УДК 343.3.7

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ МЕР ОТВЕТСТВЕННОСТИ ЗА ЭКОНОМИЧЕСКИЕ ПРЕСТУПЛЕНИЯ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

М. А. Царёва

студентка, Белорусский государственный университет, г. Минск, Беларусь, tsaryova.maria121206@gmail.com

Научный руководитель **Н. И. Шандора**

старший преподаватель, Белорусский государственный университет, г. Минск, Беларусь, shandor@bsu.by

На современном этапе информационные технологии оказывают всё большее влияние на каждую из сфер жизни человечества. Одной из таковых можно считать экономическую безопасность: в связи с расширением возможностей применения цифровой среды, данная сфера сталкивается с новыми задачами. В статье рассматривается динамика основных показателей в сфере экономических преступлений, а также проведён анализ влияния цифровых технологий на реализацию отдельных элементов экономической безопасности в Республике Беларусь.

Ключевые слова: экономическая безопасность; экономические преступления; цифровая безопасность; информационные технологии; законодательство Республики Беларусь.

PROBLEMS AND PROSPECTS OF APPLYING MEASURES OF RESPONSIBILITY FOR ECONOMIC CRIMES IN THE DIGITAL ECONOMY

M. A. Tsaryova

student, Belarusian State University, Minsk, Belarus, tsaryova.maria121206@gmail.com

Supervisor **N. I. Shandora**

senior lecturer, Belarusian State University, Belarus, shandor@bsu.by

At the present stage, information technologies are having an increasingly significant impact on every aspect of human life. One such aspect is economic security, which faces new challenges as the digital environment expands its capabilities. This article examines the dynamics of key indicators in the field of economic crimes and analyzes the impact of digital technologies on the implementation of certain elements of economic security in the Belarus.

Keywords: economic security; economic crimes; digital security; information technologies.

Вследствие активного развития цифровых технологий появляется всё большее количество мошеннических схем с применением компьютерных технологий. На данный момент преступники активно задействуют искусственный интеллект, фейковые аккаунты в социальных сетях и мессенджерах и многие другие средства. Для защиты населения от подобных правонарушений правительством регулярно вводятся нововведения, способствующие предупреждению и пресечению подобных действий. Анализируя статистику преступлений в Республике Беларусь, можно сделать вывод о ежегодном росте количества правонарушений, которые связаны с использованием различных цифровых технологий (таблица) [1].

Динамика количества правонарушений, квалифицируемых как Хищение имущества путём модификации компьютерной информации и преступлений против компьютерной безопасности, в % к общему количеству зарегистрированных преступлений

Показатель	2020	2021	2022	2023
Всего зарегистрированных преступлений	95 478	87 696	88 555	85 374
Из них хищение имущества путём модификации компьютерной информации и преступлений против компьютерной безопасности, %	3,73	5,67	6,54	6,5

Наиболее распространенными видами информационно-экономических преступлений являются: фишинг, вредоносное ПО (включая шифровальщики), компрометация бизнес-почты, социальная инженерия, подделка и фальсификация документов (фейковые счета), sim-swap и атаки на мобильную связь.

Фишингом признаётся вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователя: логинам и паролям. Мошенники под видом популярных брендов, банков или же мобильных операторов делают массовую рассылку писем, содержащие ссылки. Переходя по ним, пользователь, сам того не осознавая, открывает мошенникам доступ к своим персональным данным, в том числе, номера и пароли банковских карт.

Вредоносное ПО – это программа, либо же программный код, созданный в целях похитить данные пользователя, либо же нанести ущерб устройству. Мошенники часто используют подобное, маскируя это под видом обновленного приложения банка, скачивая которое, жертва предоставляет всю информацию, необходимую для хищения средств.

Компрометация бизнес почты – ещё один распространённый вид мошенничества, который предполагает, что мошенник представляется доверенным лицом компании либо же руководителем и требует под видом рабочей необходимости предоставить конфиденциальные данные, либо же совершить платёж, который на самом деле является мошенническим.

Sim-swap – это вид кибератаки, в следствие которой мошенник получает у мобильного оператора копию SIM-карты телефона жертвы, тем самым, получая доступ к её номеру телефона. Это позволяет преступнику читать сообщения и получать звонки, приходящие на данный номер с целью входа в приложение банка, так как очень часто именно телефон помогает пройти аутентификацию.

В свою очередь, Уголовным Кодексом Республики Беларусь, хищением имущества путем модификации компьютерной информации (ст. 212 УК) признается умышленное противоправное безвозмездное завладение чужим имуществом с корыстной целью посредством противоправного изменения компьютерной информации либо внесения в компьютерную систему заведомо ложной компьютерной информации [2].

Следует также отметить, что для более точной классификации подобных преступлений правительство регулярно обновляет и уточняет законодательство. Для примера можно привести факт, что на данный момент Законом Республики Беларусь от 17 февраля 2025 года № 61-З, пунктом 56 предусматривается редакция статьи 222 УК Республики Беларусь, которая подразумевает вынесение «распространения из корыстных побуждений находящихся в незаконном владении лица реквизитов банковских платёжных карточек либо аутентификационных данных…» отдельным пунктом статьи [3].

Говоря о цифровизации экономической безопасности, следует также проанализировать применение компьютерных технологий правоохранительными органами. В качестве примера можно привести ЕГБДП – единый государственный банк данных о правонарушениях (официально – Единая государственная система регистрации и учёта правонарушений). Данная информационная система содержит информацию о правонарушениях, совершённых физиче-

скими лицами ранее, что позволяет сотрудникам уполномоченных ведомств определить, совершено ли данное деяние повторно или же впервые, не было ли оно совершено в совокупности с другими правонарушениями, и, на основе данных фактов, более корректно квалифицировать тяжесть такового. Разумеется, большинство информационных технологий, применяемых правоохранительными органами, на данный момент находится в закрытом доступе. Однако, согласно данным официальных правовых порталов, только с 2005 по 2019 год число ресурсов и информационных систем, используемых милицией Республики Беларусь, выросло с 11 до более чем 50.

Таким образом можно сделать следующий вывод: одной из основных проблем применения мер ответственности за экономические преступления в условиях цифровой среды является изобретение всё более модернизированных схем мошенничества путём модификации компьютерных данных. В перспективе ожидается дальнейшее обновление законодательства с целью более точной квалификации подобных деяний. Для достижения сокращения процента правонарушений подобного характера, в дальнейшем будет рассматриваться возможность ужесточения мер ответственности за данные правонарушения, а также более частое проведение профилактических мероприятий и бесед с целью повышения осведомленности населения, в особенности групп, наиболее подверженных влиянию, а также предупреждения совершения преступлений подобного характера.

Библиографические ссылки

1. Статистика правосудия и правонарушений // Национальный статистический комитет Республики Беларусь : сайт. URL: https://dataportal.belstat.gov.by/osids/rubric-info/10620 (дата обращения: 13.09.2025).

2. Уголовный Кодекс Республики Беларусь : 09 июл. 1999 г. №275-З : принят Палатой представителей 2 июня 1999 г. : одобрен Советом Респ. 24 июня 1999 г. : в Кодекс с 17 фев. 2025 г. изм. и доп. не вносились // Национальный правовой Интернет-портал Республики Беларусь: сайт. URL: https://pravo.by/document/?guid=3871&p0=hk9900275 (дата обращения: 13.09.2025).

3. Об изменении кодексов по вопросам уголовной ответственности : Закон Респ. Беларусь от 17 февраля 2025 года №61-З : принят Палатой представителей 10 янв. 2025 г. : одобрен Советом Респ. 30 янв. 2025 г. // Национальный правовой Интернет-портал Республики Беларусь: сайт. URL: https://pravo.by/document/?guid=12551&p0=H12500061 (дата обращения: 13.09.2025).