

**Угрозы и риски финансовой безопасности в эпоху цифровизации
экономики**

Каракалпакский Государственный университет имени Бердаха

Доцент кафедры Финансы

Баймуратова Зина Акылбековна

В условиях перехода к цифровой экономике понятие «финансовая безопасность» существенно расширяется. В рамках цифровой экономики структура финансовой безопасности охватывает несколько типов безопасности, включая:

- 1) валютно-кредитную безопасность;
- 2) производственно-техническую безопасность;
- 3) сырьевую безопасность;
- 4) финансовую безопасность;
- 5) внешнеэкономическую безопасность.

Угрозы безопасности банковской системы

Современная банковская система сталкивается с различными угрозами, которые можно классифицировать следующим образом:

- Киберугрозы: атаки на информационные системы банков, включая фишинг, взломы, вирусы, DDoS-атаки и т.д. Эти угрозы могут привести к утечке конфиденциальной информации, потере данных и финансовым потерям.
- Мошенничество: финансовые преступления, такие как отмывание денег, мошенничество с кредитными картами, подделка документов и т.д.
- Операционные риски: ошибки или сбои в работе информационных систем, человеческий фактор, нарушение процедур и внутренних контролей.
- Рыночные риски: колебания валютных курсов, изменения процентных ставок, финансовые кризисы и другие факторы, влияющие на стабильность банков.

- Юридические и регуляторные риски: несоответствие требованиям законодательства и регуляторов, что может привести к штрафам, санкциям и репутационным потерям.

Внедрение цифровых технологий в экономику приносит не только новые возможности, но и создает новые угрозы для финансовой безопасности страны.

Финансовая безопасность в эпоху цифровизации становится одной из ключевых задач.

В качестве внешнеэкономических угроз можно привести следующее: существует вероятность зарубежного вмешательства в цифровую инфраструктуру страны, особенно в экономический сектор, что может привести к ряду проблем для стабильного функционирования экономической деятельности в условиях цифровизации.

Любые угрозы и вызовы со стороны внешнеэкономических стран представляют собой посягательство на суверенитет страны. Многие европейские страны стремятся использовать свои преимущества в развитии высоких технологий как инструмент глобальной конкуренции.

Сегодня структурный дисбаланс в мировой экономике усиливается, что угрожает внутренней финансово-экономической безопасности Узбекистана. Низкая защита финансово-экономической сферы от воздействия через Интернет может привести к блокировке работы финансово-экономических отраслей, что в свою очередь нарушит функционирование экономики.¹

В условиях цифровой экономики оценка результатов деятельности экономического сектора существенно отличается. Существующие методы оценки и статистического учета отстают от цифровой реальности, что приводит к дисбалансу в оценке реального состояния финансово-экономического сектора.

¹ Каранина Е.В. Финансовая безопасность (на уровне государства, региона, организации, личности) - Монография. - Киров: ФГБОУ ВО "ВятГУ" 2015 г, 239 стр.

Необходимо также учитывать проблему киберпреступности. Цифровизация финансово-экономического сектора позволяет осуществлять атаки дистанционно из любой точки мира. Масштабы киберпреступности в банковско-финансовом секторе расширяются, увеличивается количество скоординированных компьютерных атак на финансово-экономические и военно-стратегические объекты.

Как отмечает Дыхова А.Л., "из-за большого количества рисков и угроз, а также совершаемых киберпреступлений наблюдается снижение доверия граждан к надежности цифровых инструментов, защите персональных данных, института банковской тайны и операций, проводимых с использованием новейших цифровых технологий. Государственные органы и крупные компании используют многоуровневую систему безопасности, постоянно обновляя защиту и антивирусные программы. Это делается для предотвращения новых способов киберпреступлений, кражи данных или взлома в условиях цифровизации операций".²

Существует угроза потери и утечки персональных данных, а также различных "отслеживаний".

С увеличением объема данных в цифровом пространстве, многие люди не соблюдают приватность организаций, связанных с конфиденциальными персональными данными. Большинство граждан Узбекистана не имеют полного представления о том, что такое "цифровой портрет", и не могут полностью контролировать использование своих данных.

Таблица.1

"Классификация угроз и рисков финансовой безопасности в цифровую эпоху".

² Дыхова А.Л. Цифровая экономика и проблемы экономической безопасности / А.Л. Дыхова, К.И. Семина // Стратегии исследования в общественных и гуманитарных науках: сборник научных трудов по материалам Международной научно-практической конференции 31 января 2022 г. – Белгород: Агентство перспективных научных исследований (АПНИ), 2022. – С. 71–76.

Вид угрозы	Описание	Примеры
Киберпреступность	Преступления, совершаемые с использованием компьютерных и сетевых технологий.	Фишинг, взлом, распространение вредоносного ПО.
Технологические риски	Риски, связанные с отказом или неправильной работой технологий.	Сбои в программном обеспечении, отказы оборудования.
Операционные риски	Риски, возникающие из-за внутренних процессов, людей и систем.	Ошибки сотрудников, недостатки внутренних контролей.
Юридические риски	Риски, связанные с нарушением законов, контрактов, лицензий.	Нарушение авторских прав, несоблюдение нормативных требований.
Репутационные риски	Риски, влияющие на репутацию и доверие к организации.	Утечки данных, скандалы, связанные с конфиденциальностью.
Стратегические риски	Риски, связанные с управленческими решениями и бизнес-стратегией.	Неправильное позиционирование на рынке, неверные инвестиционные решения.

Рыночные риски	Риски, связанные с изменениями на финансовых рынках.	Колебания валютных курсов, изменение процентных ставок.
Кредитные риски	Риск невозврата долга контрагентом.	Дефолт заемщика, неплатежеспособность.

Таблица.1 представляет собой систематизированный обзор основных вызовов, с которыми сталкиваются организации и индивидуальные пользователи в условиях цифровизации.

Для обеспечения финансовой безопасности необходим комплексный подход, включающий технологические, управленческие и стратегические аспекты. Особое внимание следует уделить разработке и реализации эффективных стратегий управления рисками.

Таким образом, необходимо рассмотреть наиболее важные направления обеспечения финансово-экономической безопасности Узбекистана:

1. Расширение нормативно-правовой базы в применении цифровизации в финансово-экономическом секторе.
2. Равное использование электронных форм с другими видами информации.

Список использованной литературы

1. Каранина Е.В. Финансовая безопасность (на уровне государства, региона, организации, личности) - Монография.- Киров: ФГБОУ ВО "ВятГУ" 2015 г, 239 стр.
2. Дыхова А.Л. Цифровая экономика и проблемы экономической безопасности / А.Л. Дыхова, К.И. Семина // Стратегии исследования в общественных и гуманитарных науках: сборник научных трудов по материалам Международной научно-практической конференции 31 января

2022 г. – Белгород: Агентство перспективных научных исследований (АПНИ), 2022. – С. 71–76.

3. Kalimbetov, H. K., Baymuratova, Z. A., & Ospanova, F. B. (2022). Modern technologies that can be used in the smart farm. *Экономика и социум*, (10-1 (101)), 65-71.

4. Daniyarov, K., Baymuratova, Z., Aytmuratova, U., Dauletalieva, A., & Ospanova, F. (2023). Financial support for agricultural business subjects in the innovative development of the economy. In *E3S Web of Conferences* (Vol. 389, p. 09054). EDP Sciences.

5. Isakov J.Ya., Toymuxamedov L.R., Tojiev R.R., Baymuratova Z.A., Isakov I.J., “Pul hám bankler” ráni boyınsha oqıwlıq. –Nókis: 2022 jıl, 271 bet.

6. Садовникова, Н.А., Вахрамеева, М.В., Попова, Г.Л., & Баймуратова, З.А. (2024). *Финансовая сфера экономики методами статистики: тенденции, факторы и перспективы развития*. Ташкент: METHODIST NASHRIYOTI.