МОДЕЛИРОВАНИЕ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ

Гринева Н.В.

Финансовый университет при Правительстве Российской Федерации,
Россия, г. Москва, Ленинградский просп., 49.
ngrineva@fa.ru

Аннотация: Выявлены наиболее критичные информационные системы Банка, получен список классов угроз. Предложена методика оценки вероятности реализации угроз, прогнозируемого уровня потерь и частоты реализации угрозы, ожидаемого значения ущерба в год для каждого типа нарушений. Предложена система управления рисками и выработаны рекомендации по ее применению.

Ключевые слова: оценка рисков, управление рисками, информационная безопасность, активы компании, ущерб.

Работа выполнена по гранту РФФИ №19-010-00698 на тему: «Развитие теории интеллектуального капитала и методов его оценки в условиях цифровизации экономики».

Введение

Процесс управления рисками информационной безопасности включает в себя идентификацию значимых угроз и критичных информационных систем, проведение первичной оценки, предотвращение развития риска, выбор тактики устранения риска, восстановление безопасности после инцидента, документирование риска, оценку нанесенного ущерба, выработку превентивных и корректирующих мер.

В результате повсеместного распространения электронных платежей, банковских карт, компьютерных сетей, стремительно растущей популярности услуг, предоставляемых клиентам посредством интернет-технологий, значительно увеличилось количество угроз целью воздействия которых является влияние на информацию ограниченного доступа. Угрозы воздействуют на три свойства информационных активов: конфиденциальность, целостность и доступность. Согласно опросу, доля людей, оценивающих риски информационной безопасности «на глазок» около 30%, около 16% людей не оценивают риски или считают это бессмысленным [4].

Основная цель принимаемых мер по управлению рисками информационной безопасности и защите информации состоит в том, чтобы обеспечить целостность, доступность и конфиденциальность информации во всех ее видах и формах.

1 Идентификация риска

Под информационными активами в работе будут пониматься информационные системы Банка, так как в них хранится, обрабатывается и через них передается информация ограниченного доступа. В ходе анализа деятельности Банка были выявлены наиболее критичные информационные системы:

- Система дистанционного банковского обслуживания (ДБО).
- Система автоматического скоринга заёмщиков.
- Система IBSO(IB System Object).
- СистемаSWIFT(Society of Worldwide Interbank Financial Telecommunications).
- Корпоративная электронная почта.
- Система предоставления доступа работников в интернет.
- Система обслуживания банковских карт.

Неблагоприятное событие состоит в реализации угрозы. Разделим угрозы на 5 классов, сформированные относительно свойств информационных активов: конфиденциальности, целостности и доступности. При этом нарушения целостности и доступности проанализируем за два временных промежутка (1 час и 4 часа), таким образом сможем оценить, как изменяется уровень потерь в зависимости от времени. Получаем следующий список классов угроз: К – класс угроз, связанных с нарушением конфиденциальности информационных систем Банка; Ц1 – класс угроз, связанных с нарушением целостности информационных систем Банка в течение 1 часа; Ц2 – класс угроз, связанных с нарушением целостности информационных систем Банка в течение 4 часов; Д1 – класс угроз, связанных с нарушением доступности информационных систем Банка в течение 1 часа; Д2 – класс угроз, связанных с нарушением доступности информационных систем Банка в течение 4 часов.

Наиболее распространенным классом угроз является класс, связанный с нарушениями доступности информационных систем. Среди выявленных угроз самым распространённым видом источников угроз является антропогенный, так как он обусловлен действиями человека. Самой актуальной из внешних угроз является киберугроза [5].

По выявленным угрозам был построен шаблон рисков, в котором выявлены факторы, повышающие и понижающие информационный риск для каждого класса угроз. Список угроз был сформирован при использовании документов: ГОСТ Р ИСО/МЭК 27005-2010 [1] и банка угроз безопасности информации, разработанный Федеральной службой по техническому и экспортному контролю России (ФТСЭК).

2 Оценка риска

Оценка выявленных событий будет проведена относительно критичных информационных систем Банка. Рассчитаны вероятности реализации угроз, прогнозируемый уровень потерь и прогнозируемая частота реализации угрозы в год. Получены формулы для ожидаемого значения ущерба в год для каждого типа нарушений в информационных системах (конфиденциальности/ целостности/ доступности), которое оценивается по-разному.

С помощью вычисления суммы по всем информационным системам получаем прибыль, которую Банк мог бы получить от реализации соответствующих банковских операций. Потерянная прибыль из-за недоступности информационных систем и есть ущерб от угроз нарушения конфиденциальности/ целостности/ доступности.

Для того, чтобы оценить совокупное влияние всех выявленных угроз необходимо провести общую оценку возможных потерь при их одновременной реализации.

Все вышеперечисленные формулы при их объединении в одну систему по своей сути представляют собой методику по оценке вероятности и уровня потерь от реализации угроз. Объединим их в одну систему и отметим, что при условии зависимости параметров от времени уравнения образуют предикативную экономико-математическую модель, которая выглядит следующим образом:

$$Pu_i \quad (1 \quad PPu_i)(1 \quad PDu_i)(1 \quad Cu_i)$$
$$Fu_i \quad Pu_i \quad FOu_i$$
$$Lu_i \quad DЦ_i \quad Fu_i$$
$$DЦ_i \quad DЦ_i \quad Iu$$

(9)

$$\Sigma$$
$$\Sigma \quad \text{ax}\left(L \quad \right) + \Sigma \quad \text{ax}\left(Lu \quad \right) + \Sigma$$

где – вероятность того, что угроза (нарушение Д) соответственно будет реализована; – вероятность того, что угроза (нарушение Ц, Д) соответственно будет предотвращена; PD – вероятность того, что угроза (нарушение Ц, Д) соответственно будет обнаружена; Ck – вероятность того, что угроза (нарушение Ц, Д) не будет реализована из-за сложности реализации; – прогнозируемая частота реализации угрозы (нарушение Д) в год; – прогнозируемая частота возникновения угрозы (нарушение Д) в год; DD, DK, DЦ – ожидаемое значение ущерба от реализации угрозы в год (нарушений К, Ц, Д); – уровень потерь от реализации угрозы (нарушений Д); T – период влияния нарушения на деятельность Банка (в часах); Pr – средняя прибыль от банковской операции в час; Q – коэффициент, учитывающий уровень влияния нарушения доступности информационной системы на банковские операции; – текущий и предыдущий анализируемые периоды; i – количество типов угроз Д или Ц; j – количество информационных активов (систем) Банка.

3 Управление риском

Для выявленных опасных угроз разработаны меры, с помощью которых возможно снизить частоту реализации угрозы в год и потери, которые понесет Банк в случае ее реализации. С целью обеспечения бесперебойной доступности информационной системы, принимаем решение о дополнительных инвестициях в необходимое оборудование – покупка дополнительного оборудования для повышения мощности сервера позволит минимизировать количество простоев банкоматов / терминалов по обслуживанию банковских карт, что минимизирует упущенную выгоду (прибыль по банковским операциям) и, как следствие, потери Банка.

Предполагается, что необходимо сделать единовременные инвестиции на сумму 10 350,0 тыс. руб. Внедрение соответствующего оборудования позволит снизить потери от реализации угрозы Д1 (нарушения доступности системы обслуживания банковских карт в течение 1 часа) на 9 030,911 тыс. руб. ежегодно. С помощью предлагаемой инвестиции, Банк сможет снизить потери чуть больше чем в 2 раза за счет того, что снизит частоту реализации угрозы Д1 в год (вместо 7,02 получаем 3,5) посредством установки покупаемого оборудования в рамках проекта.

Для устранения угрозы нарушения конфиденциальности относительно системы обслуживания банковских карт (К) пойдем по уже рассмотренному пути и инвестируем в требуемое оборудование и системы защиты информации. Оценка строится аналогично: при затратах на инвестиции в 1350,0 тыс. руб. экономия на потерях составит 1130,388 тыс. руб. ежегодно. С помощью предлагаемой инвестиции, Банк сможет снизить потери по угрозе К относительно системы обслуживания банковских карт чуть больше, чем на 30% за счет того, что снизит частоту реализации угрозы в год (вместо 0,7 получаем 0,49).

Затраты на разработку продукта включают в себя только дополнительно оплачиваемые часы ответственным сотрудникам и составят 350 тыс. руб. Ожидаемый эффект от реализации разработки

будет заключаться в снижении частоты сбоев сервера практически в 2 раза (вместо 1,62 получаем 0,81).

Выводы

В работе проведен значительный блок расчетов по всем предлагаемым видам угроз и по всем информационным системам, выделенным для анализа: были оценены такие показатели как вероятность возникновения угрозы, вероятность предотвращения угрозы, вероятность реализации угрозы, сложность реализации угрозы, частота реализации угрозы, ущерб от реализации угрозы и другие.

На основе предлагаемой методики оценки информационного риска Банка сделаны рекомендации по совершенствованию системы обеспечения информационной безопасности Банка, среди которых к наиболее важным стоит отнести построение системы четкого разграничения полномочий сотрудников Банка к информационным системам, обеспечение наличия современных средств информационной защиты (и соответствующего оборудования) для функционирования информационных систем Банка в непрерывном режиме.

Литература

1. ГОСТ Р ИСО/МЭК 27001-2006. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»(утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 N 375-ст).
2. *Гринева Н. В.* Методологические основы управления рисками инвестиционно-инновационного проекта // Экономика и управление: теория и практика. – 2018. – Т. 4, № 4-1. – С. 50–55.
3. *Гринева Н.В.* Моделирование оценки убытков от информационных угроз в банковской отрасли //Актуальные проблемы прикладной математики, информатики и механики :сборник трудов Международной научной конференции, Воронеж, 17–19 декабря 2018 г. – Воронеж : Издательство «Научно-исследовательские публикации», 2019. –720-726с.
4. http://www.iso27000.ru/golosovaniya/plonepopoll.2007-02-01.0594390779
5. https://fstec.ru/