(cc) BY

Горбаченко Юлия Александровна
магистрант
Саенко Виктория Игорьевна
канд. экон. наук, старший преподаватель
НАН ЧОУ ВО «Академия маркетинга
и социально-информационных технологий – ИМСИТ»
г. Краснодар, Краснодарский край

РЕАЛИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ В КРЕДИТНЫХ ОРГАНИЗАЦИЯХ

Аннотация*: в статье рассмотрена проблема обеспечения информационной безопасности и реализация защиты информации в банковской сфере. Авторы приходят к следующему выводу: при решении задач, связанных с защитой информации, необходимо тщательное описание исходных характеристик системы, опирающееся на качественно подготовленные исходные данные.*

Ключевые слова*: защита информации, персональные данные, банковская сфера.*

Одной из наиболее критичных проблем банковской сферы в течение долгих лет была и остается проблема информационной безопасности. Здесь следует отметить, что абсолютно любая ошибка, даже самая незначительная утечка информации влечет за собой тяжелые последствия, которые могут по тяжести своей градуироваться от потерь прямого материального характера и вплоть до ухудшения репутации, как клиента, так и самого банка.

В силу этих обстоятельств, одним из основных потребителей всевозможных систем информационной безопасности был и остается банковский сектор. К слову, бюджетные дотации на решение вопросов, связанных с информационной безопасностью, в компаниях нефинансового сектора в разы ниже, чем выделяемый кредитными организациями.

При формировании и использовании информационных ресурсов Российской федерации, базирующихся на основе сбора, хранения и предоставления потребителям информации в конечном документированном виде, базовым законом является Федеральный Закон «Об информации, информатизации и защите информации». Следующая сфера применения данного федерального закона – создание и использование информационных технологий, участвующих в процессе информатизации. Данный нормативно-правовой акт существует с 1995 году.

Практически, информационная безопасность обеспечивается в среде воздействия факторов, как правило, совершенно неконтролируемых, предусмотреть которые либо весьма непросто, либо невозможно в принципе.

Очевидно, что в современных условиях глобальной информатизации возникновение такого рода факторов заранее предусмотреть на этапе проектирования системы информационной защиты возможным не представляется, что, при отсутствии регулярной технической и информационной поддержки системы, в значительной мере снижает эффективность всего комплекса мер безопасности, предусмотренного на предприятии. Неактуальность методов информационной защиты предприятия, относящегося к банковской сфере, способно скомпрометировать как все предприятие, так и создать отрицательный имидж у потенциальной целевой аудитории.

Нормативно-методическое обеспечение информационной безопасности является на данный момент отнюдь несовершенным. Отсюда следует повышенная сложность, а иногда и невозможность создания действительно эффективной системы информационной безопасности. Именно в банковской сфере информационная безопасность и методы ее обеспечения напрямую является базисом составления требований Стандарта СТО БР ИББС-1.0–2008, регламентирующих методологию оценочного соответствия высокого уровня информационной безопасности.

Неопределенность и фрагментированность – являются неотъемлемыми атрибутами в вопросах проектирования и использования систем информационной

защиты. Но омонимичность в вопросах планирования свойств систем информзащиты обусловлена не только этим фактором.

Это сказывается на том, что в значительной степени неопределенность сопутствует всему этапу проектирования систем информационной защиты. Но по мере прохождения проектом жизненного цикла своего становления и создания, уровень такой неопределенности, как правило, значительным образом снижается.

Следовательно, систему защиты информации с точки зрения ее качества объективно характеризовать, опираясь на действительные возможности ее реализации, разумеется, в прямой зависимости от комплекса условий и списка требований, возникших на начальных этапах проектирования.

Построение моделей при проектировании или модернизации системы защиты информации в банках представляется естественным путем решения задач анализа и проектирования с минимальными затратами и высокой эффективностью. Так, на этапе анализа модель системы защиты информации используется для исследования каждой выполняемой функции (операции), чтобы выявить, например, к какой информации и к каким ресурсам должен иметь доступ каждый сотрудник при выполнении служебных обязанностей.

После моделирования необходимо перейти к этапу анализа защищенности построенной модели информационной системы. Именно здесь возникает целый комплекс теоретических и практических проблем, с которыми сталкиваются разработчики алгоритмов анализа рисков. Практически невозможно автоматически, без участия эксперта, оценить защищенность информационной системы. Таких систем анализа рисков сегодня практически нет, а те, которые существуют, носят обобщенный характер. Следующая проблема – как алгоритмически определить все классы уязвимостей (достаточность) в системе защиты анализируемой системы, как оценить ущерб от всех существующих в системе угроз безопасности и как добиться адекватной оценки совокупного ущерба по всем классам угроз, избежав избыточного суммирования ущербов. И самая сложная проблема: риск –

категория сугубо вероятностная. Как оценить вероятность реализации множества угроз информационной системы?

После определения основных мотивов и целей нарушителя представляется возможным оказать влияние на них или необходимым образом скорректировать требования к системе защиты от данного типа угроз. Вопросы безопасности вычислительных систем – это большей частью вопросы человеческих отношений и человеческого поведения. При анализе нарушений защиты необходимо уделять внимание субъекту (личности) нарушителя. Устранение причин или мотивов, побудивших к нарушению, в дальнейшем может помочь избежать повторения подобного случая.

Модель не должна быть в единственном экземпляре. Рационально наличие нескольких различных моделей, поскольку потенциальные противники банковской информационной безопасности могут преследовать различные цели, следовательно, подходить к вопросу взлома банковских систем различными способами.

Для построения модели нарушителя используется информация от службы безопасности, риск-подразделений и службы внутреннего контроля банка о существующих средствах доступа к информации и ее обработки, о возможных способах перехвата данных на стадии передачи, обработки и хранения, об обстановке в коллективе и на объекте защиты, сведения о конкурентах и ситуации на рынке, об имевших место случаях хищения информации и т. п.

Кроме того, оцениваются реальные оперативные технические возможности злоумышленника для воздействия на систему защиты или на защищаемый объект. Под техническими возможностями подразумевается перечень различных технических средств, которыми может располагать злоумышленник в процессе совершения действий, направленных против системы защиты информации.

Подводя итог, сделаем следующий вывод: при решении задач, связанных с защитой информации, необходимо тщательное описание исходных характеристик системы, опирающееся на качественно подготовленные исходные данные.

В значимой степени немаловажно при этом, что неопределенность подавляющего количества исходных данных неизбежна. Следовательно, очевидна необходимость не только формирования объективных и верных исходных данных для проектирования программного продукта, но и непрерывная их актуализация в течение всего периода разработки.

Любой современный банк в значительной степени заинтересован в обеспечении высокого уровня безопасности своих клиентов. Информатизация общества, а также развитие сервисной составляющей банковского обслуживания, особенно в направлении работы с финансами через интернет и мобильные приложения, привело к значительному обострению вопросов, связанных с информационной безопасностью.

Список литературы

1. Федеральный закон от 27.07.2006 №152-ФЗ (ред. от 21.07.2014) «О персональных данных» (с изм. и доп., вступ. в силу с 01.09.2015).

2. Вишняков И.В. Анализ динамики, надежности коммерческих банков / И.В. Вишняков // Банковское дело. – 1995. – №8.

3. Левиков В.Я. Банки, компьютеры и безопасность: Защита информации / В.Я. Левиков // Конфидент. – 1999. – №4/5.

4. Альшанская Т.В. Применение методов системного анализа специалистами по информационной безопасности / Т.В. Альшанская // Информационные системы и технологии: управление и безопасность: Сб. ст. III международной заочной научно-практической конференции. – Тольятти: Издательство ПВГУС, 2014. – 348 с.

5. Трофимова В.В. Информационные системы и технологии в экономике и управлении / В.В. Трофимова. – М: Юрайт, 2012. – 521 с.