

ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ И ИХ ПРОЯВЛЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

Эгамбергенов Отабек Азаматович¹, Халмуратов Омонбой Утамурастович²

¹Магистрант Ургенчского филиала Ташкентского университета информационных технологий имени Мухаммада Ал-Хоразмий

²Заместитель директора по учебной работе Ургенчского филиала Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий
E-mail: egambergenovotabek@gmail.com

KEYWORDS

Киберпреступления, социальные сети, кибербуллинг, фишинг, мошенничество, конкурентные программы, кибератаки, интернет-безопасность, киберугрозы, цифровая преступность

ABSTRACT

В данной работе рассматриваются основные виды киберпреступлений и их проявления в социальных сетях. Анализируются такие явления, как кибербуллинг, фишинг, мошенничество с кредитными картами, распространение наследственных программ и атаки на компьютерные системы. Особое внимание уделяется влиянию киберпреступлений на пользователей социальных сетей, а также методам их предотвращения. Исследование роли государства и технологий в борьбе с кибербезопасностью, включая использование инструментов кибербезопасности и правового регулирования.

Введение

В современном обществе социальные сети стали неотъемлемой частью повседневной жизни, предоставляя платформы для общения и обмена информацией. Однако с ростом их популярности увеличивается и количество киберпреступлений, совершенных посредством таких ресурсов. Кибербуллинг, фишинг и распространение ложной информации стали распространенными явлениями, негативно влияющими на пользователей. Особенно тревожным является тот факт, что многие из этих преступлений целенаправленно ориентированы на молодежь, восприимчивую к манипуляциям в интернет-пространстве. Важным аспектом данного обсуждения является осознание платформ, таких как Даркнет, которые предоставляют анонимность и затрудняют выявление преступников. Для лучшего понимания различных типов киберпреступлений необходима визуализация их проявлений, представляемая в рамках исследования, что ярко демонстрирует изображение.

Обзор киберпреступлений и их актуальность в цифровую эпоху

В цифровую эпоху киберпреступления становятся неотъемлемой частью социальной и экономической динамики, о чем свидетельствует их растущая актуальность и сложность. Увеличение числа пользователей сетей и онлайн-платформ создает множество возможностей для злоупотреблений и преступных действий, таких как финансовые киберпреступления и преступления против целостности данных. В частности, с учетом увеличения преступности в киберпространстве, исследователи обращают внимание на необходимость анализа, как эти преступления влияют на социальные структуры и организованные преступные сети. Например, в современных научных исследованиях обсуждаются виды киберпреступлений и их влияние на организованную преступность в контексте государственных структур [1], что подчеркивает трансформацию отношений между государством и преступностью. Кроме того, исследования о рынке преступлений в киберпространстве помогают понять, как

технологии меняют природу правонарушений и преступников [2].

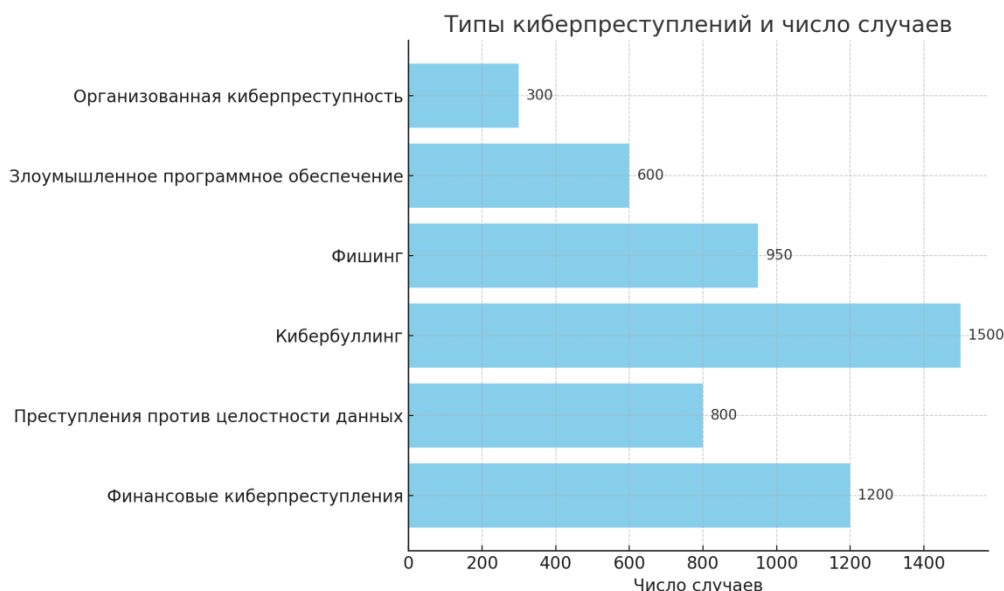


Диаграмма показывает различные типы киберпреступлений и количество случаев для каждого из них. Число случаев варьируется от 300 до 1500, с кибербуллингом как наиболее распространенным типом преступления.

Виды киберпреступлений

Киберпреступления представляют собой разнообразный набор незаконных действий, осуществляемых в цифровой среде, и их последствия становятся все более заметными в контексте социальных сетей. Виды киберпреступлений охватывают как финансовые махинации, так и преступления, связанные с нарушением прав личности, такие как кибербуллинг, о чем свидетельствует исследование Н.Р. Шевко и И.И. Исакова,

которое подчеркивает психологические аспекты такого поведения. Важно отметить, что цифровизация, способствующая изменению коммуникационных процессов, также повлияла на уровень преступности, обострив взаимодействие между законопослушными гражданами и преступниками [4]. В этом контексте следует также учитывать, что наряду с традиционными киберпреступлениями, современное государство сталкивается с новыми вызовами, включая оргпреступность в киберпространстве [3].

Виды киберпреступлений

Тип киберпреступления	Описание	Доля (% в 2023)	Источник
Фишинг	Мошенничество с использованием поддельных сайтов для получения личных данных.	34	Cybersecurity Ventures
Мошенничество с кредитными картами	Использование украденных данных кредитных карт для несанкционированных покупок.	25	Statista
Вредоносные программы	Программы, направленные на повреждение или кражу данных.	20	Kaspersky Lab

Кибербуллинг	Запугивание или преследование через социальные сети.	15	Pew Research Center
Атаки на системы	Попытки взлома и нарушения работы компьютерных систем.	6	Verizon Data Breach Investigations Report

Определение и примеры распространенных киберпреступлений

Киберпреступления представляют собой сложный набор деяний, осуществляемых в сетевой среде, и их разнообразие сложно переоценить. Чаще всего встречающиеся виды включают кибербуллинг, фишинг и несанкционированный доступ к данным. Кибербуллинг, как подчеркивается в документе, являясь одной из форм online-травли, может иметь серьезные психологические последствия для жертв. В свою очередь, фишинг, представляющий собой метод мошенничества из-за ненадлежащих действий, требует внимания как со стороны исследователей, так и практиков, что обсуждается в [6]. Кроме того, недостаток согласия среди социальных контактов может снизить вероятность совершения преступлений в интернете, о чем говорит исследование о сходстве в девиантности, представленное в [5]. Эти примеры подчеркивают важность комплексного понимания киберпреступлений для эффективного противодействия им в рамках социальных сетей.

Проявление киберпреступлений в социальных сетях

Современные социальные сети становятся площадкой для разнообразных киберпреступлений, о чём свидетельствует рост инцидентов, связанных с кибербуллингом и мошенничеством. Виртуальное пространство облегчает анонимность злоумышленников, что создаёт условия для распространения угроз, таких как шантаж и кибердискриминация. Объединение различных подходов к противодействию киберпреступности важно для защиты пользователей, что включает использование технологий вроде honeypot для предотвращения кибератак, как отмечается в исследовании [7]. Вдобавок, ответственность

государства за защите цифровых активов и соблюдение законов против киберпреступлений остаётся высоко актуальной темой, особенно в контексте международных норм, отмеченных в [8]. Таким образом, анализ проявлений киберпреступлений в социальных сетях требует глубокой интерпретации психологических эффектов, а также оценки правовых и технологических мер, направленных на борьбу с данными угрозами, включая кибербуллинг.

Анализ того, как киберпреступления происходят на платформах социальных медиа

В последние годы платформы социальных медиа стали основными полями для киберпреступлений, которые варьируются от кражи личных данных до распространения дезинформации. Мошенники используют уязвимости платформ для осуществления атак, однако общественное внимание в основном сосредоточено на последствиях этих преступлений, а не на слабых местах самих технологий, которые делают возможным их совершение. Согласно исследованию, простое игнорирование уязвимостей препятствует эффективному управлению рисками киберугроз [9]. Социальные медиа, в частности, расширили возможности преступников, позволяя им действовать дистанционно, что кардинально изменило характер преступлений [10]. Более того, в исследовании о кибербуллинге отмечается, как динамика взаимодействий в интернете способствует созданию агрессивной среды, в которой жертвы оказываются легко доступны, подчеркивая необходимость осознания этих механизмов для разработки эффективных мер безопасности.

В современном цифровом обществе социальные сети стали неотъемлемой частью повседневной жизни, предоставляя пользователям платформы для общения, обмена

информацией и ведения бизнеса. Однако с ростом популярности этих платформ увеличивается и количество киберпреступлений, совершаемых в их рамках. Ниже представлены основные виды киберпреступлений, их проявления в социальных сетях и методы защиты от них.

1. Фишинг

Описание: Фишинг — это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей, таким как логины и пароли, путем обмана. Мошенники отправляют сообщения или создают сайты, маскируясь под доверенные организации, чтобы заставить пользователей раскрыть личную информацию.

Проявления в социальных сетях:

- Рассылка личных сообщений от имени друзей или известных компаний с просьбой перейти по ссылке и ввести личные данные.
- Создание поддельных страниц входа, имитирующих реальные сайты социальных сетей, для кражи учетных данных.

Методы защиты:

- Внимательно проверяйте адреса ссылок перед переходом по ним.
- Не вводите личные данные на подозрительных сайтах.
- Используйте двухфакторную аутентификацию для защиты аккаунтов.

2. Кетфишинг

Описание: Кетфишинг (от англ. "catfishing") — это форма мошенничества, при которой злоумышленник создает фальшивый профиль в социальных сетях или на сайтах знакомств с целью обмана жертвы. Мошенник может использовать вымышленные или украденные фотографии и информацию, чтобы завоевать доверие и в конечном итоге получить личные данные или деньги.

Проявления в социальных сетях:

- Создание привлекательных фальшивых профилей для установления доверительных отношений с целью последующего обмана.
- Использование украденных фотографий и информации для создания иллюзии реального человека.

Методы защиты:

- Будьте осторожны при общении с незнакомыми людьми в сети.
- Проверяйте подлинность профилей, используя обратный поиск изображений.
- Не делитесь личной информацией с малознакомыми людьми.

3. Социальная инженерия

Описание: Социальная инженерия — это метод манипуляции людьми с целью получения конфиденциальной информации или доступа к системам. Злоумышленники используют психологические приемы, чтобы заставить жертву раскрыть пароли, финансовые данные или другую важную информацию.

Проявления в социальных сетях:

- Сообщения от "друзей" с просьбой о срочной финансовой помощи.
- Предложения принять участие в опросах или конкурсах, требующих ввода личных данных.

Методы защиты:

- Скептически относитесь к неожиданным просьбам о помощи или информации.
- Подтверждайте личность отправителя через другие каналы связи.
- Не переходите по ссылкам и не скачивайте вложения из подозрительных сообщений.

4. Киберсталкинг

Описание: Киберсталкинг — это форма преследования, при которой злоумышленник использует интернет и социальные сети для слежки, запугивания или домогательства жертвы. Это может включать отправку угрожающих сообщений, распространение

ложной информации или публикацию личных данных без согласия.

Проявления в социальных сетях:

- Постоянные нежелательные сообщения или комментарии.
- Создание фальшивых профилей для слежки за жертвой.
- Публикация личной информации или фотографий без разрешения.

Методы защиты:

- Настройте параметры конфиденциальности, ограничив доступ к вашей информации.
- Блокируйте и сообщайте о подозрительных пользователях.
- Сохраняйте доказательства преследования и обращайтесь в правоохранительные органы при необходимости.

5. Мошенничество в электронной коммерции

Описание: Мошенничество в электронной коммерции включает создание поддельных интернет-магазинов или объявлений с целью обмана пользователей и кражи их денег или личных данных. Злоумышленники могут предлагать несуществующие товары по заниженным ценам или продавать поддельные продукты.

Проявления в социальных сетях:

- Реклама товаров или услуг с чрезмерно низкими ценами.
- Продажа товаров через поддельные страницы или группы.

Методы защиты:

- Проверяйте репутацию продавца и читайте отзывы других покупателей.
- Используйте безопасные методы оплаты, такие как наложенный платеж или защищенные платежные системы.
- Будьте осторожны с предложениями, которые кажутся слишком хорошими, чтобы быть правдой.

Заключение

Анализируя различные формы киберпреступлений и их проявления в социальных сетях, можно сделать вывод о необходимости комплексного подхода к их предотвращению и регулированию. Современные технологии значительно изменили ландшафт преступности, в том числе через пропаганду и использование кибертерроризма, что подчеркивается исследованием, согласно которому кибертерроризм считается транснациональным преступлением и требует документов, регламентирующих его развитие в киберпространстве [11]. Кроме того, использование информационных технологий преступными группами создает новые угрозы, сочетая традиционные методы с современными цифровыми инструментами [12]. Эти исследования подчеркивают необходимость не только совершенствования законодательства и правоохранительных механизмов, но и повышения осведомленности пользователей об опасностях киберпреступлений. Для дальнейшего анализа, изображение иллюстрирует специфику кибербуллинга, что подчеркивает значимость данного исследования для понимания манипуляций в социальных сетях.

Подведение итогов ключевых моментов и важности осведомленности о кибербезопасности

Осведомленность о кибербезопасности становится все более актуальной в условиях повсеместной цифровизации жизни и непрерывного роста числа пользователей социальных сетей. Киберпреступления, такие как кибербуллинг, фишинг и кража личных данных, не только наносят вред индивидуумам, но и подрывают доверие к онлайн-платформам. Упоминание о кибербуллинге, подробно изложенном в документе, иллюстрирует, как негативное поведение в виртуальном пространстве может иметь долгосрочные психологические последствия. Понимание структуры интернета, описанной в , подчеркивает необходимость тщательной навигации через разные уровни сети для защиты

своей информации. Таким образом, повышая осведомленность о киберугрозах, пользователи становятся более защищенными и способны противостоять потенциальным рискам. Завершая анализ, можно сказать, что профилактика киберпреступлений должна основываться на комплексном подходе, сочетая образование, технологические решения и социальную ответственность.

References

1. J. J. K. N. K. M. M. "Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes" 'Fiat Justisia', 2019, [Online]. Available: <https://core.ac.uk/download/297833029.pdf> [Accessed: 2025-04-01]
2. K. E. K. E. L. E. R. E. A. "Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness" 'Springer Science and Business Media LLC', 2019, [Online]. Available: <https://core.ac.uk/download/219690178.pdf> [Accessed: 2025-04-01]
3. G. A. "Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy" 'University of South Florida Libraries', 2011,
4. S. G. "Adversarial behaviours knowledge area" 2019,
5. P. V. "Características de los métodos de criminalística para cometer delitos informáticos y peculiaridades de su prevención" CICSIAL-RELIGACIÓN. CENTRO DE INVESTIGACIONES EN CIENCIAS SOCIALES Y HUMANIDADES DESDE AMÉRICA LATINA, 2019, [Online]. Available: <https://core.ac.uk/download/305104738.pdf> [Accessed: 2025-04-01]
6. C. D. A. "Applying the Full Protection and Security Standard of International Investment Law to Digital Assets" WERNER PUBLISHING COMPANY, 2011, [Online]. Available: <https://core.ac.uk/download/2707938.pdf> [Accessed: 2025-04-01]
7. R. S. V. G. J. W. K. M. "Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders" 'SAGE Publications', 2019, [Accessed: 2025-04-01]
8. H. P. J. M. W. R. "Cyber-crime Science = Crime Science + Information Security" Centre for Telematics and Information Technology, University of Twente, 2010, [Online]. Available: <https://core.ac.uk/download/pdf/11476794.pdf> [Accessed: 2025-04-01]
9. L. A. "Unpacking the political-criminal nexus in state-cybercrimes: a macro-level typology" 2023, [Online]. Available: <https://core.ac.uk/download/573436804.pdf> [Accessed: 2025-04-01]
10. A. L. D. M. D. O. F. E. A. "The effect of digitalization on the extent of criminal activity in the context of the pandemic" Primmate, 2023, [Online]. Available: <https://core.ac.uk/download/578306270.pdf> [Accessed: 2025-04-01]
11. L. A. "Unpacking the political-criminal nexus in state-cybercrimes: a macro-level typology" 2023, [Online]. Available: <https://core.ac.uk/download/573436804.pdf> [Accessed: 2025-04-01]
12. A. G. L. A. "Criminal markets and networks in cyberspace" 2022, [Online]. Available: <https://core.ac.uk/download/554062474.pdf> [Accessed: 2025-04-01]
13. Особенности проявления кибербуллинга в социальных сетях, 2025. [Online]. Available: <https://sciup.org/file/picture/142215809/osobennosti-projavenija-kiberbullinga-v-socialnyh-setjah.png>
14. Представление слоев Интернета: КЛИРХЕТ, ГЛУБОКАЯ СЕТЬ и ДАРКХЕТ., 2025. [Online]. Available: https://syntheticdrugs.unodc.org/uploads/syntheticdrugs/res/cybercrime/online trafficking/online sales platforms_html/Cyber_4_RU.PNG
15. Образ хакера в современных концепциях кибербезопасности., 2025.