DOI: https://doi.org/10.53486/sstc2024.v2.11
CZU: 004:343.37

CYBERCRIME IN THE MODERN ECONOMY

КИБЕРПРЕСТУПЛЕНИЯ В СОВРЕМЕННОЙ ЭКОНОМИКЕ

PECHCOVSKAIA Olga, studentă, *specialitatea:* TI
Academia de Studii Economice din Moldova, Republica Moldova,
Chișinău, str. Bănulescu-Bodoni 61, www.ase.md

Abstract: *The article explores key trends related to the evolution of cybercrime as a form of economic criminal activity. The characteristics of the modern cybercriminal and the influence of globalization processes in the field of information and communication technologies on their actions are analyzed. The main categories of cybercrimes and their impact on business activities are examined. Key approaches to combating cybercrime are identified, and suggestions for improving legislation are proposed.*
Keywords: *cybercrime, hacker, cyberattack, globalization, internet, information and communication technologies, economic crime*

Среди современных тенденций в мировой экономике отмечается увеличение активности экономической преступной деятельности. Глобализация процессов способствует расширению и усложнению этой проблемы, делая её одной из ключевых для человечества. Экономическая преступность наносит ущерб как экономикам отдельных страх, так и стабильному развитию мировой экономики в целом. Киберпреступность стала ключевым аспектом информационной эры, в которой компьютеры, телекоммуникационные системы и Интернет занимают центральное место, создавая новые риски для экономической безопасности. Преступные группы теперь используют Интернет не только как вспомогательный инструмент, но и как основную платформу для совершения таких преступлений, как мошенничество, кражи и вымогательство [1].

Киберпреступность трудно описать одним определением: ей можно понимать как набор действий или поведения, которые нацелены на компьютерные данные или системы. Термин «киберпреступление» охватывает противоправные действия, в которых цифровые устройства или информационные системы выступают как инструменты, цели или их комбинация.

Киберпреступность сегодня выделяется среди других экономических преступлений из-за своего быстрого роста. Этот рост связан с увеличением числа интернет-пользователей, постоянным повышением уровня мастерства киберпреступников и развитием информационных технологий.

Любые достижения в сфере информаций и технологий значительно увеличивают возможности для киберпреступности, создавая условия для более эффективных хакерских атак. В итоге киберпреступность прогрессирует быстрее, чем другие виды преступлений [2].

По данным Всемирного обзора экономических преступлений, проведённого PricewaterhouseCoopers (PWC) в 2022 году, несмотря на небольшое снижение общего уровня экономической преступности, киберпреступления продемонстрировали наибольший рост за всё время наблюдений.

Более половины организаций сообщили, что мошенничество привело к финансовым убыткам, и свыше четверти из них потеряли около 1 миллиона долларов. На (рис. 1) приведена статистика внутренний воздействий, полученная в результате мошенничества [3].

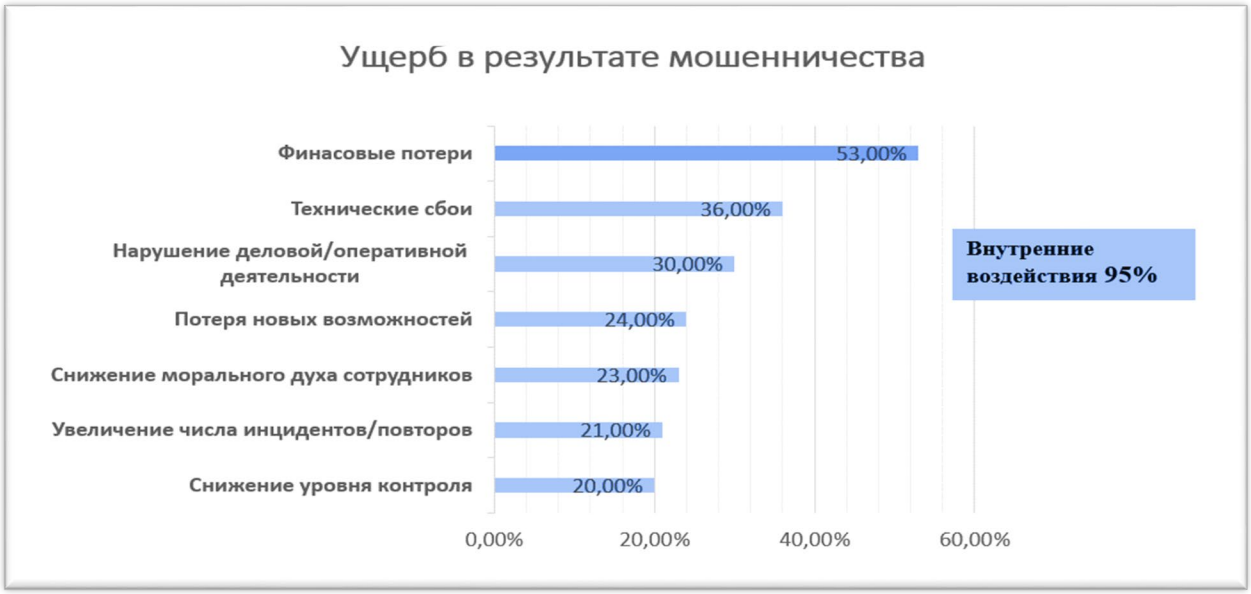

Рисунок 1 Статистика внутренних воздействий

На рис. 2 приведена статистика внешних воздействий, полученная в результате мошенничества.

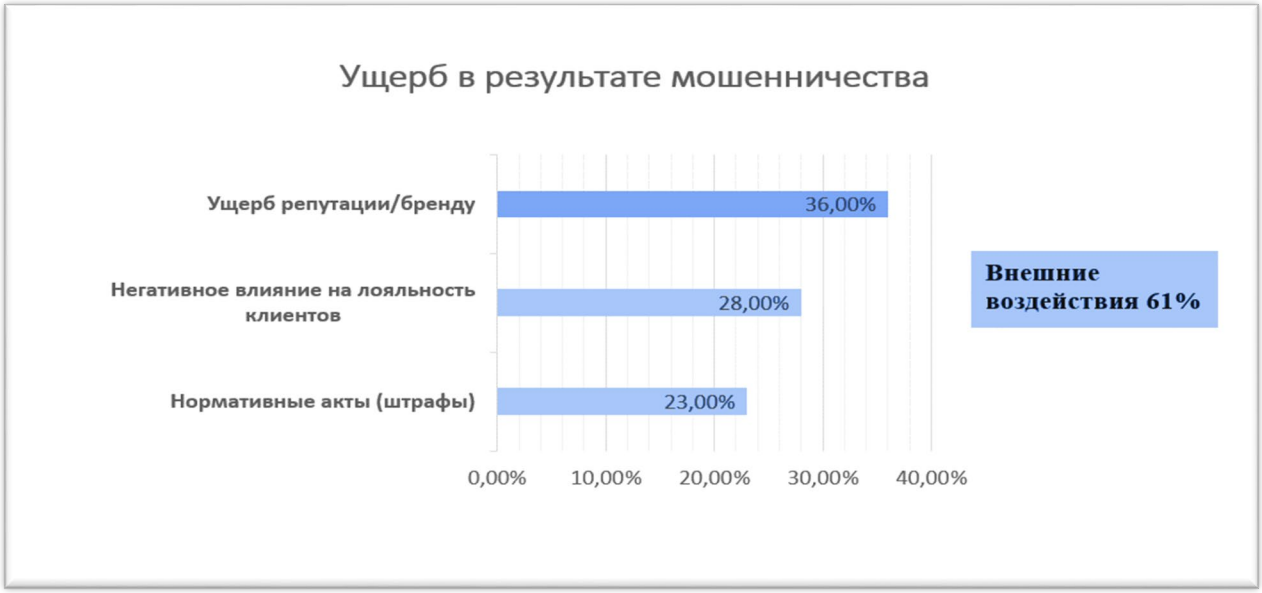

Рисунок 2 Статистика внешних воздействий

Тем не менее, представленные данные не полностью отражают действительное положение дел с киберпреступностью, поскольку отсутствуют чёткие и общепринятые методы для систематического сбора подобной информации.

Киберпреступления можно классифицировать на четыре основные группы:

- преступления, направленные против конфиденциальности, целостности и доступности компьютерных данных и систем;
- преступления, непосредственно связанные с использованием компьютеров;
- преступления, связанные с содержанием и распространением контента;
- преступления, касающиеся нарушений авторских прав и смежных прав.

С развитием киберпреступности трансформировался и образ хакера: если раньше это были энтузиасты с техническими навыками, стремящиеся к исследованию нового, то сегодня их деятельность часто движима интересами криминального бизнеса.

Расширение интернета привело к утрате национальных границ в киберпреступности, превратив её в по-настоящему интернациональное явление. Хакер может быть гражданином одной страны, находиться в другой, а его действия могут осуществляться через сервер в третьей стране. Трансграничность киберпреступности позволяет совершать кражи и вывод средств в странах, значительно удалённых друг от друга. Преступные действия не всегда очевидны и могут быть скрытыми, что приводит к тому, что пострадавшая сторона узнаёт о них только спустя значительное время. Локация преступника, факты совершения преступления и сбор доказательств часто представляют собой значительные трудности для правоохранительных органов.

Средства и методы защиты от киберпреступности обычно подразделяются на две основные категории: организационные и технические. К организационным относятся законодательные, административные и физические меры, тогда как к техническим — аппаратные, программные и криптографические методы, направленные на защиту объектов, людей и информации [4].

На государственном уровне и в частных компаниях требуется активно развивать профилактическую и образовательную деятельность. Повышение уровня компетентности пользователей и сотрудников в области компьютерных технологий поможет снизить вероятность того, что они станут жертвами киберпреступлений, а также уменьшит распространение угроз в информационных сетях.

Киберпреступность достигла нового уровня, охватывающего вымогательство, промышленный шпионаж и целевые атаки. Хакеры из любителей превратились в профессионалов, став частью организованного криминального бизнеса. Эти преступники наносят значительный ущерб как отдельным гражданам, организациям и предприятиям, так и национальной экономике в целом, при этом сводя собственные риски к минимуму. Они опережают существующие системы безопасности компаний, увеличивая своё преимущество. Для решения проблемы киберпреступности важно не просто адаптировать компании к современным угрозам, а активно разрабатывать стратегии информационной безопасности, которые будут опережать эти угрозы.

БИБЛИОГРАФИЯ

1. Номоконов В. А. «Киберпреступность как новая криминальная угроза». Криминология: вчера, сегодня, завтра – 2012 - стр. 53.
2. Морозов Н.А. «Борьба с компьютерной преступностью в Японии». Общество и право. – 2014 - стр. 141
3. PricewaterhouseCoopers. «Всемирный обзор экономических преступлений за 2022 год»
4. «Методы и приемы обеспечения информационной безопасности». - стр. 15

Coordonator ştiinţific: OHRIMENCO Serghei A.,dr.hab., prof.univ.
Academia de Studii Economice din Moldova
Republica Moldova, mun.Chișinău
str. Bănulescu Bodoni 61,
Telephone: + 373 79359405
E-mail: osa@ase.md