Научная статья
УДК 343.98
DOI: 10.47475/2311-696X-2024-41-2-130-133

С. 130–133

КИБЕРПРЕСТУПНОСТЬ: СОВРЕМЕННОЕ СОСТОЯНИЕ И МЕРЫ ПРОТИВОДЕЙСТВИЯ

Наиля Рашидовна Шевко[1], **Марина Алексеевна Лукина**[2]
[1,2] *Российский государственный университет правосудия, Казанский филиал, Казань, Россия*
[1] *mos_shev@mail.ru*
https://orcid.org/0000-0003-1092-3389
[2] *lukina_ma@mail.ru*

Аннотация. Современный этап развития общества характеризуется повсеместным внедрением современных телекоммуникационных технологий во все сферы жизнедеятельности людей. К сожалению, информационные технологии все чаще используются злоумышленниками в преступных целях. Причиной этому служат отличительные особенности виртуального пространства и технологий, применяемых для передачи и использования информации. В статье дается краткая характеристика состояния киберпреступности на современном этапе развития, а также выделены специфические особенности преступлений, совершаемых с использованием информационных технологий, обеспечивающих рост общего числа, а также высокого уровня латентности. Авторы уделяют особое внимание таким характеристикам киберпреступности, как трансграничность, анонимность преступника и высокая скорость распространения информации среди большого числа пользователей интернет-аудитории, способствующих использованию высоких технологий злоумышленниками, надеющимися скрыть следы преступлений и остаться незамеченными. Кроме того, дана краткая характеристика жертв киберпреступлений. Авторами выделены основные тенденции развития новых способов и методов их совершения, предложены меры по предупреждению роста числа преступлений в киберпространстве посредством информирования граждан, повышения уровня информационной и финансовой грамотности, международного сотрудничества по эффективному взаимодействию в целях обеспечения кибербезопасности.

Ключевые слова: киберпреступность, виртуальное пространство, киберпреступник, информационная безопасность, защита данных, трансграничность, интернет-пространство

Для цитирования: Шевко Н. Р., Лукина М. А. Киберпреступность: современное состояние и меры противодействия // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 130–133. DOI: 10.47475/2311-696X-2024-41-2-130-133

Research article

CYBERCRIME: CURRENT STATUS AND COUNTERMEASURES

Nailya R. Shevko[1], **Marina A. Lukina**[2]
[1,2] *Kazan branch of the Russian State University of Justice, Kazan, Russia*
[1] *mos_shev@mail.ru*
http://orcid.org/0000-0003-1092-3389
[2] *lukina_ma@mail.ru*

Abstract. The current stage of development of society is characterized by the widespread introduction of modern telecommunication technologies into all spheres of people's lives. Unfortunately, information technologies are increasingly being used by attackers for criminal purposes. The reason for this is the distinctive features of virtual space and technologies used to transmit and use information. The article provides a brief description of the state of cybercrime at the current stage of development, and also highlights the specific features of crimes committed using information technology, which ensure an increase in the total number, as well as a high level of latency. The authors pay special attention to such characteristics of cybercrime as transborder nature, the anonymity of the criminal and the high speed of dissemination of information among a large number of Internet users, facilitating the use of high technologies by attackers hoping to hide traces of crimes and remain undetected. In addition, a brief description of victims of cybercrime is given. The authors have identified the main trends in the development of new ways and methods of committing them, and proposed measures to prevent the increase in the number of crimes in cyberspace by informing citizens, increasing the level of information and financial literacy, and international cooperation for effective interaction in order to ensure cybersecurity.

Keywords: cybercrime, virtual space, cybercriminal, information security, data protection, cross-border, Internet space

For citation: Shevko NR, Lukina MA. Cybercrime: current status and countermeasures. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2024;(2):130-133. DOI: 10.47475/2311-696X-2024-41-2-130-133 (In Russ.)

Введение

Развитие современных технологий привнесло в нашу жизнь и такие негативные явления, как киберпреступления. Киберпреступность — это преступность в виртуальном пространстве [1, с. 144]. Для совершения преступного деяния в киберпространстве современному преступнику в большинстве случаев не нужны специальные знания и навыки. Достаточно быть просто грамотным пользователем компьютерной техники, при необходимости уметь найти нужные инструкции в сети Интернет. Современные программные средства максимально удобны для пользователей. Даже дети, которые хоть раз пользовались каким-нибудь гаджетом, с легкостью осваивают новые приложения.

Материал и методы

В статье использованы нормативные правовые акты, регламентирующие вопросы уголовно-правового регулирования ответственности за преступления, совершенные с использованием информационных технологий, специальная литература по предмету исследования. Основу исследования составили общенаучные и частнонаучные методы научного познания, анализ теоретических источников, статистический метод.

Описание исследования

Киберпреступления, в отличие от традиционных преступлений, обладают рядом отличительных особенностей [2, с. 84]. К таковым можно отнести такие особенности, как трансграничность, анонимность, охват большого числа пользователей, моментальное распространение информации и другие [3, с. 276].

Трансграничность. Киберпреступления — это один из немногих видов преступлений, которые можно совершить в одном месте, а вред нанести на противоположной стороне земного шара. Преступления, совершаемые с использованием информационных технологий, не имеют границ, так как совершаются в виртуальном пространстве — едином для всех стран и народов, не имеющем осязаемых в привычном смысле границ территорий.

Анонимность. Эта особенность характеризуется сразу двумя составляющими. С одной стороны, злоумышленник может совершать свои противоправные действия анонимно, например, представившись вымышленным персонажем. Эта особенность в большинстве случаев чисто психологически, что называется, «развязывает руки» преступнику, создавая уверенность безнаказанности. С другой стороны, такие преступления, как правило, не требуют активных физических действий со стороны злоумышленника, создавая для него более комфортные условия без ощущения страха быть изобличенным или пойманным «за руку». Даже в случае неудачной попытки он просто будет искать следующую жертву, не испытывая раскаяние или угрызения совести.

Моментальное распространение информации и охват многочисленной аудитории. Известно, что на начало 2024 года на Земле проживает около 8 млрд человек, почти 70 % из которых являются уникальными пользователями мобильных телефонов[1]. При этом 66 % всех жителей планеты пользуются всемирной сетью Интернет (около 5,35 млрд человек). Кроме того, известно, что единицей скорости передачи информации является Мбит/с, то есть практически моментально можно распространить нужную информацию во всем мире среди 5 млрд пользователей. Даже если с ней ознакомятся не все пользователи сразу, число оповещенных за считанные секунды впечатляет. При этом затраты на передачу информации с мировой зоной покрытия минимальны и доступны практически любому пользователю.

В 2023 году МВД РФ выявило более 100 тыс. ИТ-преступников[2]. Число ИТ-преступлений в России за 2023 год выросло на 29,7 % по сравнению с 2022-м. Доля преступлений, совершенных с использованием высоких технологий, в России последние годы держится на уровне 25 % от общего числа преступлений. Популярность телекоммуникационных технологий, социальных сетей при отсутствии адекватных средств защиты породила рост количества киберпреступлений.

Опираясь на исследования, проведенные нами ранее [4, с. 140], типичный современный киберпреступник — холостой мужчина чуть старше 30 лет со средним или средним профессиональным образованием, ранее не судим, проживающий в городе и в основном промышляющий кибермошенничеством. Жертвы киберпреступников — это пользователи гаджетов, которые не заботятся о кибербезопасности. За последний год более ⅓ пользователей подверглись атакам злоумышленников (59 % из них зафиксировано в России)[3]. Опираясь на данные исследований аналитиков Центробанка России[4], проведенного в 2023 году, среди респондентов 55,5 % пострадавших — это женщины

[1] Более 60 % человечества используют социальные сети // Интерфакс. URL: https://www.interfax.ru/world/912624 (дата обращения: 10.04.2024).

[2] Число киберпреступлений в России // TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (дата обращения: 10.03.2024).

[3] Жертвы телефонных мошенников // TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Жертвы_телефонных_мошенников (дата обращения: 10.03.2024).

[4] Центробанк составил обобщённый портрет жертвы кибермошенников // Digital Russia. URL: https://d-russia.ru/centrobank-sostavil-obobshhjonnyj-portret-zhertvy-kibermoshennikov.html (дата обращения: 10.04.2024).

(в 2022 году мужчины чаще страдали от жертв мошенников). Самым популярным среди киберпреступников способом наладить контакт с жертвой остаются телефонные звонки (54 %). Аналитики также отметили существенный рост мошенничества с помощью мессенджеров, на долю которого приходится 22,5 % случаев (+10,5 %). В мессенджерах нет системы фильтрации подозрительных звонков, как в случае с сотовыми операторами или онлайн-банкингом. Злоумышленники могут подделать аккаунт интернет-магазина, банка, портала «Госуслуги». Киберпреступники обычно выдают себя за следователей, сотрудников организаций и ведомств. Иногда они обращаются к сотрудникам организаций от имени начальства. Чаще всего провернуть мошеннические схемы удается с гражданами, имеющими среднее образование (41,3 %) и средний уровень дохода (44,8 %). В подавляющем большинстве случаев (64,1 %) вымогателям удается выманить у жертвы до 20 тыс. рублей. В других ситуациях размер ущерба значительно выше. Так, 4,3 % граждан перевели злоумышленникам более 1 млн рублей. Примечательно, что о правилах безопасности вспоминают 86,2 % респондентов, пострадавших или столкнувшихся с мошенниками. 9,8 % забыли о них, а еще 4 % опрошенных вовсе не знают о таких правилах. Признаком общения с киберпреступником является разговор о деньгах и ограничение времени на принятие решения.

В последнее время все чаще стали фиксироваться DDoS-атаки [5, с. 190], в том числе целевые. В целях противодействия им в Оренбурге на базе госуниверситета открылся центр Национального киберполигона, где моделируются потенциальные кибератаки, позволяя специалистам учиться и реально отрабатывать отражение атак.

Международный уровень противодействия киберпреступности закреплен Советом Европы в 2001 году подписанием Будапештской конвенции по кибепреступности. Российский законодатель старается оперативно реагировать на появление новых видов преступных деяний. Так, помимо главы 28 УК РФ «Преступления в сфере компьютерной информации», за последние годы не раз вносились изменения и дополнения в Уголовный кодекс (ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа» и др.) [2, с. 282].

Важными в целях предотвращения роста числа киберпреступлений являются анализ методов и техник, используемых злоумышленниками в киберпространстве, и изучение их мотиваций, целей и стратегий. Немаловажным является и изучение уязвимостей информационных систем и сетей, анализ средств и методов защиты от кибератак, и разработку стратегий и политик для предотвращения и противодействия киберпреступности. Эффективными способами противодействия кибермошенничеству являются своевременное информирование потенциальных жертв (обычных граждан) посредством социальной рекламы, проведение разъяснительных бесед, а также повышение грамотности граждан, в первую очередь, информационной и финансовой.

Заключение и выводы

В настоящее время рост количества преступлений, совершенных в киберпространстве с использованием современных информационных технологий, угрозы информационной безопасности становятся все более серьезными и вызывают значительное беспокойство во всем мире. Все мировое сообщество находится под постоянным давлением. Чтобы обеспечить кибербезопасность, необходимо постоянное соблюдение правил защиты информации на всех уровнях, разработка стратегий для снижения рисков, повышение компьютерной и информационной грамотности сотрудников и граждан. Это поможет повысить уровень безопасности, сократить степень уязвимости и сохранить стабильность.

В целом, решение проблем кибербезопасности требует комплексного подхода и совместных усилий всех стран и компаний. Необходимо разрабатывать эффективные стратегии и программы, которые позволят обеспечить стабильное развитие экономики и защиту национальных интересов. Необходимо усиливать международное сотрудничество и координацию действий, чтобы обеспечить эффективную защиту интересов всех стран.

Список источников

1. Хоменко А. Н. К вопросу о виктимизации жертв киберпреступлений // Виктимология. 2021. Т. 8, № 2. С. 143–148.

2. Мордвинов К. В., Удавихина У. А. Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция. 2022. № 1 (11). С. 83–88.

3. Шевко Н. Р. Мошенничество в киберпространстве: реальный ущерб в виртуальном мире // Вестник Восточно-Сибирского института МВД России. 2023. № 3 (106). С. 276–284.

4. Шевко Н. Р. Особенности киберпреступности: состояние и тенденции // Уголовная политика в условиях цифровой трансформации : сборник материалов II Всероссийской научно-практической конференции (Казань, 27 апреля 2023 г.). Казань : Отечество, 2023. С. 135–141.

5. Ляпин А. Е. Новые угрозы кибербезопасности как следствие цифровизации в топливно-энергетическом комплексе // Цифровая трансформация промышленности: современные формы устойчивого развития : сборник научных трудов по материалам 4-й Всероссийской научно-практической конференции (Москва, 09 ноября 2023 г.). Москва : Русайнс, 2023. С. 188–195.

ВКЛАД АВТОРОВ
Вклад авторов равноценный.

CONTRIBUTION OF AUTHORS
Contributions by the authors are equal.

КОНФЛИКТ ИНТЕРЕСОВ
Конфликт интересов отсутствует.

CONFLICT OF INTEREST
There is no conflict of interest.

Дата поступления статьи / Received: 16.04.2024.
Дата рецензирования статьи / Revised: 15.05.2024.
Дата принятия статьи к публикации / Accepted: 20.05.2024.