

3. Молодой ученый : научный журнал [Электронный ресурс]. – Режим доступа: <https://moluch.ru/archive/75/12830/>. – Дата доступа: 15.10.2023.
4. Компания StudyQA [Электронный ресурс]. – Режим доступа: <https://ru.studyqa.com/-for-universities/blog/6-tools-to-attract-students>. Дата доступа: 16.10.2023.

References

1. Institut ekonomiki i prava Ivana Kushnera [Elektronnyj resurs]. – Rezhim dostupa: <https://be5.biz/ekonomika1/r2014/3767.htm>. – Data dostupa: 14.10.2023.
2. Konzept : nauchno-metodicheskij elektronnyj zhurnal [Elektronnyj resurs]. – Rezhim dostupa: <https://e-koncept.ru/2017/970681.htm>. – Data dostupa: 14.10.2023.
3. Molodoj uchenyj : nauchnyj zhurnal [Elektronnyj resurs]. – Rezhim dostupa: <https://moluch.ru/archive/75/12830/>. – Data dostupa: 15.10.2023.
4. Kompaniya StudyQA [Elektronnyj resurs]. – Rezhim dostupa: <https://ru.studyqa.com/-for-universities/blog/6-tools-to-attract-students>. Data dostupa: 16.10.2023.

© Dzhigan M.S., Zhukova E.A., 2023

УДК 336.77

КРЕДИТНЫЙ МОНИТОРИНГ В БАНКЕ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

А. Л. Дроздовский

Научный руководитель: Н. А. Антипенко, к. э. н., доцент

Российский экономический университет им. Г. В. Плеханова (Минский филиал)
Республика Беларусь, 220070, г. Минск, ул. Радиальная, 40
a.drozdovskij@bk.ru

В данной статье рассматриваются современные состояния кредитного мониторинга в банках, применение различных методов и моделей для оценки кредитного риска и принятия решений о выдаче кредитов, а также обеспечение надежности и безопасности системы кредитного мониторинга.

Ключевые слова: мониторинг, методы, модели, надежность, автоматизация, технологии.

CREDIT MONITORING IN A BANK: CURRENT STATE AND DEVELOPMENT PROSPECTS

A. L. Drozdovsky

Scientific supervisor: N. A. Antipenko, Ph.D., Associate Professor

Russian Economic University named after. G.V. Plekhanov (Minsk branch)
Republic of Belarus, 220070, Minsk, st. Radialnaya, 40
a.drozdovskij@bk.ru

This article discusses the current state of credit monitoring in banks, the use of various methods and models for assessing credit risk and making decisions on issuing loans, as well as ensuring the reliability and security of the credit monitoring system.

Key words: Monitoring, methods, models, reliability, automation, technologies

Кредитный мониторинг в банке является важным инструментом для оценки кредитоспособности заемщиков и управления кредитным портфелем. В Республике Беларусь кредитный мониторинг также играет значительную роль в банковской системе.

Современные состояния кредитного мониторинга в банках Беларуси включают использование автоматизированных систем для сбора и анализа данных о заемщиках. Банки активно применяют различные методы и модели для оценки кредитного риска и принятия решений о выдаче кредитов. Это позволяет банкам более точно оценивать кредитоспособность клиентов и снижать риски неплатежей [1].

Перспективы развития кредитного мониторинга в банках Беларуси связаны с применением новых технологий и аналитических инструментов. Внедрение искусственного интеллекта, машинного обучения и больших данных позволяет банкам более эффективно анализировать информацию о заемщиках и прогнозировать их платежеспособность. Такие инновации помогают банкам принимать более обоснованные решения и снижать риски кредитного портфеля.

Однако следует отметить, что развитие кредитного мониторинга в банках Беларуси также может сталкиваться с некоторыми вызовами. Например, необходимость соблюдения законодательства о защите персональных данных может ограничивать доступ к определенным источникам информации о заемщиках. Важно также обеспечить надежность и безопасность системы кредитного мониторинга, чтобы предотвратить возможные случаи мошенничества или несанкционированного доступа к данным [3].

В целом, кредитный мониторинг в банках Беларуси продолжает развиваться и совершенствоваться, основываясь на современных технологиях и аналитических методах. Это позволяет банкам более эффективно управлять кредитным портфелем и минимизировать риски.

Банки в Беларуси обеспечивают безопасность и надежность системы кредитного мониторинга с помощью различных мер и технологий. Вот некоторые из них: [3]

1. Конфиденциальность данных. Банки строго соблюдают принцип конфиденциальности данных клиентов. Они применяют современные системы шифрования и защиты информации, чтобы предотвратить несанкционированный доступ к конфиденциальным данным.

2. Многоуровневая аутентификация. Банки используют многоуровневую аутентификацию для проверки подлинности пользователей. Это может включать использование паролей, пин-кодов, отпечатков пальцев или других биометрических данных.

3. Мониторинг транзакций. Банки активно мониторят транзакции, особенно те, которые могут быть связаны с мошенничеством или другими незаконными действиями. Они используют специализированные системы и алгоритмы для обнаружения подозрительных операций и предотвращения финансовых преступлений.

4. Антивирусная защита. Банки устанавливают и регулярно обновляют антивирусное программное обеспечение на своих компьютерах и серверах, чтобы предотвратить вредоносные программы и кибератаки.

5. Обучение персонала. Банки проводят обучение своего персонала по вопросам безопасности и надежности системы кредитного мониторинга. Это помогает сотрудникам банка быть в курсе последних угроз и уязвимостей, а также принимать соответствующие меры для защиты системы.

6. Резервное копирование данных. Банки регулярно создают резервные копии данных, чтобы в случае сбоя системы или потери информации можно было быстро восстановить работу и минимизировать потери.

При сбое системы кредитного мониторинга возможно возникновение различных последствий, которые могут негативно сказаться как на банке, так и на его клиентах. Вот некоторые из возможных последствий:

- Затруднения в выдаче и обработке кредитов. Система кредитного мониторинга играет важную роль в процессе выдачи и обработки кредитов. Сбой в системе может привести к задержкам и ошибкам в обработке заявок на кредит, что негативно скажется на клиентах, которым требуется финансирование.

- Нарушение контроля за кредитным риском. Система кредитного мониторинга помогает банкам контролировать и оценивать кредитный риск. Сбой в системе может привести

к недостаточной оценке риска и неправильному принятию решений о выдаче кредитов. Это приведет к увеличению неплатежей и потерь для банка.

- **Нарушение соответствия законодательству.** Система кредитного мониторинга также помогает банкам соблюдать требования законодательства, включая проверку клиентов на предмет соответствия антикоррупционным и противодействию отмыванию денег. Сбой в системе может привести к нарушению этих требований и повлечь за собой негативные юридические последствия для банка.

- **Потеря доверия клиентов.** Если система кредитного мониторинга не функционирует должным образом, это может вызвать недоверие у клиентов. Они могут сомневаться в надежности банка и его способности обеспечить безопасность и конфиденциальность их данных. Потеря доверия клиентов может привести к уходу клиентов и ухудшению репутации банка.

- **Финансовые потери.** Сбой в системе кредитного мониторинга может привести к финансовым потерям для банка. Неправильное выявление и оценка кредитного риска может привести к неплатежам и дефолтам по кредитам, что повлечет за собой финансовые потери для банка [4].

Для предотвращения сбоев в системе кредитного мониторинга можно принять следующие меры:

Резервное копирование данных. Регулярное создание резервных копий данных является важным шагом для предотвращения потери информации в случае сбоев. Резервные копии должны быть сохранены на отдельных устройствах или в облачном хранилище, чтобы обеспечить их доступность и сохранность.

Мониторинг и анализ системы. Регулярный мониторинг и анализ системы кредитного мониторинга позволяют выявлять потенциальные проблемы и сбои. Использование инструментов мониторинга и аналитики позволяет оперативно реагировать на возникающие проблемы и принимать меры по их устранению.

Обновление программного обеспечения. Регулярное обновление программного обеспечения системы кредитного мониторинга позволяет исправлять уязвимости и ошибки, которые могут привести к сбоям. Обновления должны быть установлены сразу после их выпуска, чтобы обеспечить безопасность и стабильность системы.

Установка защитных мер. Для предотвращения несанкционированного доступа и вредоносных атак необходимо установить защитные меры, такие как межсетевые экраны, антивирусное программное обеспечение, системы обнаружения вторжений и шифрование данных. Эти меры помогут защитить систему от угроз и сбоев.

Обучение персонала. Обучение персонала, работающего с системой кредитного мониторинга по вопросам безопасности и правильному использованию системы, является важным шагом для предотвращения сбоев. Персонал должен быть осведомлен о возможных угрозах и знать, как правильно реагировать на них [5].

Список использованных источников

1. Антипенко, Н. А. Экономика устойчивого развития: коллективная монография / Н. А. Антипенко [и др.] // Институт бизнеса Бел. гос. университета. – Минск : ИВЦ Минфина, 2022. – 460 с.

2. Антипенко, Н. А. Системный подход к финансовому анализу в рамках концепции управления ценностью / Н. А. Антипенко, Л. И. Тищенко // Бухгалтерский учет и анализ. – 2022. – № 7. – С. 50–54.

3. Антипенко, Н. А. О методике оценки эффективности инвестиционных проектов / Н. А. Антипенко // материалы X научной сессии преподавателей и студентов, 19, 20 апр. 2007 г. ; редкол.: И. В. Мандрик [и др.]. – Витебск, УО ФПБ ВМ МИТСО, 2007. – С.25–26.

4. Бусыгин, Д. Ю. Аналитическая оценка ключевых методов анализа угрозы банкротства / Д.Ю. Бусыгин // Бухгалтерский учет и анализ. – 2023. – № 1. – С. 42–49.

5. Бусыгин, Ю. Н. Особенности и пути совершенствования действующей практики анализа кредитоспособности корпоративного клиента банком / Ю. Н. Бусыгин, В. Л. Савич // Фундаментальные проблемы экономики : сб. статей Междунар. науч.-практ. конф. 27, 28 сент. 2013 г.: в 2 ч. ; отв. ред. Р. Г. Юсупов. – УФА: РИЦ БашГУ, Ч. 1 – 2013. – С. 21–23.

References

1. Antipenko, N. A. *Ekonomika ustojchivogo razvitiya: kollektivnaya monografiya* / N. A. Antipenko [i dr.] // Institut biznesa Bel. gos. universiteta. – Minsk : IVC Minfina, 2022. – 460 s.
2. Antipenko, N. A. *Sistemnyj podhod k finansovomu analizu v ramkah koncepcii upravleniya cennost'yu* / N. A. Antipenko, L. I. Tishchenko // *Buhgalterskij uchet i analiz.* – 2022. – № 7. – S. 50–54.
3. Antipenko, N. A. *O metodike ocenki effektivnosti investicionnyh proektov* / N. A. Antipenko // *materialy H nauchnoj sessii prepodavatelej i studentov*, 19, 20 apr. 2007 g. ; redkol.: I. V. Mandrik [i dr.]. – Vitebsk, UO FPB VM MITSO, 2007. – S.25–26.
4. Busygin, D. Yu. *Analiticheskaya ocenka klyuchevykh metodov analiza ugrozy bankrotstva* / D.Yu. Busygin // *Buhgalterskij uchet i analiz.* – 2023. – № 1. – S. 42–49.
5. Busygin, Yu. N. *Osobennosti i puti sovershenstvovaniya dejstvuyushchej praktiki analiza kreditosposobnosti korporativnogo klienta bankom* / Yu. N. Busygin, V. L. Savich // *Fundamental'nye problemy ekonomiki : sb. statej Mezhdunar. nauch.-prakt. konf.* 27, 28 sent. 2013 g.: v 2 ch. ; otv. red. R. G. YUusopov. – UFA: RIC BashGU, CH. 1 – 2013. – S. 21–23.

© Drozdovsky A.L., Antipenko N.A., 2023

УДК 004

СОВЕРШЕНСТВОВАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

А. А. Евдокимова

Научный руководитель: Е. В. Зеленцова, к. т. н., доцент

Московский государственный технический университет имени Н. Э. Баумана
(национальный исследовательский университет)

Российская Федерация, г. Москва, ул 2-я Бауманская, д. 5, стр. 1
uaevdokimova@yandex.ru

В статье рассматриваются вопросы обеспечения информационной безопасности в Российской Федерации, сделан анализ существующих изменений в законодательном регулировании вопросов обеспечения информационной безопасности на национальном уровне, изучены технологические аспекты, выявлены основные тенденции изменений, подведены общие итоги.

Ключевые слова: информационная безопасность, законодательство, персональные данные, кибератаки, программное обеспечение.

IMPROVING INFORMATION SECURITY IN THE RUSSIAN FEDERATION

A. A. Evdokimova

Scientific supervisor: E. V. Zelentsova

Bauman Moscow State Technical University
(National Research University)

Russian Federation, Moscow, 2nd Baumanskaya str., 5, p. 1
uaevdokimova@yandex.ru

The article examines the issues of information security in the Russian Federation, analyzes the existing changes in the legislative regulation of information security issues at the national level,