УДК 004.056

О НЕКОТОРЫХ МЕТОДАХ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФИНАНСОВЫХ УЧРЕЖДЕНИЯХ

Л.В. МИХАЙЛОВСКАЯ, Е.В. ВАЛАХАНОВИЧ

Военная Академия Республики Беларусь,
пр-т Независимости, 220, г. Минск, 220057, Республика Беларусь
ludmila_mi@mail.ru

Применение методов оценки рисков информационной безопасности в финансовых учреждениях позволяет выполнить мероприятия по обеспечению защиты информации при условии минимизации затрат на их проведение.

Ключевые слова: информационная безопасность, оценка рисков, защита автоматизированных систем обработки информации.

В настоящее время информация – это один из самых ценных ресурсов. Жизненно важные интересы финансовых учреждений (ФУ), участвующих в процессе автоматизированной обработки и передачи информации, а также предоставления информационных услуг заключаются в том, чтобы определенная часть информации с одной стороны была бы легко доступна, с другой стороны – надежно защищена от неправомерного ее использования.

По этой причине проблема защиты автоматизированных систем обработки информации (АСОИ) в ФУ является достаточно актуальной. Это связано, во-первых, с тем, чтобы обеспечить режим защиты коммерческой тайны и персональных данных клиентов и служащих, во-вторых, чтобы затраты на выполнение данных мероприятий не превышали необходимого ресурса. В целях формирования стратегии по управлению рисками и планированию расходов на проведение мероприятий по защите информации необходимо проводить оценку рисков информационной безопасности.

Под риском в ФУ понимаются возможные потери вследствие воздействия угроз на основные активы (ресурсы): непосредственно информацию, инфраструктуру, персонал, имидж и репутацию. Количество информационных активов может быть очень велико. Поэтому первоочередной задачей управления рисками становится определение наиболее значимых активов и их ценности.

В ходе анализа ценности активов применяются следующие методы оценки риска: в денежном выражении, вероятностный и балльный, которые позволяют определить соответствующий уровень уязвимости для каждой комбинации информационного актива и угрозы ФУ и степень потенциальной опасности угроз.

Для оценки стоимости потерь в денежном выражении используется так называемая «аддитивная модель» [1] ценности информации, когда информация представляется в виде конечного множества элементов и осуществляется экспертная оценка компонент. Отдельные компоненты сравнивают по ценности относительно друг друга. Оценка возможных потерь (оценка риска) строится на основе полученных стоимостей компонент, исходя из прогноза возможных угроз этим компонентам. Возможности угроз оцениваются вероятностями соответствующих событий, а потери подсчитываются как сумма математических ожиданий потерь для компонент по распределению возможных угроз.

При использовании метода вероятностной оценки риска оценивается риск вероятности обхода системы защиты. С этой целью задается формальное описание структуры системы защиты и связности для множества элементов системы защиты и для множества элементов информационных угроз. Математическое описание связности построено на использовании теории графов и алгебраической топологии. Результаты анализа риска представляются как в качественной, так и в количественной формах.

Существует много предложений по оценке риска, основанных на балльном методе, например, в [2, 3]. В то же время, они не учитывают влияния уровней уязвимости системы при действии на нее определенной угрозы. При оценке рисков для ФУ целесообразно определенным категориям угроз присваивать различные значения баллов в зависимости от уровня воздействия угроз. Также присваивается соответствующий балл и уровням уязвимости системы при действии на нее определенной угрозы. Затем производится перемножение баллов воздействия на баллы уязвимости и по результату оценивается уровень риска для системы при воздействии на нее угрозы определенных категории и типа.

Задачами о принятии решений в условиях неопределенности (наиболее непредсказуемые элементы для систем защиты информации – люди: персонал, партнеры, клиенты) занимается теория игр. С помощью теории игр ФУ получает возможность предусмотреть ходы своих партнеров и конкурентов в соответствии с концепцией приемлемого риска. Особенностью такого подхода является использование качественных критериев и характеристик риска, включая оценку влияния на него лиц, принимающих решение (ЛПР). Причем учитывается влияние как ЛПР данного ФУ, так и ЛПР конкурентов. Между ЛПР в составе ФУ и у его конкурентов возникает ситуация игры с противоположными интересами, в рамках которой применяются как вполне законные действия, так и «на грани закона». Наиболее рациональным представляется расчет риска, связанного с однократными событиями, каждое из которых имеет свою вероятность появления и достаточно высокую «стоимость». Сложный инструментарий данной теории следует использовать только при принятии принципиально важных стратегических решений.

Применение приведенных методов по оценке рисков информационной безопасности для ФУ позволяет определить проблемные области обеспечения информационной безопасности и определить оптимальный комплекс мероприятий по защите информации. Если в процессе анализа будет выяснено, что меры по снижению риска малоэффективны и дороги одновременно, то может оказаться экономически более целесообразно застраховать свои действия. При этом будет ставится задача не предотвращения, а возмещения ущерба.

Список литературы

1. *Маслов О.Н.* // Inside. Защита информации. 2011. №4 (40). С. 16–22.

2. *Удалов Н.П.* Методика оценки риска инвестиционного проекта для различных уровней неопределенности проектной информации: Дис. … канд. экон. наук. Москва, 2007.

3. *Макоско А.В., Перемышленников Н.А.* // BIS Journal – Информационная безопасность банков. 2013. №1(8). С. 25–31.