КИБЕРПРЕСТУПНОСТЬ КАК НОВЕЙШАЯ РАЗНОВИДНОСТЬ ТЕНЕВОЙ ЭКОНОМИКИ РФ

С.Е. Козырева, *студент*
Н.В. Яковлева, *канд. экон. наук, доцент*
Иркутский государственный университет путей сообщения
(Россия, г. Иркутск)

DOI:10.24412/2500-1000-2023-6-1-70-73

Аннотация. *Статья посвящена киберпреступности как части современной экономики страны. Рассмотрен теоретический аспект теневой цифровой экономики, влияние киберугроз на объекты социальной инфраструктуры и факторы роста киберпреступности. Также, описано современное состояние киберпреступности в Российской Федерации, количество кибепреступлений и ущерб от них.*

Ключевые слова: *киберпреступность, цифровая теневая экономика, цифровизация.*

Развитие информационных технологий все больше актуализирует угрозы киберпреступлений, разрабатываются новые и более сложные методы атак. В связи с чем государство, организации и граждане несут ощутимые потери. Создаются угрозы общественной безопасности и тормозится развитие цифровизации, из-за снижения доверия к онлайн-сервисам.

Исследуя сущность киберпреступности, нужно отметить, что она относится к новейшей разновидности теневой цифровой экономики, которая в свою очередь представляет собой все незаконные и скрываемые продукты и услуги, использующиеся и основывающиеся на информационных технологиях [5].

Исключительные особенности цифровой теневой экономики, такие как электронное общение между участниками цифрового рынка, транзакции, цифровые денежные потоки и т.д., определяют трудности в корректировке принципов налогообложения, применяемых для традиционной экономической деятельности. Фактически, онлайн–торговля может включать в себя продажу любых видов товаров и услуг, т.е. материальные и нематериальные [2].

Далее в таблице 1 рассмотрим то, каким именно образом киберугрозы влияют различные объекты социальной инфраструктуры.

Таблица 1 Объекты и виды киберугроз [1]

Объект угроз	Виды угроз
Граждане	– Воздействие на личность (сбор персональных данных и атаки на персональные компьютеры и мобильные устройства) – Утечка и обнародование частной информации – Мошенничество – Распространение опасного контента
Бизнес	– Воздействие на системы интернет-банкинга – Воздействие на информационную инфраструктуру – Блокирование систем онлайн-торговли, геоинформационных систем – Хакерские атаки на сайты компаний
Государство	– Атаки на ключевые государственные системы управления (электронное правительство, сайты государственных структур) – Экономическая блокада (масштабное отключение платежных систем, систем бронирования) – Аппаратные атаки на персональные компьютеры и критически важную инфраструктуру государственных предприятий

Одним из наиболее популярных методов атак по-прежнему является социальная инженерия: количество атак на организации в 2023г. составило 50%, на частных лиц 91%. Электронная почта в 86%, остается основным каналом атак на организации. На частных лиц в 59% – это веб-ресурсы и сервисы. Хакерские атаки становятся более сложными и профессиональными, направленными не только на отдельных пользователей, но и на крупные промышленные системы.

Если сравнивать киберпреступность с другими видами преступной деятельности, то киберпреступность растет гораздо большими темпами. Это связано со следующими факторами: постоянное увеличение числа пользователей компьютеров и сети Интернет; постоянное повышение уровня профессионализма преступников в киберпространстве; совершенствование, развитие IT-технологий [3]. Киберпреступность уже прошла стадию становления, перешла на новый уровень и развивается с каждым днем. Например, в конце января 2023 года МВД РФ обнародовало статистику по преступности в стране. Показатели киберпреступности в целом остались стабильными. Четверть преступлений совершается с использованием IT. В 2022 году зарегистрировано на 27,6% меньше краж, на 29% – фактов мошенничества с использованием электронных средств платежа, на 22,5% – криминальных деяний в сфере компьютерной информации.

Рассмотрим на рисунке 1 динамику по количеству киберпреступлений в России за 2020-2022 гг.

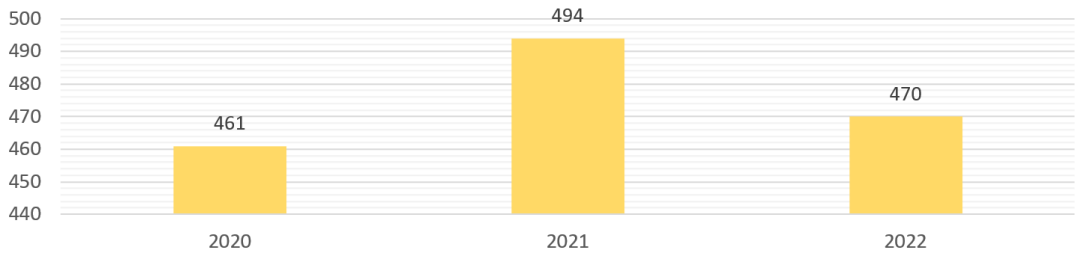

Рис. 1. Динамика количества киберпреступлений в России за 2020-2022 гг., тыс.

В целом количество преступлений к 2022 году, снизилось на 24 тыс. За этот период сотрудниками правоохранительных органов было раскрыто более 1 млн преступлений. Здесь повлияло повышение осведомленности граждан [4].

И тем не менее, с начала 2022 года сумма ущерба от IT-преступлений в России составила 65 млрд рублей. Подробнее динамику ущерба от кибепреступлений в России рассмотрим на рисунке 2.

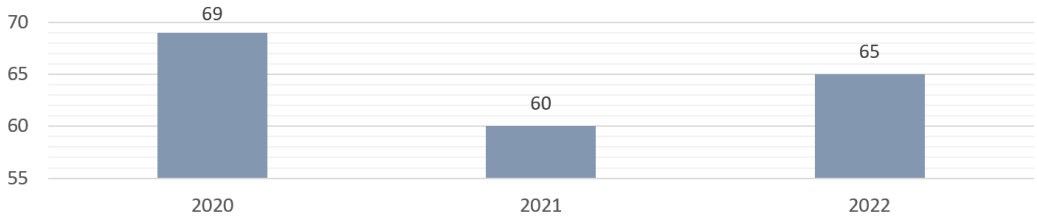

Рис. 2. Динамика ущерба от киберпреступлений в России, 2020-2022 гг., млрд. руб.

По словам эксперта, в основном кибер-хищения совершаются из зарубежных колцентров, преимущественно на территории Украины. Глава МВД отметил, что мошенники всё чаще пользуются тем, что заключение кредитных договоров можно производить удалённо. По его словам, это и явилось одной из основных причин усугубления ситуации. Нужно отметить, что 68% всех атак – это целевые атаки, т.е. направленные на конкретные данные. На рисунке 3 представлены категории потерпевших от кибератак.

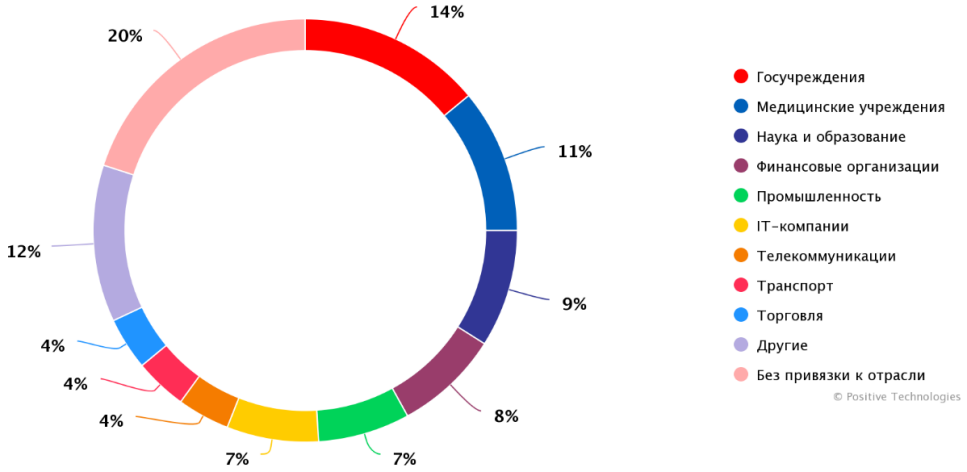

Рис. 3. Структура потерпевших от кибератак в 2023 г.

Главным выводом данной статьи является то, что киберпреступность стала значительной и динамично развивающейся как часть теневой экономики России. Киберпреступники все более активно развивают и внедряют новые методы и технологии, например, криптовалютное мошенничество, или использование облачных сервисов как базу для фишинга.

Статья также подчеркивает, что киберпреступность имеет негативное влияние на российскую экономику. Наносит вред бизнесу и инвестициям в России, а также подрывает репутацию страны в глазах международного сообщества.

В целом, киберпреступность является серьезной проблемой для России, требующей немедленных мер по улучшению кибербезопасности и пресечению различных форм киберпреступности. Это также подчеркивает необходимость государственной поддержки и разработки соответствующих стратегий и политик для противодействия киберпреступности и защиты экономики страны.

Библиографический список

1. Глотина И.М. Киберпреступность: Основные проявления и экономические последствия // Вопросы экономики и права. – 2014. – № 8. – 12 с. – [Электронный ресурс]. – Режим доступа: https://law-journal.ru/files/pdf/201408/201408_11.pdf (дата обращения: 04.03.2023).

2. Морозов Н.А. Борьба с компьютерной преступностью в Японии // Общество и право. – 2014. – №2 (48). – 141 с.

3. Нами Ф. Цифровая теневая экономика // Онлайн-журнал ИдаТен, 2020 г. – [Электронный ресурс]. – Режим доступа: https://idaten.ru/economic/cifrovaya-tenevaya-ekonomika (дата обращения: 11.03.2023).

4. Суслов С. Ущерб от киберпреступлений исчисляется миллиардами //Онлайн-ресурс iCHIP.ru. – 2020. – [Электронный ресурс]. – Режим доступа: https://ichip.ru/novosti/ushherb-ot-kiberprestuplenijj-ischislyaetsya-milliardami-61533 (дата обращения: 04.03.2023).

5. Шарыпова Т.Н., Сидоренко А.А. Киберпреступность в XXI веке // Аллея науки. – 2019. – Т. 2, № 1 (28). – С. 978-981.

CYBERCRIME AS THE NEWEST TYPE OF SHADOW ECONOMY

S.E. Kozyreva, *Student*
N.V. Yakovleva, *Candidate of Economic Sciences, Associate Professor*
Irkutsk State Transport University
(Russia, Irkutsk)

Abstract. *The article is devoted to cybercrime as part of the modern economy of the country. The theoretical aspect of the shadow digital economy, the impact of cyber threats on social infrastructure facilities and the growth factors of cybercrime are considered. Also, the current state of cybercrime in the Russian Federation, the number of cybercrime and the damage from them are described.*

Keywords: *cybercrime, digital shadow economy, digitalization.*