

## **МИНИМИЗАЦИЯ УГРОЗ НЕГАТИВНОГО ВЛИЯНИЯ КИБЕРПРЕСТУПНОСТИ В ЭПОХУ ЦИФРОВИЗАЦИИ**

**А. А. Васенина**

*студентка экономического факультета, Пермский государственный национальный  
исследовательский университет, г. Пермь, Россия, e-mail: a.a.vasenina@mail.ru*

**Научный руководитель: А. В. Бобков**

*кандидат экономических наук, доцент, доцент кафедры предпринимательства  
и экономической безопасности, Пермский государственный национальный  
исследовательский университет, г. Пермь, Россия, e-mail: Bobkovav@yandex.ru*

В настоящее время киберпреступность стала одной из глобальных проблем человечества, что подтверждает статистика за 2015–2022 гг. Тотальный рост произошел в 2020 году с 180 тыс. до 510,4 тыс., в связи с появлением пандемии COVID-19 и наступлением периода дистанционного взаимодействия граждан. На начало 2023 г. было выявлено 261 тыс. кибератак, что превышает на 27,5% равный период прошлого года. Подобный темп роста говорит о недейственности методов по борьбе с проблемой и заставляет искать новые пути решения. В настоящей статье проводится анализ и рассматриваются причины совершения преступлений в сфере информационно-коммуникационных технологий, предложены авторские мероприятия по противодействию киберпреступности цифровыми и правовыми инструментами.

**Ключевые слова:** киберпреступность; цифровая экономика; нефинансовый фишинг; хакерство.

## **MINIMIZING THE THREATS OF THE NEGATIVE IMPACT OF CYBERCRIME IN THE ERA OF DIGITALIZATION**

**A. A. Vasenina**

*Student of the Faculty of Economics, Perm State National Research University, Perm,  
Russia, e-mail: a.a.vasenina@mail.ru*

**Scientific supervisor: A. V. Bobkov**

*PhD in Economics, Associate Professor, Associate Professor of the Department  
of Entrepreneurship and Economic Security, Perm State National Research University,  
Perm, Russia, e-mail: Bobkovav@yandex.ru*

Currently, cybercrime has become one of the global problems of mankind, which is confirmed by statistics for 2015–2022. Total growth occurred in 2020 from 180 thousand to 510.4 thousand, due to the emergence of the COVID-19 pandemic and the onset of the

period of remote interaction of citizens. At the beginning of 2023, 261 thousand cyberattacks were detected, which exceeds by 27.5% the same period last year. Such a growth rate indicates the ineffectiveness of methods to combat the problem and forces us to look for new solutions. This article analyzes and examines the reasons for committing crimes in the field of information and communication technologies, suggests author's measures to counter cybercrime with digital and legal tools.

**Keywords:** cybercrime; digital economy; non-financial phishing; hacking.

Появление информационного сектора в жизни человечества безусловно позитивный показатель, который свидетельствует о развитии общества. Настоящая экспансия прямо отражается на экономической составляющей. Благодаря информационной сети люди могут совершать действия мгновенно, что безусловно экономит их бесценный ресурс-время. Вместе с этим увеличивается рост количества киберпреступлений, что является негативным фактором, влияющим на экономику страны. (рис. 1).

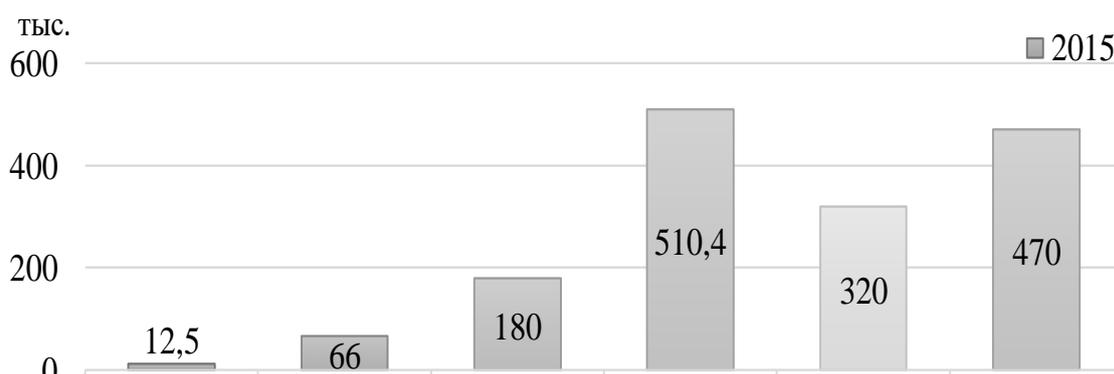


Рис. 1. Количество киберпреступлений в Российской Федерации за 2015–2016 гг. / 2019–2022 гг.

Число киберпреступлений за последние пять лет выросло почти в 5 раз. Самого пика показатель достиг в 2020 г. Существенные изменения произошли в связи с пандемией коронавируса, когда возникла потребность в дистанционном взаимодействии. На данном этапе проблему преступности, переросшую в онлайн-среду можно назвать не только государственной, но и глобальной. Развитие многоаспектных интернет инстанций приводит к утечке информации на просторах сети, это и есть начальный этап возникновения опасности. Киберпреступность проявляется в любом месте информационно-коммуникационных структур. К группе экономических преступлений в интернет пространстве причислены: хакерство, к специальным программам по защите пользователей от хакерства можно отнести: Snort, DEFT, Kali Linux [4]; шпионаж; мошен-

ничество/обман пользователей в сети; взлом социальных сетей и личных кабинетов пользователей, фишинг. На долю нефинансового фишинга приходится 80 % всех кибератак. Он заключается в отправке поддельного уведомления от маркетплейсов и банков, с просьбой перейти в приложение для ознакомления товара или подтвердить оплату, которую человек не совершал, введя персональные данные мошенники получают информацию и списывают деньги с карты.

Киберпреступления наносят огромный ущерб национальной экономике страны (рис. 2).

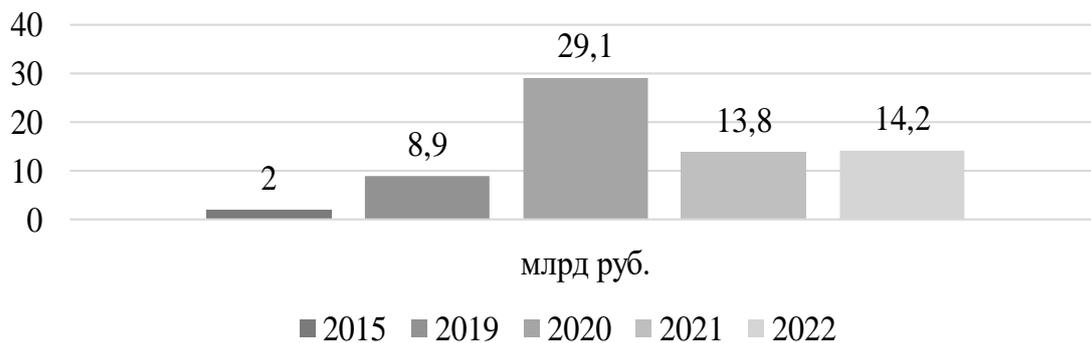


Рис. 2. Ущерб кибератак национальной экономики Российской Федерации за 2015–2019 гг. / 2020–2022 гг.

«Из масштабного количества преступлений раскрывается только 1/4 часть от общего числа»-Генпрокуратура РФ. Это связано с использованием злоумышленниками различных серверов, скрывающих свою реальную личность, таких как VPN. Причина такой раскрываемости в том, что агрегаторы информации собирают данные, которые связаны с уникальными идентификаторами пользовательских персональных данных, а не с конкретными устройствами.

Базовые методы защиты от киберпреступности:

1. Использование двухуровневой защиты пароля.
2. Не переходить по непроверенным ссылкам и сайтам.
3. Не игнорировать систему обновлений браузера и сетей. В них обычно исправляются обнаруженные проблемы кибербезопасности.
4. Подключение резервное копирование данных, для восстановления в случае утечки.

Исходя из методов защиты от киберпреступности, можно заметить, что большую роль играет человеческая ошибка, а именно собственноручный ввод данных. Разработка закона о проведении комплекса мероприятий по повышению информационной грамотности у населения, как один из главных методов борьбы. Специальные уроки в школах для под-

ростков, введения специальности в вузах, в качестве дополнительного факультатива, инструктажи на работе. Для усиления эффекта данного рода мероприятий можно разработать специальную программу, обязательной установки на любой смартфон. Программа будет действовать как антивирус, в случае ложного уведомления на телефон давать определенный сигнал. Такая программа будет очень актуальна для пожилых людей, которые несильны в современных интернет-инфраструктурах. Мероприятия подобного законного характера приведут к снижению количества преступлений и уровню ущерба.