DOI 10.35775/PSI.2025.66.1.013
УДК 32

В.В. КОМЕРЦОВ
старший преподаватель кафедры
информационного обеспечения ОВД РЮИ МВД России,
Россия, г. Ростов-на-Дону

С.В. ХАРЛАМОВА
магистрант кафедры политологии и этнополитики
РАНХ и ГС при Президенте РФ,
Россия, г. Москва

Д.КЁ. ГРИГОРЯН
кандидат политических наук, профессор кафедры
политологии и этнополитики РАНХ и ГС при Президенте РФ,
Россия, г. Москва

К ВОПРОСУ О КИБЕРПРЕСТУПЛЕНИЯХ В ОНЛАЙН ПРОСТРАНСТВЕ

В данной статье рассмотрены актуальные проблемы кибербезопасности, которые имеют место в онлайн пространстве, а также современные тенденции в развитии киберпреступности. Анализ охватывает различные ее виды, такие как фишинг, кражи, взломы, мошенничество с использованием технологий и распространения дезинформации и вредоносного ПО. Освещены способы борьбы с киберугрозами в контексте как законодательной регуляции, так и развития технологических решений.

Ключевые слова: *киберпреступность, законность, безопасность, мошенничество, цифровые технологии.*

Мир стремительно движется в цифровую эпоху. Технологии проникают во все сферы жизни общества, стараясь сделать ее удобнее и эффективнее, облегчая как профессиональную деятельность – электронный документооборот, онлайн-коммуникации, так и решения повседневных задач – онлайн-платежи, получение государственных услуг. Но, вместе с этим, распространение новых технологий создает и новые риски. Киберпреступность представляет угрозу личной безопасности, собственности, а также стабильности общества и государства в целом, потенциально нарушая основные принципы правопорядка. В Уголовном кодексе Российской Федерации содержатся статьи, относящиеся к так называемым «киберпреступлениям», а именно ст. 272, ст. 273, ст. 274, 274.1. Данные статьи находятся в главе 28 «Преступления в сфере компьютерной информации» УК РФ [15].

Киберпреступность – это форма преступной деятельности, которая использует компьютерные системы и сети для совершения правонарушений. От кражи

личных данных до несанкционированного доступа к критически важной инфраструктуре, от финансовых махинаций до дискредитации и дезинформации – спектр киберпреступлений велик и постоянно расширяется, что еще больше усложняет систему контроля над ними.

Однако, не смотря на развитые технологии современности, тенденция киберпреступности наблюдалась в западных странах еще в 1960-1970 гг. В СССР первые киберпреступления были зафиксированы в начале 1980-х годов. Официально первое преступление с использованием компьютера было зарегистрировано в 1979 г. В Вильнюсе. Занесение этого преступления в международный реестр подобных правонарушений стало началом развития нового вида преступности в России, а также актуализировало необходимость в разработке эффективных механизмов уголовно-правового регулирования ответственности за подобные деяния.

В 1991 году была предпринята одна из первых попыток законодательного регулирования преступлений в компьютерной сфере, а именно – введение проекта Закона РСФСР «Об ответственности за правонарушения при работе с информацией», который предлагал введение различных видов ответственности: дисциплинарной, гражданско-правовой, административной и уголовной, а также поправки в Уголовный Кодекс. Однако проект так и не был принят из-за неразработанного законодательного поля в России в такой области права [19].

Принятие Верховным Советом России в 1992 году постановления о порядке введения в действие Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» стало более успешным шагом в реформировании уголовного законодательства. Этот закон впервые предусматривал уголовную ответственность за выпуск чужих программ или баз данных под чужим именем, а также за их незаконное воспроизведение или распространение.

Правительству Российской Федерации было поручено до конца 1992 года подготовить поправки в Гражданский, Уголовный кодексы и другие законодательные акты, касающиеся правовой охраны компьютерных программ и информации.

В 1994 году был разработан проект поправок к Уголовному Кодексу Российской Федерации, устанавливающий ответственность за такие преступления, как незаконное присвоение программ, личных файлов или баз данных; фальсификацию или уничтожение информации в автоматизированных системах; несанкционированный доступ к информационным системам – путем получения паролей, нарушения порядка доступа или обхода защитной системы; а также рассылки опасных компьютерных вирусов, которые могут заблокировать доступ к важной информации. Но проект не реализовался до конца года.

Но уже в начале 1995 года была создана программа, включающая главу 29 Уголовного Кодекса Российской Федерации «Компьютерные преступления». Глава, посвященная кибербезопасности, регулировала несанкционированный доступ к компьютерным системам, незаконное завладение программами

и данными, повреждение или уничтожение программ и баз данных, распространение компьютерных вирусов, и нарушение правил безопасности информационных систем.

Глава 28 «Преступления в сфере компьютерной информации» была включена в Уголовный Кодекс Российской Федерации 1 января 1997 года, включая статьи – 272 «О неправомерном доступе к компьютерной информации», 273 ««О создании и распространении вредоносных программ» и 274 «О нарушении правил эксплуатации компьютерных систем».

В 2011 году были внесены последние поправки в главу 28 УК РФ, но проблемы киберпреступности продолжали и продолжают расти в условиях информационного общества [9].

Современная киберпреступность обладает рядом характерных особенностей. Прежде всего она всегда связана с использованием компьютерной техники и информацией, хранящейся, обрабатывающейся и используемой в сети Интернет. Компьютерные устройства и сети выступают в качестве инструмента преступления, а вредоносные программы – как орудие ее совершения. В отличие от традиционных преступлений, киберпреступления часто характеризуются транснациональным характером, сложностью расследования из-за анонимности и географической распределенности злоумышленников, а также высокой скоростью распространения вредоносного воздействия.

Исследователи считают, что факторами изменения киберугроз и рисков в 2024 году стали: искусственный интеллект, машинное обучение, различные дипфейки, также целевые атаки, такие как – хактивизм и различные технологии, которые получают широкое распространение в обществе [9]. (рис. 1.).

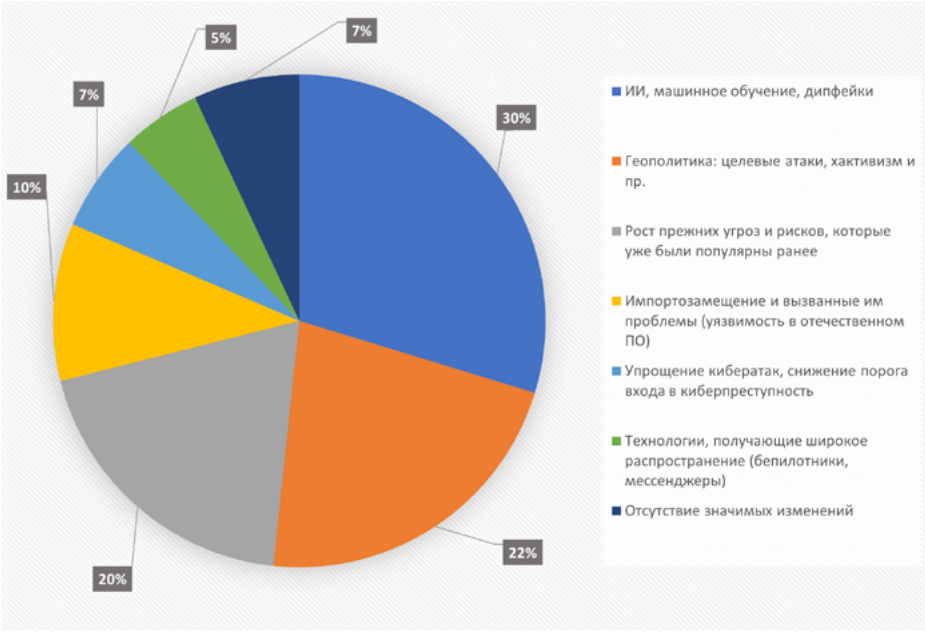
Киберпреступления затрагивают сразу два типа общественных отношений – отношения безопасности обращения компьютерной информации и отношения, связанные с ней, но имеющие влияние на реальный мир, например, отношения собственности. Отличительной чертой является то, что для совершения таких преступлений используют специальные знания в области информационных технологий или сложные программные комплексы, поэтому часто расследование киберпреступлений сталкивается с рядом трудностей, вызванными недостатком или отсутствием определенных и нужных навыков в данной сфере.

Киберпреступления можно классифицировать по разным критериям, например: объект посягательства, предмет преступления и методы совершения.

В зависимости от объекта преступления, выделяют экономические киберпреступления. Они направлены на причинение материального вреда компаниям, организациям и частным лицам, включая кражи денежных средств, финансовые мошенничества и незаконный доступ к конфиденциальной информации.

Также существуют посягательства на личные права и неприкосновенность частной жизни в киберпространстве, которые проявляются в краже личных данных граждан, шантаже, дискредитации, незаконной слежке и других подобных серьезных нарушениях прав и свобод людей.

Рисунок 1 .Факторы изменения киберугроз и рисков в 2024 году



Так, например, 8 января 2023 года в сети неизвестные хакеры опубликовали базу данных более 115 миллионов пользователей «Альфа-банка». Данные содержали ФИО, даты рождения, номера телефонов, банковских карт и счетов граждан. Злоумышленники утверждали, что получили данные еще в октябре 2023 года и распространили информацию через собственный сайт и Telegram-канал. Они подчеркивали, что база содержит данные 38 миллионов уникальных физических и юридических лиц. Независимая проверка данных, проведенная корреспондентом CNews, подтвердила наличие в утечке личной информации.

Несмотря на эти доказательства, «Альфа-банк» неоднократно опровергал информацию об утечке как осенью 2023 года, так и в январе 2024 года. Заявление сводилось к тому, что опубликованные данные были собраны из различных открытых источников, где пользователи добровольно оставляли личную информацию о себе. Однако масштабы данной утечки, заставляют усомниться в этом объяснении [18].

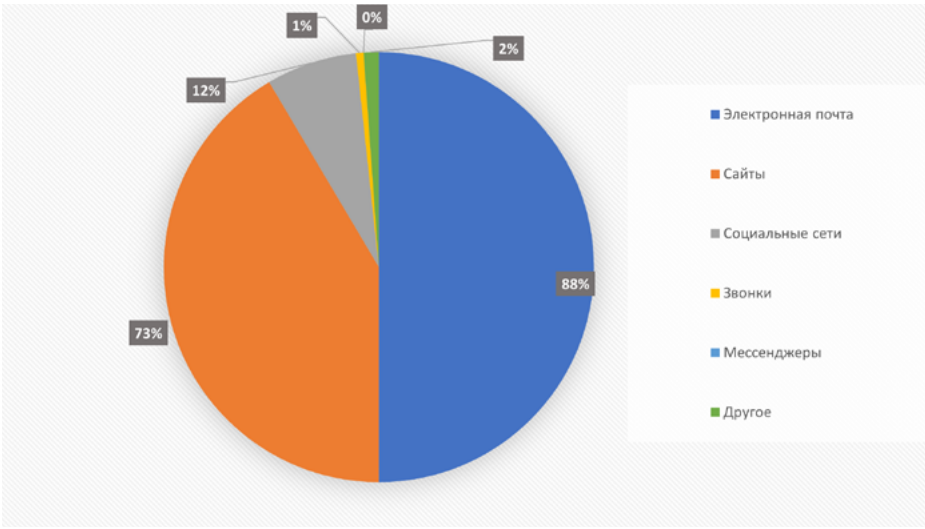
Кроме того, отличают киберпреступления против общественных и государственных интересов, которые заключаются в дестабилизации безопасности государства и общественного порядка, например, несанкционированный доступ к государственным системам, кибератаки на критические важную инфраструктуру, распространение дезинформации.

Киберпреступления в глобальных сетях характеризуются высокой степенью скрытности, обусловленной особенностями киберпространства; трансграничным характером, охватывающим разные государства; высокой квалификацией

преступников, использующих сложные и постоянно меняющиеся методы; возможностью автоматизированного совершения преступления в нескольких точках одновременно, а также способностью объединять относительно слабые компьютерные ресурсы в мощную преступную силу.

В условиях глобализации число кибернападений растет, при этом все больше атак направляется не только на отдельного индивида, но и на малые и крупные предприятия и организации, а также различные органы власти. На основе III квартала 2024 года, было выявлено, что социальная инженерия по-прежнему остается одним из самых распространенных методов атак как на компании, так и на частные лица. Для организаций ведущим каналом социальной инженерии остается электронная почта, тогда как для частных пользователей – сайты. Злоумышленники активно используют популярность социальных сетей среди обычных пользователей для проведения кибератак. В сравнении с предыдущим кварталом, этот метод стал применяться на 4% чаще. Наиболее востребованной социальной сетью среди преступников стал Facebook [1]. (рис. 2).

Рисунок 2. Используемые злоумышленниками каналы социальной инженерии



Также, в ноябре нынешнего года, граждан Российской Федерации предупредили о новейшей схеме киберпреступности, связанной с порталом «Госуслуги». О таком виде мошенничества информировало МВД в Telegram-канале «Вестник киберполиции России» [3]. В ведомстве предупреждают о том, что мошенники рассылают электронные письма или SMS-сообщения, утверждая, что была предпринята попытка войти в аккаунт на портале. В этих сообщениях также содержится просьба о том, что нужно как можно срочно позвонить по указанному номеру телефона.

Во время телефонного разговора преступники выдают себя за сотрудников службы поддержки «Госуслуг». В МВД отметили, что после выполнения всех указаний злоумышленников абонент лишается доступа к своему профилю на портале. В результате на жертву оформляются кредиты на огромные суммы. После ряда таких событий в МВД порекомендовали в таких случаях сразу обращаться в полицию и проверять свою кредитную историю, чтобы убедиться в том, что мошенники не успели оформить кредит [10].

19 июля произошел крупный сбой в работе операционных систем Windows, который вызвал появление «синих экранов смерти» по всему миру. Причиной этого стала ошибка в обновлении CrowdStrike Falcon Sensor – агента кибербезопасности, разработанного для защиты устройств от различных угроз. По информации Microsoft, инцидент затронул 8,5 миллионов устройств из разных секторов, таких как авиаперевозки, медицинские учреждения, банки и другие.

Такое событие не осталось незамеченным злоумышленниками. Поэтому киберпреступники использовали проблему в качестве для социальной инженерии. Уже через несколько дней после произошедшего Bleeping Computer – сообщество пользователей, созданное для решения проблем, возникающих при использовании компьютеров и интернета, обнаружили фишинговые письма, замаскированные под руководство по восстановлению от Microsoft. В прикрепленном документе были инструкции по использованию инструмента, который автоматизирует удаление проблемного драйвера CrowdStrike с устройств Windows. Но при его запуске на устройство жертвы устанавливалось Daolpu – вредоносное ПО, похищающее данные [1].

Обеспечение безопасности в онлайн-пространстве как для государственных органов, так и для общества в целом требует разработки комплексного подхода по борьбе с киберпреступностью, разработанного на основе строгого контроля. Эти меры должны включать в себя усиленную бдительность государственных структур в отношении обработки персональных данных, а также создание и доступность продуктов цифровой безопасности для широкой общественности, чтобы каждый гражданин мог сам себя обезопасить и предостеречь от нападений киберпреступников.

Считается необходимым обеспечить всестороннюю поддержку жертвам киберпреступлений, включая социальную и юридическую помощь, и гарантировать им доступ к правоохранительным органам в любое время. Поскольку киберпреступность часто носит затяжной и повторяющийся характер, то своевременное обращение в правоохранительные органы является критически важным фактором в борьбе с киберугрозами.

В настоящее время, Российская Федерация ставит одной из своих важнейших и приоритетных задач – борьбу с киберпреступлениями. Глава страны, Владимир Владимирович Путин, уделяет значительное внимание вопросам, связанных с кибербезопасностью страны. В своем выступлении на заседании коллегии ФСБ России 24 февраля 2021 года он отметил необходимость разработки эффективной стратегии борьбы с киберпреступностью. По мнению, Президента,

в условиях жесткой геополитической конкуренции в цифровом пространстве необходимы новые подходы к обеспечению кибербезопасности [6].

Цифровизация всех сфер жизни, от банковских операций, до государственного управления, создает беспрецедентные возможности для злоумышленников. Распространение высокоскоростного интернета, мобильных устройств и облачных технологий расширяет географию преступной деятельности и затрудняет ее пресечение. В современном мире, киберпреступления модифицируются, становятся более масштабными и опасными.

В связи с этим правоохранительные органы должны не просто реагировать на уже совершенные преступления, а активно выявлять и предотвращать их, используя современные технологии анализа данных для прогнозирования преступных тенденций и выявление потенциальных угроз.

Кроме того, борьба с киберпреступностью требует международного сотрудничества, совершенствования законодательной базы, постоянного развития технологий защиты информации и повышения цифровой грамотности населения. Только комплексный подход, объединяющий усилия правоохранительных органов, частного сектора и граждан, позволит эффективно противостоять растущей угрозе киберпреступлений и обеспечить безопасность в онлайн-пространстве.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Актуальные киберугрозы: III квартал 2024 года // https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/#id4.
2. **Арипшев А.М.** Развитие киберпреступности в цифровом обществе // Журнал прикладных исследований. 2023. № 5.
3. Вестник Киберполиции России // https://t.me/cyberpolice_rus.
4. **Григорян Д.К., Кондратенко Е.Н.** Характерные особенности современных информационных войн политической направленности // Государственное и муниципальное управление. Ученые записки. 2024. № 2.
5. **Иванова Л.В.** Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1.
6. **Кобец П.Н.** Киберпреступность: современные виды, причины, ее порождающие, и особенности предупреждения // Вестник Самарского юридического института. 2022. № 1 (47).
7. **Нестерович С.А.** Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов // Вестник науки и образования. 2018. № 8 (44).
8. **Номоконов В.А., Тропина Т.Л.** Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24.
9. Прогноз развития киберугроз и средств защиты информации – 2024 // https://www.anti-malware.ru/analytics/Threats_Analysis/2024-Forecast.

10. Россиян предупредили о новой схеме мошенничества с «Госуслугами» // https://lenta.ru/news/2024/11/25/rossiyan-predupredili-o-novoy-sheme-moshennichestva-s-gosuslugami/amp/.
11. **Солоненко К.М.** Киберпреступления в Российской Федерации: сущность, особенности, виды // Вопросы российской юстиции. 2022. № 20.
12. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».
13. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернетпортал правовой информации // http://www.pravo.gov.ru.
14. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Официальный интернетпортал правовой информации.
15. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 25.03.2022) // «Собрание законодательства РФ». 17.06.1996. № 25.
16. Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ.
17. **Хачидогов Р.А.** Основные методы противодействия киберпреступности в Российской Федерации // Журнал прикладных исследований. 2023. № 6.
18. Хакеры опубликовали данные 38 млн клиентов «Альфа-банка». Банк опровергает утечку // https://www.cnews.ru/news/top/2024-01-09_alfa-bank_byl_vzloman.
19. **Шогенов З.А.** Киберпреступность как одна из основных проблем современного общества // Право и управление. 2023.

V.V. KOMERTSOV
Senior Lecturer Departments of Information
support Department of Internal Affairs of the Ministry
of Internal Affairs of Russia, Rostov-on-Don

S.V. KHARLAMOVA
Undergraduate of the Department of Political
Science and Ethnopolitics of the Russian Academy of Sciences
and GS under the President of the Russian Federation,
Moscow, Russia

D.K. GRIGORYAN
Candidate of Political Sciences, Professor
of the Department of Political Science and Ethnopolitics of the Russian
Academy of Sciences and the State Duma under the President
of the Russian Federation, Moscow, Russia

ON THE ISSUE OF CYBERCRIMES IN THE ONLINE SPACE

This article examines the current problems of cybersecurity that occur in the online space, as well as current trends in the development of cybercrime. The analysis covers various types of phishing, theft, hacking, fraud using technology and spreading disinformation and malware. The article highlights ways to combat cyber threats in the context of both legislative regulation and the development of technological solutions.

Key words: *cybercrime, legality, security, fraud, digital technologies.*