Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 5, May, 2026
Website: usajournals.org

CYBER RISKS IN THE BANKING SECTOR OF UZBEKISTAN: SOURCES, CONSEQUENCES, AND MITIGATION METHODS

Bardigina Anastasiya
Student, Tashkent State University of Economics,
Uzbekistan, Tashkent

Boburjon Baxriddinovich Izbosarov,
Scientific Supervisor, Doctor of Economics, Professor
Tashkent State University of Economics,
Uzbekistan, Tashkent

Abstract
The article examines cyber risks in the banking sector of Uzbekistan, as well as their main sources, consequences, and mitigation methods. Through an analysis of the legislative framework, statistical data, and reviews, key threats have been identified, including phishing, attacks on payment infrastructure, and internal incidents. The Central Bank has tightened requirements for commercial banks and has also introduced a development perspective for artificial intelligence in banking.

Keywords: Cyber risks, banking sector, cybersecurity, digital threats, commercial banks, anti-fraud.

КИБЕРРИСКИ В БАНКОВСКОМ СЕКТЕРЕ УЗБЕКИСТАНА: ИСТОЧНИКИ, ПОСЛЕДСТВИЯ И МЕТОДЫ МИНИМИЗАЦИИ

Бардыгина Анастасия Алексеевна студент,
Научный руководитель: Избосаров Бобуржон Бахриддинович,
доктор экономических наук, профессор
Ташкентский государственный экономический университет,
Республика Узбекистан, г. Ташкент

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 5, May, 2026
Website: usajournals.org

АННОТАЦИЯ

В статье рассматривается киберриски в банковской сфере Узбекистана, а также их основные источники, последствия и методы минимизации. С помощью анализа законодательной базы, статистических данных и обзоров были выявлены ключевые угрозы, к которым относятся фишинг, атаки на платежную инфраструктуру, внутренние инциденты. ЦБ ужесточил требования к коммерческим банкам, а также внедрил перспективу развития искусственного интеллекта в банковском деле.

Ключевые слова: киберриски, банковская сфера, кибербезопасность, цифровые угрозы, коммерческие банки, анти-фрод,

В современном мире невозможно представить ни одну сферу без учета кибербезопасности, в том числе и банковский сектор. 19 июня 2025 года в интернете появилась информация о том, что 16 миллиардов логинов и паролей от аккаунтов Apple, Google, Facebook, GitHub, Telegram, VPN-сервисы, банки и даже госуслуги утекли в открытый доступ в интернет. С начала 2025 года было обнаружено 30 крупных открытых наборов данных, которые содержат более чем 3,5 млрд записей. В списках находятся учетные записи пользователей социальных сетей, корпоративных платформ и порталов разработчиков [5]. Кроме того, 3 февраля 2026 года в Узбекистане появилась информация об утечке 15 млн. данных узбекистанцев, которые коснулись некоторых государственных учреждений. Примером подобного сайта является E-Gov, который использовался в качестве доверенного центра аутентификации для множества клиентов, включая сайты университетов, банков, госорганов, коммерческих организаций и системы Министерства внутренних дел [4].
Как отмечает И. Н. Рабыко, киберриски - очень серьезная угроза в наши дни ежегодно миллионы долларов вымогаются у организаций, таких как школы и больницы. С апреля 2018 НБ РБ дал четкое определение что является киберриском и обязал банки распознавать данный вид риска в системе, как отдельный вид риска. До этого момента киберриск оценивался как операционный риск тем самым методы его решения были не верны. В

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 5, May, 2026
Website: usajournals.org

2019 году НБ РБ принял решение о создании конвенции по мониторингу и решению киберугроз в банковской сфере, который способствует быстрому и точечному реагированию на киберриски в сторону как клиентов, так и банковской системы (в Беларуси) [6].

20 ноября 2025 года в силу вступает постановление об утверждении положения о минимальных требованиях к информационной безопасности и кибербезопасности коммерческих банков Республики Узбекистан. К данным требованиям относится внедрение антивирусной программы, аутентификации, автоматизированной банковской системы, электронный архив, DLP (от англ. Data Loss Prevention или Data Leak Prevention). Кроме того, сервис несет ответственность за обеспечение информационной безопасности банка, а также за устранение ситуаций временного простоя системы и несанкционированного изменения данных [1]. В дополнение к выше сказанному от 30-го апреля 2025 года был введен Указ Президента по борьбе с киберпреступностью. Приоритетными задачами в этом указе являются внедрение единой рабочей практики в сфере борьбы с киберпреступлениями на территории Республики Узбекистан. Президент обязал государственные органы, организации, банки, операторы платежных систем и платежные организации строго контролировать и уведомлять о киберпреступлениях и повышении киберкультуры среди всего населения. Важно отметить, что ключевой задачей для банков, операторов платежных систем и платежных организаций является обеспечить финансовый безопасности клиентов [3]. Помимо этого, 15-го апреля 2022 года в силу вступил Закон “О кибербезопасности” целью данного закона регулирования отношений в сфере кибербезопасности [2].

Для минимизации выше сказанных рисков можно использовать организационные меры, технологические методы защиты и человеческие меры. К организационным мерам относятся все выше перечисленные Законы, указы и постановление президента Республики Узбекистан, где запрещает аутсорсинг, IT-инфраструктуры что запрещает банкам передавать управление своими системами безопасности сторонним компаниям. Кроме того, банки должны создать службу кибербезопасности, которая в свою очередь должна отвечать за сохранность данных и

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 5, May, 2026
Website: usajournals.org

реагировать на кибератаки. В дополнение к перечисленному банк обязан не медленно сообщать о серьезных киберинцидентах в центральный банк. Если говорить о технологических методах защиты, то от банков требуется введение многофакторной аутентификации для подтверждения личности пользователей. Также важно внедрить антифрод-системы, которая анализирует транзакции в реальном времени и блокирует подозрительные операции. Для контроля передачи данных сотрудниками, утечек, кражи или случайной потери данных должна использоваться ранее упомянутая система DLP она, в свою очередь, непрерывно работает со всей информацией, с которой, в частности, работают и сотрудники будь то на компьютере, в сети или в облаке, и закрывает возможность передачи секретных персональных сведений за пределы данной организации [1]. Также важно учитывать человеческий фактор, по вине людей происходит 70-80% успешных атак. В данной проблеме поможет обучение людей цифровой грамотности, в случае банков, данная процедура должна осуществляться с клиентами. Регулярные тренинги, как распознать фишинговое письмо, и отправка "фейковых" атак для проверки реакции. Кроме того, сотрудники и клиенты должны знать, что возможно подделать голос и лицо других людей, вследствии чего, получить кредит или другую банковскую услугу.

В заключении важно отметить, что киберриски существуют и их негативное влияние будет только возрастать, однако комплексными мерами можно предотвратить их влияние. Если регуляторные, технологические и человеческие меры соединить в одно целое и бороться за кибербезопасность в целом, то преодолеть кибермошенничество будет легче.

Список литературы:

1. Центральный банк Республики Узбекистан. Об утверждении Положения о минимальных требованиях к информационной безопасности и кибербезопасности коммерческих банков Республики Узбекистан. Источник: https://lex.uz/ru/docs/7692335

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 5, May, 2026
Website: usajournals.org

2. Закон Республики Узбекистан «О кибербезопасности» № ЗРУ-764 от 15.04.2022. — Источник: https://lex.uz/ru/docs/5946314
3. Указ Президента по борьбе с киберпреступностью (от 30.04.2025): https://lex.uz/ru/docs/5946314
4. Новостной канал Podrobno.uz. https://podrobno.uz/cat/obchestvo/dannye-ne-menee-15-millionov-uzbekistantsev-utekli-v-set-iz-za-krupnoy-utechki-v-gosuchrezhdeniyakh/
5. Российский новостной канал "Ведомости" https://www.vedomosti.ru/technology/news/2025/06/19/1118417-16-mlrd-parolei
6. Рабыко И.Н.: Оценка киберриска в банках и его место в модели оценки эффективности управления рисками. Научные труды Белорусского государственного экономического университета. — Выпуск 15. — Минск: БГЭУ, 2022. — С. 393-400.