В. Гайкович, А.С. Першин. – М.: Единая Европа, 1994. – с. 87.

2. Информационные технологии / В.В.Трофимов [и др.]; под ред. В.В. Трофимова. – М.: Юрайт, 2011. – с. 589.

Савельева Янина Олеговна

Белорусский государственный экономический университет

ИСПОЛЬЗОВАНИЕ WEB-СЕРВИСОВ В ЭКОНОМИКЕ НА ПРИМЕРЕ РАБОТЫ БАНСКОВСКОЙ СИСТЕМЫ

Использование информационных технологий на сегодняшний день является одним из ключевых факторов, влияющих на успех и скорость развития той или иной сферы деятельности человека. То, насколько эффективно работает предприятие, во многом определяется теми техническими средствами и тем программным обеспечением, которыми оно располагает. Нельзя утверждать, что использование самых последних технологий и технических средств решает все проблемы и автоматизирует все процессы, однако инновации могут значительно упростить и ускорить работу.

Скорость передачи информации растет ежедневно, возрастают и технологические мощности. С помощью технических средств люди с разных концов Земли могут общаться друг с другом, сеть Интернет – это один из популярнейших способов связи на сегодняшний день, главным образом потому, что она общедоступна. Также информационные технологии сегодня позволяют людям практически мгновенно получить доступ к необходимой информации, в процесс обмена информацией – это то, на чем строится быстрое и качественное функционирование сферы деятельности человека.

На данный момент информационные технологии в экономике, их изучение и разработка является наиболее актуальной задачей для специалистов. Потому что без