- обеспечение стабильности банковской системы;
- совершенствование системы валютного регулирования и контроля;
- расширение форм и инструментов оказания финансовых услуг;
- повышение надежности, скорости и удобства расчетов.

Данные направления способствуют активизации сберегательного процесса, эффективной трансформации сбережений в инвестиции и рациональному распределению денежных ресурсов в экономике, сохранению покупательной способности доходов и сбережений граждан, формированию устойчивой и предсказуемой среды для работы организаций и долгосрочных инвестиций, что создает условия, необходимые для устойчивого экономического развития страны.

Заключение. Таким образом, в настоящее время проблема эффективности денежно-кредитной политики приобрела особую актуальность, поскольку становится все очевиднее, что от ее решения зависит будущее не только отдельных стран, но и мировой экономики. В своей основе данная проблема предполагает нахождения оптимального баланса рычагов внутренней и внешней экономической политики, которые обеспечивали бы для государства благоприятные условия с точки зрения достижения положительных параметров экономического роста при стабильности ценовой и финансовой среды.

Подводя итог, можно говорить о том, реализация обозначенных направлений денежно-кредитной политики с целью обеспечения макроэкономической стабильности, формирования прозрачной и комфортной бизнес-среды, повышения уровня защиты населения в финансовой сфере внесет значимый вклад в создание условий для устойчивого экономического развития Республики Беларусь, роста благосостояния и повышения качества жизни населения.

Список цитируемых источников

1. О целевых показателях денежно-кредитной политики Республики Беларусь на 2024 год [Электронный ресурс] : Указ Президента Республики Беларусь от 02.10.2023 г. № 307 // Национальный правовой Интернет-портал Республики Беларусь. — URL: https://pravo.by/document/?guid=12551&p0=P32300307 (дата обращения: 26.10.2024).
2. *Лученок А. И.* Макроэкономическое регулирование развития Республики Беларусь : монография / А. И. Лученок, О. Л. Шулейко, В. Г. Герасимова [и др.] ; под общ. ред. А. И. Лученка ; Национальная академия наук Беларуси, Институт экономики Национальной академии наук Беларуси. — Минск : Белорусская наука, 2023. — 227 с.
3. Об утверждении Основных направлений денежно-кредитной политики Республики Беларусь на 2024 год [Электронный ресурс] : постановление Правления Национального банка Республики Беларусь от 26.10.2024 г. № 363 // Национальный банк Республики Беларусь. — URL: https://www.nbrb.by/Legislation/Documents/ondkp2024.pdf. (дата обращения: 26.10.2024).
4. О важнейших параметрах прогноза социально-экономического развития Республики Беларусь на 2024 год [Электронный ресурс] : Указ Президента Республики Беларусь от 02.10.2023 г. № 308 // Национальный правовой Интернет-портал Республики Беларусь. — URL: https://pravo.by/document/?guid=12551&p0=P32300308 (дата обращения: 26.10.2024).

УДК 339

В. В. Чудук

Учреждение образования «Барановичский государственный университет», Барановичи, Республика Беларусь

Научный руководитель
М. М. Хованская

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ КОММЕРЦИИ: ЗАЩИТА ДАННЫХ И ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ

Введение. Электронная коммерция стала неотъемлемой частью современной экономики, предоставляя потребителям удобный доступ к товарам и услугам через интернет. Однако с ростом популярности онлайн-покупок увеличивается и количество угроз, связанных с безопасностью данных и мошенничеством. Безопасности электронной коммерции требует рассмотрения ключевых аспектов, таких как защита данных пользователей, предотвращение мошенничества и обеспечение надежности транзакций.

Основная часть. Электронная коммерция — это процесс покупки и продажи товаров и услуг через интернет. Она включает в себя различные виды онлайн-транзакций, такие как интернет-магазины, онлайн-аукционы, электронные платежи и мобильные приложения для покупок. Электронная коммерция позволяет потребителям и бизнесменам взаимодействовать без необходимости физического присутствия, что делает покупки более удобными и доступными.

Однако электронная коммерция сталкивается с различными угрозами, такими как мошенничество, незаконный обмен данными, вредоносное программное обеспечение, нарушения безопасности и проблемы с обслуживанием клиентов. Безопасность в электронной коммерции играет ключевую роль в защите данных клиентов и поддержании доверия к онлайн-бизнесу. В условиях, когда кибератаки становятся все более изощ-

ренными, защита личной информации, такой как данные кредитных карт и адреса, становится приоритетом. Компании, которые инвестируют в современные системы безопасности, не только защищают своих клиентов, но и укрепляют свою репутацию на рынке.

Одними из самых крупных взломов в истории электронной коммерции являются:

− eBay, 2014 г. — хакеры получили доступ к данным 145 млн пользователей, включая имена, адреса и зашифрованные пароли;

− **Alibaba, 2019 г.** — взлом, в результате которого были скомпрометированы данные 1,1 млн пользователей;

− **Adobe, 2013 г. —** хакеры украли почти 3 млн зашифрованных записей кредитных карт клиентов и данные для входа в систему для неопределенного количества учетных записей пользователей;

− Facebook, **2019 г. —** два набора данных из приложения были раскрыты в открытом доступе в Интернете. Информация касалась более 530 млн пользователей и включала номера телефонов, имена учетных записей и идентификаторы [1].

На рисунке 1 отражена статистика киберпреступности по странам мира по состоянию на начало 2024 г.

Rank	Country	I	P	TS	WCI Score	Tech	Attacks	Data	Scams	Cash
1	Russia	8.96	8.81	8.73	58.39	82.17	81.34	65.18	21.70	41.56
2	Ukraine	8.37	8.29	8.24	36.44	52.97	50.76	36.01	11.20	31.27
3	China	8.22	7.70	7.81	27.86	40.22	24.24	34.89	15.83	24.13
4	United States	7.99	7.21	7.21	25.01	27.64	17.68	30.36	22.72	26.63
5	Nigeria	8.25	6.49	5.80	21.28	7.93	8.41	23.04	52.17	14.86
6	Romania	7.12	7.04	7.15	14.83	17.83	9.17	22.50	13.15	11.49
7	North Korea	7.91	7.23	7.38	10.61	8.66	25.33	13.01	2.17	3.88
8	United Kingdom	7.86	7.21	6.75	9.01	5.04	4.75	5.80	7.86	21.63
9	Brazil	6.90	6.35	6.32	8.93	13.70	8.77	10.29	7.28	4.64
10	India	7.90	6.60	6.65	6.13	4.46	3.62	6.81	12.75	3.01
11	Iran	6.88	6.45	6.64	4.78	8.62	10.00	3.59	0.94	0.72
12	Belarus	6.84	7.20	7.32	3.87	11.92	5.58	1.85	--	--
13	Ghana	8.57	6.83	6.09	3.58	1.23	0.76	2.97	10.36	2.57
14	South Africa	6.95	5.35	5.50	2.58	1.20	0.65	0.58	7.17	3.30
15	Moldova	7.38	7.19	7.56	2.57	6.70	0.98	2.43	0.83	1.88

I = Impact; P = Professionalism; TS = Technical skill, Technical = *Technical products/services*, Attacks = *Attacks and extortion*, Data = *Data/identity theft*, Cash = *Cashing out and money laundering*. I, P, and TS are scored out of 10. 'WCI Score', and all columns following, are scored out of 100. Each country's top score across all cybercrime types is shaded in grey.

Рисунок 1 — Мировой индекс киберпреступности

Примечание — Источник: [2].

Таким образом, киберпреступность наиболее распространена в таких странах, как Россия, Украина, Китай, США. Возможными причинами данного явления являются мировое положение, законодательная база в области цифровых преступлений, уровень проникновения Интернета среди населения, а также технологическая инфраструктура страны. В Республике Беларусь также преобладает киберпреступность, но не в таком масштабе, как в вышеперечисленных странах.

Существуют способы защиты:

1. Симметричное шифрование использует один и тот же ключ для шифрования и расшифровки данных. Это быстрый и эффективный метод для защиты больших объёмов данных, такой как AES. Асимметричное шифрование использует пару ключей: публичный и приватный. Публичный ключ можно сравнить с замком, а приватный — с ключом к этому замку. Таким образом, можно раздать публичные ключи всем желающим отправить вам зашифрованное сообщение, но только у вас есть приватный ключ для его расшифровки. Примером асимметричного шифрования является RSA, который обеспечивает безопасный обмен данными в интернете.

2. Применение протоколов TLS/SSL для обеспечения безопасного соединения. Они обеспечивают безопасное соединение, аутентификацию и защиту от несанкционированного доступа и нарушения целостности передаваемых данных. Они используют надёжные методы аутентификации, шифрование канала связи и коды целостности сообщений. Протокол SSL был разработан компанией Netscape и широко используется для VoIP-приложений и сервисов обмена мгновенными сообщениями. Он обеспечивает частный и аутентифицированный канал связи с проверкой целостности сообщений. Протокол TLS является криптографическим протоколом, который пришёл на смену SSL. Он применяется для защищённой передачи данных между различными узлами в Интернете, например, в VoIP-приложениях, веб-браузерах и приложениях для мгновенного обмена сообщениями.

3. Регулярное обновление программного обеспечения и операционных систем. Регулярное обновление программного обеспечения и операционных систем — это процесс установки новых версий программ

и системных файлов, выпущенных разработчиками для исправления ошибок, улучшения производительности и добавления новых функций.

4. Использование многофакторной аутентификации (MFA) для усиления безопасности. Этот метод усиления безопасности использует несколько независимых способов проверки подлинности пользователя для подтверждения его личности, что помогает предотвратить несанкционированный доступ к учётным записям и защищает конфиденциальные данные от кражи. При использовании MFA пользователь должен предоставить несколько доказательств своей идентичности, таких как пароль, биометрические данные, одноразовые коды или токены. Это делает взлом учётной записи гораздо сложнее, так как злоумышленнику необходимо получить доступ к нескольким каналам аутентификации одновременно.

Интернет стал настолько привычной частью нашей жизни, что иногда мы забываем, что не все, с кем мы пересекаемся онлайн, заботятся о наших интересах. Киберпреступники делают все возможное, чтобы извлечь выгоду, используя для этого обычных пользователей интернета, поэтому об угрозе онлайн-мошенничества нужно помнить всегда. Лучший способ защиты от онлайн-мошенников — знать о рисках и уметь их избегать.

Одним из самых популярных способов мошенничества является фишинг — вид мошенничества, при котором злоумышленники пытаются обмануть людей, выдавая себя за доверенные организации или лица, чтобы получить конфиденциальную информацию, такую как логины, пароли, данные кредитных карт и другие чувствительные данные [3].

Часто киберпреступники прибегают к «социальной инженерии» (social engineering) или «атаке на человека» — это совокупность психологических и социологических приёмов, методов и технологий, которые позволяют получить конфиденциальную информацию [4]. Самый простой пример — телефонный звонок, где злоумышленник выдаёт себя за кого-то другого, пытаясь узнать у абонента конфиденциальную информацию, играя на чувствах человека, обманывая или шантажируя его. Чтобы не попасться на «удочку» мошенникам, нужно соблюдать «цифровую гигиену»:

5. Не переходить по ссылкам из электронных писем, сообщений в социальных сетях, чатах и баннерной рекламы.
6. Проверять URL-адрес перед вводом конфиденциальных данных.
7. Использовать шифрование для передачи данных.
8. Пользоваться своим компьютером и подключением к интернету.
9. Не использовать основную кредитную или дебетовую карту для онлайн-покупок.
10. Изучить отзывы о магазинах перед совершением покупок.
11. Избегать покупок на потенциально ненадёжных сайтах [5].

Заключение. В эпоху цифровой трансформации электронная коммерция стала неотъемлемой частью нашей повседневной жизни. С каждым годом всё больше людей предпочитают совершать покупки онлайн, что приводит к росту объёмов данных и увеличению числа транзакций. Однако вместе с этим растут и угрозы безопасности, связанные с защитой данных и предотвращением мошенничества. Поэтому организации, которые осуществляют свою деятельность в просторах Интернета, должны позаботиться о своей безопасности и безопасности своих клиентов.

Список цитируемых источников

1. Leyden J., Swinhoe D., Hill M. The 18 biggest data breaches of the 21st century [Электронный ресурс]. — URL: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html. (дата обращения: 18.09.2024).
2. Miranda B., Jonathan L., Ridhi K., Nigel P., Federico V. Mapping the global geography of cybercrime with the World Cybercrime Index [Электронный ресурс]. — URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312. — (дата обращения: 19.09.2024).
3. *Боженко, Я.* Что такое фишинг и как не стать жертвой хакеров [Электронный ресурс]. — URL: https://www.nur.kz/technologies/internet/2046135-chto-takoe-fishing-i-kak-ne-stat-zhertvoy-hakerov/ (дата обращения: 19.09.2024)
4. Что такое социальная инженерия: история, методы, примеры [Электронный ресурс]. — URL: https://www.reg.ru/blog/chto-takoe-sotsialnaya-inzheneriya/ (дата обращения: 20.09.2024).
5. Как защитить свои деньги и электронные кошельки от мошенников в Интернете хакеров [Электронный ресурс]. — URL: https://www.kaspersky.ru/resource-center/preemptive-safety/money-online (дата обращения: 20.09.2024).