УДК 339.562.4

ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ ЗАО «МТ БАНК»

И. А. Коренкович, С.В. Рогозин,
Белорусский государственный университет, г. Минск

Аннотация. Сегодня спектр предоставляемых банком услуг постоянно растёт и модернизируется, при этом растет и численность пользователей банковскими услугами и продуктами. В таких условиях объемы обрабатываемой информации растут соответствующими темпами. Зачастую, информация, которая попадает в банки от пользователей их услугами и продуктами, носит конфиденциальный характер, и требует усиленного контроля за сохранностью и ограниченностью доступа к ней. Следовательно, актуальной становится тема организации эффективного аудита информационной безопасности в банке и формирование адекватной оценки рисков информационной безопасности. Нечёткая продукционная модель, принадлежащая классу «мягких вычислений», выступает ответом на данный вызов, так как она способна дать оценку риска в условиях большого количества влияющих факторов и неопределенности информации.

Ключевые слова*:* современный банк, аудит информационной безопасности, оценка рисков, нечёткая продукционная модель.

EVALUATION OF INFORMATION RISKS OF MT BANK CJSC

I. A. Korenkovich, S. V. Rogosin,
Belarusian State University, Minsk

Abstract. Today, the range of services provided by the bank is constantly growing and modernizing, while the number of users of banking services and products is also growing. In such conditions, the volume of processed information is growing at an appropriate pace. Often, the information that gets to banks from users of their services and products is confidential, and requires enhanced control over the safety and limited access to it. Consequently, the topic of organizing an effective audit of information security in a bank and the formation of an adequate assessment of information security risks is becoming relevant. A fuzzy production model belonging to the class of “soft computing” is the answer to this challenge, as it is able to give a risk assessment in the face of a large number of influencing factors and information uncertainty.

Keywords*:* modern bank, information security audit, risk assessment, fuzzy production model.

Актуальность темы заключается в необходимости поиска наиболее эффективных методов оценки рисков информационной безопасности банков в сложившейся и прогрессирующей ситуации наличия у банков больших объемов информации, которые требуют сохранности и поддержания определенного уровня конфиденциальности. Так как методы обеспечения информационной безопасности, которые используются в белорусских банках на сегодняшний день, как показывает практика, дают сбои и не всегда способны обеспечить достаточную защищенность данных клиентов банка.

Аудит информационной безопасности определяется как оценка текущего состояния обеспечения безопасности информации и персональных данных, устанавливающая уровень

их соответствия определённым критериям и отраслевым стандартам, и предоставление результатов в виде рекомендаций.

Вопрос состоит в выборе методов оценки риска информационной безопасности. Количественные методы анализа и оценки рисков информационной безопасности, которые преимущественно применяются на белорусских просторах, обладают рядом недостатков. Есть элементы риска, которые никак не учитываются в количественных методах анализа риска информационной безопасности: убыток в результате простоя бизнес-процесса; затраты на создание информации; восстановительная стоимость; будущая стоимость; судебные издержки и некоторые другие составляющие.

Кроме того, есть составляющие риска, которые принципиально не поддаются подсчёту: репутация банка; нанесенные моральный ущерб; влияние риска на сотрудников; влияние риска на акционеров; влияние риска на потребителей; влияние риска на поставщиков и партнеров.

Можно допустить, что эти составляющие могут быть как-то математически оценены и представлены в виде некоторых численных показателей. Однако для этого необходимо проанализировать большое количество разнородных параметров. Исчерпывающее и актуальное количественное описание состояния банка в этом случае получить вряд ли возможно, поскольку за время, необходимое для его получения, положение дел может меняться.

Получаем, что на сегодняшний день для этапа оценки рисков информационной безопасности статистических данных и экспертных оценок недостаточно. Здесь необходимы сложные математические расчёты, которые смогли бы обрабатывать данные о факторах риска, получаемые от экспертов на предыдущих этапах анализа риска информационной безопасности. Такими возможностями обладают методы, использующие элементы искусственного интеллекта (табл. 1).

Таблица 1 – Интеллектуальные подходы к оценке рисков информационной безопасности

Категория	Подходы
Нейронные сети	1. Многослойный перцептрон 2. Метод обратного распространения ошибки 3. Нейронная сеть радиально-базисных функций 4. Вероятностная нейронная сеть 5. Самоорганизованная конкуренция
Обучающий вектор	1. Метод опорных векторов
Мягкие вычисления	1. Приближённые множества 2. «Серые отношения» 3. Генетический алгоритм 4. Нечёткие множества
Гибридные модели	1. Байесовская нечёткая сеть 2. Нейронечёткая сеть 3. Нечётко-приближённые множества 4. Нечёткий метод анализа иерархий 5. Нечёткий метод анализа сетей 6. «Серая иерархическая модель» 7. Нейронная сеть с генетическим алгоритмом

Источник: [1]

Задачей является выбор из существующих такого метода оценки риска информационной безопасности, который обеспечил бы максимальную вероятность адекватной оценки с учётом адаптивности к качественным данным о факторах риска. Из перечисленных в таблице 1 методов оценки риска информационной безопасности для рассмотрения был выбран метод мягких вычислений – нечёткие множества, а именно, нечёткая продукционная модель.

Ниже будет представлена реализация работы нечёткой продукционной модели на примере ЗАО «МТБанк», но для начала некоторые сведения о деятельности Банка.

ЗАО «МТБанк» начал свою деятельность 14 марта 1994 года и является одним из 24 банков, осуществляющих свою деятельность на территории РБ на начало 2020 года. ЗАО «МТБанк» – член Ассоциации белорусских банков, Сообщества всемирных межбанковских финансовых коммуникаций (S.W.I.F.T.), международных платежных систем VISA International и MasterCard. С начала своей деятельности Банк является универсальным и имеет на белорусском рынке репутацию надежного банка. [2]

По состоянию на 01.01.2019 в 7 банках, удельный вес активов в совокупных активах банковского сектора превышает 5% (диаграмма 1). Данные банки отнесены к 1 группе системной значимости. Всего на их долю приходится почти 86,2% всех активов. Большую часть активов банковского сектора составляют активы Беларусбанка (41,8%). Доля активов МТБанка в совокупных активах банковского сектора по состоянию на 01.01.2019 составила 1,58% (11 позиция из 24 банков, или 4 позиция из 6 банков, отнесенных к 2 группе системной значимости).

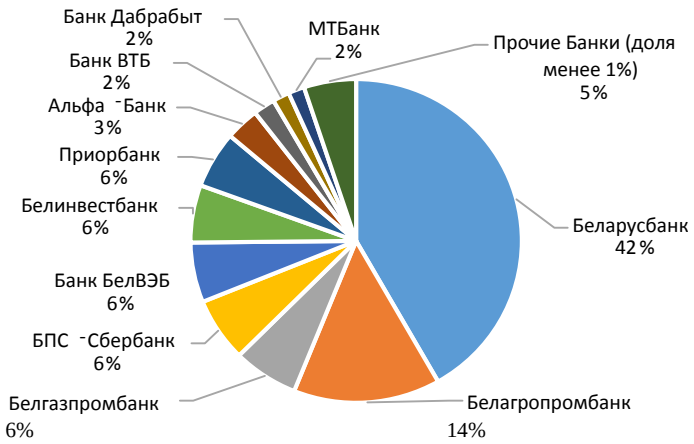

Рисунок 1 - Удельный вес активов в совокупных активах банковского сектора
Источник: собственная разработка

Прирост активов Банка за 2017 год составил 24,1%, за 2018 год – 21,5%. Общий объем активов банка по состоянию на 01.01.2019 составил 1 123 834 тыс. бел. рублей. За период с 01.01.2017 по 01.01.2019 активы банка выросли на 50,8%. [4]

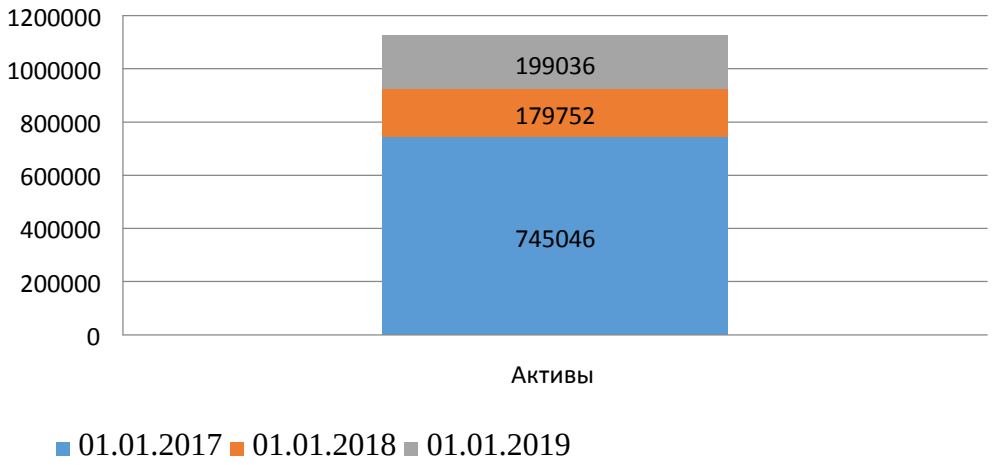

Рисунок 2 -Прирост активов Банка за период с 2017-2019 г.г.

Источник – собственная разработка

Пророст капитала Банка за 2017 год составил 40,2%, за 2018 год – 39,2%. Общий объем капитала по состоянию на 01.01.2019 составил 164 774 тыс. бел. рублей. За период с 01.01.2017 по 01.01.2019 капитал банка увеличился на 95,2 %.

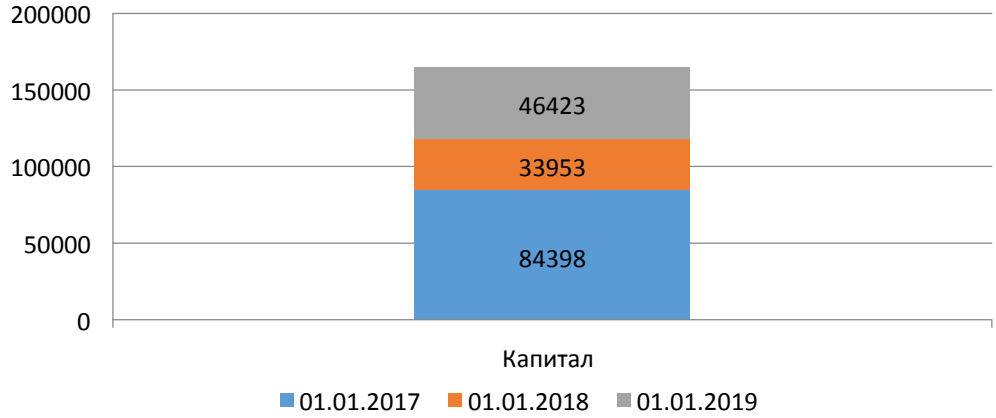

Рисунок 3 - Прирост капитала Банка за период с 2017-2019 г.г.

Источник: собственная разработка.

По состоянию на 01.01.2019 Банком заработана чистая прибыль в размере 71036 тыс. бел. рублей. Это 5 позиция по размеру чистой прибыли за 2018 год среди банков системной значимости (за 2017 года – 7 позиция, за 2016 год – 6 позиция) и 1 позиция среди банков 2 группы системной значимости. За период с 01.01.2017 по 01.01.2019 отмечен общий прирост показателя ЧП на 89,1%. (на 01.01.2019 по сравнению с показателем на 01.01.2018 прирост составил 66,1%; на 01.01.2018 по сравнению с показателем на 01.01.2017 - 13,8%). Динамика роста показателя ЧП и капитала Банка за период с 01.01.2017 по 01.01.2019 приведен ниже.

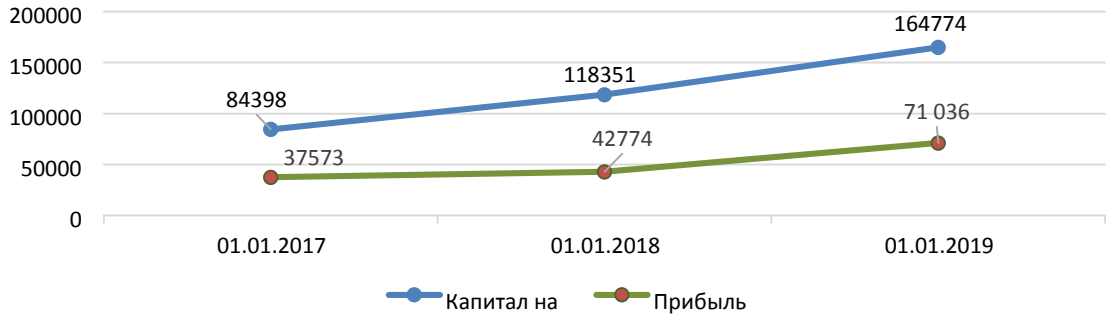

Рисунок 4 - Динамика роста капитала и прибыли Банка за 2017-2019 г.г.

Источник – собственная разработка

Следует отметить, что по рентабельности активов и рентабельности капитала МТБанк занимает лидирующую позицию в банковском секторе РБ. Кроме того, по результатам конкурса «Банк года-2017», прошедшем в апреле 2018 года, МТБанк стал самым награждаемым финансовым учреждением Беларуси, завоевав 9 наград, в том числе Гранпри премии «Банк года». В 2018 году на Конкурсе «Банк года» МТБанком завоеваны 5 наград. В категории «Карты рассрочки» Карта «Халва» награждена золотой медалью в Потребительской номинации профессионального конкурса «БРЕНД ГОДА-2018».

Рассмотрим возможность применения нечёткой продукционной модели, как категории мягких вычислений, на примере оценки риска информационной безопасности ЗАО «МТБанк».

В нечёткой продукционной модели для моделирования риска информационной безопасности организации (банка), нечёткие модели целесообразно представлять в виде нечётких сетей, составные части и совокупности элементов которых реализуют различные компоненты нечётких моделей и этапы нечеткого вывода. Этапы реализации нечёткой продукционной модели: определение входных переменных; формирование базы правил; фаззификация входных переменных; агрегирование подусловий; дефаззификация выходных переменных; управляющие (выходные) переменные. [5],[6],[7].

Взаимосвязь между факторами (антецедентом) и показателями риска (консеквентом) представляет собой бинарное нечеткое отношение соответствующих нечетких множеств. Нечеткое причинно-следственное отношение между антецедентом и консеквентом задается в виде нечёткой продукции.

Для реализации демонстрационного примера рассмотрим следующие входные переменные (факторы риска): обеспечение защиты от вредоносного программного обеспечения (1,4 – экспертная оценка), управление чувствительными документами и устройствами вывода (1,8 – экспертная оценка) и следующий показатель риска информационной безопасности банка: риск утечки конфиденциальной информации.

База правил системы нечеткого вывода, соответствующая знаниям эксперта о том, каким необходимо поддерживать уровень обеспечения защиты от вредоносного программного обеспечении, чтобы показатель риска утечки конфиденциальной информации оставался средним, будет выглядеть следующим образом:

ПРАВИЛО <1>: ЕСЛИ «обеспечение защиты от вредоносного программного обеспечения Н» И «управление чувствительными документами и устройствами вывода Н» ТО «риск утечки конфиденциальной информации высокий» и т.д. (фрагмент).

На этапе фаззификации происходит формализация описания уровня обеспечения защиты от вредоносного программного обеспечения и степени управления чувствительными документами и устройствами вывода при помощи лингвистических переменных, в кортеже которых содержится по три нечетких переменных, соответствующих понятиям низкого,

среднего и высокого значения соответствующих физических величин, соответственно строятся функции принадлежности.

Если (в соответствии с агрегированными экспертными оценками) текущие степень обеспечения защиты от вредоносного программного обеспечения банка и уровень управления чувствительными документами и устройствами вывода 1,4 и 1,8 соответственно, то при фаззификации получаем степени истинности элементарных нечетких высказываний:

- «обеспечение защиты от вредоносного программного обеспечения банка низкое» – 0.00;
- «обеспечение защиты от вредоносного программного обеспечения банка среднее» – 0.39;
- «обеспечение защиты от вредоносного программного обеспечения банка высокое» – 0.00;
- «уровень управления чувствительными документами и устройствами вывода низкий» – 0,00;
- «уровень управления чувствительными документами и устройствами вывода средний» – 0,80;
- «уровень управления чувствительными документами и устройствами вывода высокий» – 0,00.

Переходим к этапу «агрегирование». Агрегирование – это процедура определения степени истинности условий по каждому из правил системы нечеткого вывода (табл. 2).

Таблица 2 – Агрегирование

	Обеспечение защиты от вредоносного программного обеспечения			
Уровень управления чувствительными документами и устройствами		0,00	0,39	0,00
	0,00	0,00	0,00	0,00
	0,80	0,00	0,39	0,00
	0,00	0,00	0,00	0,00

Источник: собственная разработка.

Далее следует заключительный этап – дефаззификация. В системах нечеткого вывода дефаззификация – это процесс перехода от функции принадлежности выходной лингвистической переменной к её числовому значению. Для продукционных правил системы нечеткого вывода по управлению степенью риска утечки конфиденциальной информации под влиянем факторов уровня обеспечения защиты от вредоносного программного обеспечения банка и уровень управления чувствительными документами и устройствами вывода дефаззификация функции принадлежности лингвистической переменной «риск утечки конфиденциальной информаци» приводит к следующим результатам (расчеты проводились в MATLAB): метод центра тяжести y=0,64500; метод центра площади y=0,63500; метод левого модального значения y=0,63475; метод правого модального значения y=0,62987.

Интерпретируем этот результат как степень (степень риска - это вероятность наступления случая потерь, а также размер возможного ущерба от него) риска утечки конфиденциальной информации при экспертных оценках факторов риска обеспечение защиты от вредоносного программного обеспечения и управление чувствительными документами и устройствами вывода соответственно 1,4 и 1,8 равна 63% из 100%. Реализация

подобного алгоритма для всех возможных комбинаций факторов и показателей риска позволит получить высококачественную оценку риска ИБ, при этом такая оценка будет отражать степень влияния каждого фактора на каждый показатель риска и на итоговую оценку риска ИБ.

Такой способ оценки риска ИБ будет являться в значительно более эффективным для самой оценки и последующего управления риском ИБ особенно в сравнении с тем методом, основанным на построении моделей зрелости процессов, обеспечивающих информационную безопасность банка, который сейчас используется в банки и может активно реализовываться в том числе в белорусских банках.

Список использованных источников:

1. Булдакова Т.И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде MATLAB // Вопросы кибербезопасности. 2015. №4(12). С. 53-60. 2. ЗАО «МТБанк» [Электронный ресурс]. – Минск, 2020. – Режим доступа: https://www.mtbank.by. – Дата доступа: 01.03.2020.
2. Финансовая отчётность ЗАО «МТБанк» [Электронный ресурс]. – Минск, 2020. – Режим доступа: https://www.mtbank.by/about/reporting/finreports– Дата доступа: 01.03.2020.
3. Миков Д.А. Основные этапы оценки информационных рисков и способы их реализации // Теоретические и прикладные аспекты современной науки. 2014. №5-3. С. 103-106.
4. Аникин И.В. Метод оценки рисков для уязвимостей информационных систем, основанный на нечеткой логике // Информация и безопасность. 2014. Т.17. № 3. С. 468–471.
5. КовалевМ.М., Господарик Е.Г.Рейтинг белорусских банков по предварительным итогам 2016 г // Вестник Ассоциации белорусских банков. –2017. –No 4 (803).–С. 13-23.4.
6. Абакумова Ю. Г., Белый С. А. Применение эконометрических методов для оценки влияния экономических факторов на объемы долгосрочного кредитования // Журнал Белорусского государственного университета. Экономика.–2019. –No1. –С. 28-35.5.
7. Большакова И., Куприянова М. Оптимизация портфеля ценных бумаг // Вестник Ассоциации белорусских банков. –2012. –/No15(659).–С.10-14.