rivojlantirish uchun xalqaro tajribalarni joriy etish muhim ahamiyat kasb etadi.

Foydalanilgan adabiyotlar

1. O'zbekiston Respublikasining "Qimmatli qog'ozlar bozori to'g'risadi"gi Qonuni. (https://lex.uz/acts/-1374865)

2. O'zbekiston Respublikasi Prezidentining 2024-yil 19-apreldagi "Iqtisodiyotda davlat ishtirokini qisqartirishga doir qo'shimcha chora-tadbirlar to'g'risida"gi PQ-162-son Qarori. (https://lex.uz/docs/68987062.)

3. S.Elmirzayev – "Korporativ boshqaruv" darsligi (2021-yil).

4. https://xalqchilipo.uz/company/tovar_xomashyo_birjasi.html

5. https://davaktiv.uz/oz/news/halchil-ipo-dasturiga-start-berildi-roadshow-tadimoti-tafsilotlari.

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ПЛАТЕЖАХ ПО БАНКОВСКИМ КАРТАМ

Бабаева Г.Я.
доцент кафедры
«Банковского учета и аудита» ТГЭУ

Цифровые технологии, искусственный интеллект, криптоэкономика и другие стали основным катализатором глобализации. Однако, есть обратная сторона монеты данного развития. Современные технологии стали использоваться злоумышленниками ради достижения преступных целей. Возник феномен киберпреступности, который по своим масштабам и степени общественной опасности намного опережает традиционную преступность. предполагаемый ущерб к 2025 году составит 10,5 триллионов долларов США. Для сравнения, этот прогнозируемый показатель превышает ВВП всех стран мира, кроме Китая и США, равен 10 % мирового ВВП.[158]

За последние годы значительно увеличилось количество киберпреступлений, связанных с вредоносной сетевой деятельностью. Например, в 2024 году было зафиксировано более 12 млн попыток совершения кибератак, в то время как в 2023 году этот показатель составил 11 млн. по данным Центра кибербезопасности. В Узбекистане в 2024 году зафиксировано более 50 тысяч случаев хищения денежных средств с банковских карт граждан. Эта тревожная статистика была озвучена 27 февраля 2025 года на заседании Комитета Сената Олий Мажлиса по вопросам обороны и безопасности. Всего за прошедший год в республике зарегистрировано почти 59 тысяч киберпреступлений (58,8 тысячи), из которых подавляющее большинство, а именно 97,7%, связаны с

[158] Расулев А. К.. Перспективы правовой политики в области противодействия киберпреступности в Узбекистане/ Институт законодательства и правовой политики при Президенте Республики Узбекистан. /https://illp.uz/

несанкционированным снятием денег с банковских счетов.[159] Отметим, что одной из основных причин роста мошенничества является увеличение числа пользователей банковских карт. В начале года их количество составляло менее 40 млн, а к настоящему времени (на 01.01. 2025 г) [160]оно возросло более чем до 54 млн.

Мошенничество с использованием банковских карт включает, но не ограничивается:

- Несанкционированное использование карточных данных.
- Фальсификация и клонирование карт.
- Использование украденных или потерянных карт.
- Получение доступа к конфиденциальным данным пользователя карты (логин, пароль) посредством интернет-мошенничества (Фишинг).

В ЕОПЦ применяются следующие методы противодействия мошенничеству с банковскими картами:

- Технологии безопасности: Применение передовых технологий, включая EMV чипы, токенизацию данных и многофакторную аутентификацию, включая SMS информирование.
- Мониторинг транзакций: Использование системы мониторинга транзакций в реальном времени и пост-контрольные процедуры для выявления подозрительной активности.
- Обмен информацией: Сотрудничество с банками, другими платежными системами и правоохранительными органами для обмена информацией о мошеннических схемах.
- Повышение квалификации: Регулярное обучение сотрудников ЕОПЦ методам защиты и распознавания мошеннических действий. Сотрудники отдела администрирования системы фрод мониторинга операционного департамента и отдела по выявлению подозрительных операций службы внутреннего контроля, комплаенс и рисков минимум 1 раз в год проходят курсы по повышению квалификации. Служба внутреннего контроля, комплаенс и рисков на постоянной основе организует проведение брифингов, тренингов, а также готовит публикации на официальных страницах и каналах ЕОПЦ в социальных сетях о распространенных схемах мошенничества и средствах защиты от них, в целях повышения грамотности населения по предупреждению современных угроз, в части незаконных операций с банковскими картами. В случае соответствия транзакции критериям подозрительных мошеннических транзакций, ответственные сотрудники ЕОПЦ должны немедленно блокировать подозрительные карты и операции, вовлеченных в мошенничество.

Денежные средства, которые предположительно определены как объект мошенничества должны быть недоступны для вывода из карточного счета. Если будет выявлено, что средства были выведены на другие карты, необходимо выявить и блокировать средства на этих

[159] https://upl.uz/incidents/49355-news.html
[160] https://cbu.uz/upload/medialibrar

вовлеченных картах до выявления всех обстоятельств, но не более чем на 3 дня, если нет законного обоснования для более длительной блокировки. Если вовлечены карты других платежных систем, необходимо оперативно связаться с подразделением фрод мониторинга данной платежной системы и в рамках сотрудничества запросить блокирование средств на картах, подозреваемых в вовлеченности в мошенничество.

Необходимо письменно по установленным каналам связи сообщить участникам о выявленных мошеннических транзакциях, предпринятых действиях и далее передать им полномочия для решения вопроса. Кроме того, следует сообщить в правоохранительные органы, если есть обоснованное мнение о том, что совершено мошенничество.

Отдел администрирования системы фрод мониторинга операционного департамента и отдел по выявлению подозрительных операций службы внутреннего контроля, комплаенс и рисков должны совместно проанализировать каждый случай мошенничества и выявить коренные причины, которые предоставили возможность для совершения мошенничества. В системе фрод мониторинга ЕОПЦ должны оперативно вноситься все известные сценарии мошенничества для эффективного противодействия мошенничеству. Сценарии содержат в себе критерии, по которым та или иная транзакция должна считаться подозрительной и меры, которые необходимо предпринять при соответствии транзакции этим критериям. Внести сценарий в систему фрод мониторинга может только отдел администрирования фрод мониторинга операционного департамента в следующих случаях:

- Запрос участников платежной системы.
- Получение информации о новых схемах мошенничества от Центрального Банка Республики Узбекистан, правоохранительных органов, других платежных систем.
- По результатам изучения информации из открытых источников.
- Запрос отдела по выявлению подозрительных операций службы внутреннего контроля, комплаенс и рисков.

Борьба с мошенничеством может быть эффективной только при вовлеченности всех заинтересованных сторон. В связи с этим необходимо проводить обмен данными о мошеннических операциях с участниками платежной системы, другими платежными системами, платежными организациями с учетом требований Закона Республики Узбекистан «О персональных данных» и Закона Республики Узбекистан «О банковской тайне».

Список использованных источников:

1. Расулев А.К. Перспективы правовой политики в области противодействия киберпреступности в Узбекистане/ Институт законодательства и правовой политики при Президенте Республики Узбекистан. /https://illp.uz/

2. https://upl.uz/incidents/49355-news.html

3. https://cbu.uz/upload/medialibrar
4. Политика по борьбе с мошенничеством с использованием банковских карт в платежной системе «UZCARD» Акционерного общества «Единый общереспубликанский процессинговый центр»/ https://api.uzcard.uz/wp-content/uploads/2024/07/Politika-po-borbe-s-moshennechestvom-1.pdf

КОРХОНА МОЛИЯВИЙ СТРАТЕГИЯСИНИ ИШЛАБ ЧИҚИШ ПРИНЦИПЛАРИ

Расулов Мухаммад Бобур Фазлиддин ўғли
ТДИУ Мустақил изланувчиси

Аннотация. Ҳозирда жаҳонда корхоналар фаолиятини молиявий стратегиясини ишлаб чиқишга доир илмий тадқиқотлар олиб борилмоқда. Жаҳон бозори конъюктурасидаги ўзгаришлар, бугунги кундаги бизнес муҳити, рақобатнинг миллий доирадан жаҳон даражасига чиққанлиги асосида ўрта ва узоқ муддатли молиявий стратегияларга таъсир этувчи омилларни олдиндан баҳолаш кабиларга алоҳида эътибор қаратилмоқда. Корхоналар молиявий стратегияларини ишлаб чиқиш ва амалиётга жорий этиш самарадорлигини баҳолаш, корхоналарда молиявий кўрсаткичларни ўстириш имконини берувчи асосий омилларни аниқлаш орқали иқтисодий ўсишни таъминлаш, маҳсулотлар таннархини камайтириш, диверсификациялаш ҳамда рақобатбардошлигини ошириш бу борадаги устувор илмий тадқиқотлар вазифалари ҳисобланади.

Калит сўзлар: Молия сиёсати стратегияси, ЯИМ, солиқ қарзи, Солиқ тушуми, солиқларнинг эластиклик коэифисенти.

Стратегик бошқарувнинг ушбу тамойили шундан иборатки, молиявий стратегияни ишлаб чиқишда корхона ташқи ва ички омиллари билан фаол ўзаро таъсир қилиш учун мутлақо очиқ бўлган маълум бир тизим сифатида қаралади. Бундай ўзаро таъсир жараёнида корхона бозор типидаги иқтисодиёт шароитида ўзига хос бўлмаган ташқи таъсирнинг вақтинчалик ёки функционал тузилмасини олиш хусусиятига эга бўлиб, бу унинг ўзини ўзи ташкил этиш қобилияти деб ҳисобланади. Корхонанинг ижтимоий-иқтисодий тизим сифатида очиқлиги ва унинг ўзини ўзи ташкил этиш қобилияти унинг молиявий стратегиясини сифат жиҳатидан янги даражага кўтариш имконини беради.

Корхонанинг оператив фаолиятининг асосий стратегияларини ҳисобга олиш. Корхонанинг иқтисодий ривожланишининг умумий стратегиясининг бир қисми сифатида, биринчи навбатда, операцион фаолиятнинг ривожланишини таъминлаган ҳолда молиявий стратегия унга бўйсунади. Шунинг учун у корхонанинг операцион фаолиятининг стратегик мақсадлари ва йўналишларига мос келиши керак, молиявий стратегия эса у танлаган корпоратив стратегияга мувофиқ корхонанинг