EURASIAN JOURNAL OF ACADEMIC RESEARCH
Innovative Academy Research Support Center
UIF = 8.1 | SJIF = 5.685 www.in-academy.uz

ОБЗОР КИБЕРПРЕСТУПНОСТИ В КОНТЕКСТЕ СОЦИАЛЬНЫХ СЕТЕЙ

Норкулова Гавхаршодбегим Алишер кизи

https://www.doi.org/10.5281/zenodo.8069174

ARTICLE INFO

Received: 14th June 2023
Accepted: 21th June 2023
Online: 22th June 2023

KEY WORDS

ABSTRACT

Платформы социальных медиа стали основными источниками новостей и информации для значительной части населения. Простота обмена и распространения информации на этих платформах привела к быстрому распространению фальшивых новостей, что делает крайне важным понимание их влияния на общество и кибербезопасность.

Также в данной работу рассматривается распространение фальшивых новостей. Фальшивые новости способны манипулировать общественным мнением, подрывать доверие к институтам и способствовать социальным беспорядкам. Изучая динамику распространения фальшивых новостей в сетях социальных медиа, данное исследование может дать представление о факторах, способствующих их широкому распространению.

Распространение фальшивых новостей в социальных сетях может иметь значительные последствия для кибербезопасности. Оно может привести к распространению вредоносных программ, фишинговых атак и краже личных данных, создавая риски для отдельных людей, организаций и даже национальной безопасности. Понимание этих последствий необходимо для разработки эффективных стратегий кибербезопасности.

Фальшивые новости способны формировать общественный дискурс, влиять на выборы и усугублять социальные разногласия. Изучая мотивы создания и распространения фальшивых новостей в социальных сетях, данное исследование может способствовать более глубокому пониманию их влияния на общество[1].

Онлайн-платформы должны брать на себя ответственность за предоставляемые ими информацию. Платформы социальных сетей играют решающую роль в борьбе с распространением фальшивых новостей. Анализ эффективности текущих технологических и политических мер, реализуемых этими платформами, может дать представление об их ответственности и необходимости совершенствования стратегий борьбы с фальшивыми новостями и защиты пользователей.

[1] Стратегия развития информационного общества Указ Президента Республики Узбекистан, от 05.10.2020 г. № УП-6079 https://lex.uz/docs/5031048?ONDATE2=02.04.2021&action=compare (дата обращения: 1.02.2023)

Также большую роль играет осведомленность и образование пользователей. Понимание поведения пользователей, когнитивных предубеждений и общественных факторов, связанных с потреблением и распространением фальшивых новостей, может помочь в разработке образовательных инициатив, способствующих развитию критического мышления, медиаграмотности и ответственного поведения в Интернете.

В целом, данная тема исследования является весьма актуальной, поскольку она затрагивает пересечение социальных сетей, фальшивых новостей и кибербезопасности, способствуя всестороннему пониманию проблем и возможностей в борьбе с распространением дезинформации и защите людей и общества от связанных с ней киберугроз.

Содержание

Киберпреступность относится к преступной деятельности, которая осуществляется с использованием Интернета или других электронных коммуникационных технологий. Эти преступления могут принимать различные формы, включая взлом, кражу личных данных, киберпреступление, фишинг и распространение вредоносного программного обеспечения.

Одной из наиболее серьезных угроз, создаваемых киберпреступностью, является кража личной информации, такой как номера кредитных карт, номера социального страхования и пароли. Киберпреступники могут использовать эту информацию для кражи денег, совершения мошенничества или даже продажи ее в темной сети.

Другой распространенной формой киберпреступности являются атаки программ-вымогателей. При атаке с помощью программы-вымогателя киберпреступник заражает компьютер жертвы вредоносным ПО, которое шифрует их файлы и требует оплаты в обмен на ключ дешифрования.

Другие формы киберпреступности включают взлом, когда преступник получает несанкционированный доступ к компьютерной системе или сети, и киберпреступление, когда человек подвергается преследованиям или угрозам онлайн.

По мере дальнейшего развития технологий угроза, создаваемая киберпреступностью, скорее всего, будет только расти. Правительства и правоохранительные органы по всему миру работают над борьбой с этой угрозой, но она остается серьезной проблемой для общества в целом.

Для борьбы с растущей угрозой киберпреступности правительство Узбекистана предприняло несколько шагов по улучшению кибербезопасности в стране. Например, в 2020 году Совет национальной безопасности Узбекистана утвердил новую стратегию кибербезопасности, направленную на укрепление обороноспособности страны от кибератак и повышение осведомленности общественности о рисках, связанных с использованием цифровых технологий.

Кроме того, правительство создало Центр кибербезопасности для координации усилий по обеспечению кибербезопасности различных правительственных учреждений и для работы с организациями частного сектора по защите критически важной инфраструктуры и данных.

Несмотря на эти усилия, киберпреступность остается серьезной проблемой в Узбекистане, и необходимо сделать больше для улучшения кибербезопасности и защиты отдельных лиц и организаций от киберугроз.

Некоторые из недавних инцидентов, связанных с киберпреступностью в Узбекистане, включают:

В 2020 году Министерство внутренних дел Узбекистана сообщило, что оно арестовало группу хакеров, которые совершили серию кибератак на различные государственные учреждения и предприятия Узбекистана.

В 2019 году была предпринята масштабная кибератака на официальный сайт правительства Узбекистана. Атака была приписана группе хакеров, базирующихся в Китае.

В 2018 году кибератака была направлена на веб-сайт Узбекской фондовой биржи. Атака привела к отключению веб-сайта на несколько часов и нарушила торговую активность.

Чтобы противостоять растущей угрозе киберпреступности, Узбекистан работает над совершенствованием своей правовой базы и возможностей правоохранительных органов. В 2019 году в стране был принят новый закон о кибербезопасности, который включает положения о защите критически важной инфраструктуры и судебном преследовании киберпреступников[2].

Правительство также работает над повышением осведомленности общественности о киберугрозах и проводит обучение отдельных лиц и организаций тому, как защитить себя от кибератак. Например, Министерство развития информационных технологий и коммуникаций запустило несколько инициатив по продвижению кибербезопасности, включая мобильное приложение, которое предоставляет пользователям советы о том, как оставаться в безопасности онлайн.

В целом, киберпреступность вызывает растущую озабоченность в Узбекистане, но правительство и другие заинтересованные стороны предпринимают шаги по улучшению кибербезопасности и защите цифровой инфраструктуры страны.

Киберпреступность в контексте социальных сетей является растущей проблемой во всем мире. Социальные сети стали неотъемлемой частью жизни многих людей, предоставляя платформу для общения, обмена информацией и ведения бизнеса. Однако эти сети также уязвимы для различных форм киберпреступности, включая:

1. Фишинг и кража личных данных: киберпреступники могут использовать социальные сети для создания поддельных профилей и получения личной информации, такой как пароли, номера кредитных карт и другие конфиденциальные данные.

2. Киберпреступление и домогательства: Социальные сети могут использоваться для преследования, запугивания или угроз отдельным лицам, что может привести к эмоциональному расстройству и проблемам с психическим здоровьем.

[2] Решетова В. А., Шарыпова Т. Н. Вопросы противодействия киберпреступности // Инновации. Наука. Образование. 2022. № 56. С. 60-64.

3. Вредоносные программы и вирусные атаки: Социальные сети могут использоваться для распространения вредоносных программ и вирусов, которые могут повредить компьютерные системы, украсть данные или поставить под угрозу безопасность[3].

4. Спам и фишинговые мошенничества: Социальные сети могут использоваться для распространения спам-сообщений и фишинговых афер, которые обманом заставляют пользователей предоставлять конфиденциальную информацию или загружать вредоносное программное обеспечение.

Далее рассмотрим каждый из вышеперечисленных видов киберпреступлений по отдельности.

Фишинг - это вид киберпреступности, при котором преступники используют электронную почту, мгновенные сообщения или другие формы коммуникации, чтобы обманом заставить людей выдать свою конфиденциальную информацию, такую как имена пользователей, пароли, номера кредитных карт или реквизиты банковского счета.

Фишинговые атаки обычно включают в себя создание поддельного веб-сайта или страницы входа в систему, которая спроектирована так, чтобы выглядеть как законный веб-сайт, такой как банк или сайт онлайн-покупок. Злоумышленник рассылает большое количество электронных писем или сообщений, которые кажутся с законного веб-сайта и содержат ссылку на поддельный веб-сайт.

Когда пользователь нажимает на ссылку и вводит свои учетные данные для входа или другую конфиденциальную информацию на поддельный веб-сайт, злоумышленник затем может использовать эту информацию для получения доступа к учетным записям пользователя, кражи его денег или совершения других видов мошенничества.

Фишинговые атаки часто бывают высоконаправленными и изощренными, когда злоумышленники используют тактику социальной инженерии, чтобы обманом вынудить пользователей предоставить свою информацию. Например, они могут создать ощущение срочности, заявив, что учетная запись пользователя была скомпрометирована и что требуются немедленные действия для предотвращения дальнейшего ущерба.

Чтобы защитить себя от фишинговых атак, важно проявлять бдительность и принимать меры для защиты личной информации. Некоторые советы включают в себя:

1. Быть осторожным с нежелательными электронными письмами или сообщениями, в которых вас просят перейти по ссылке или предоставить личную информацию.

2. Проверять URL любого веб-сайта, который просит вас ввести свои учетные данные для входа или другую конфиденциальную информацию, чтобы убедиться, что это законный сайт.

[3] Там же.

3. Устанавливать и использовать антифишинговое программное обеспечение, которое может помочь обнаруживать и предотвращать фишинговые атаки.

4. Использовать надежные, уникальные пароли для каждой из ваших учетных записей и по возможности включать двухфакторную аутентификацию.

5. Делиться с другими о рисках фишинга и о том, как его избежать.

Социальная инженерия - это тактика, которую киберпреступники используют, чтобы обманом заставить людей раскрыть конфиденциальную информацию или выполнить действия, которые они обычно не стали бы выполнять. Она включает в себя психологическую манипуляцию и опирается на естественную человеческую склонность доверять другим, быть полезным и следовать правилам и процедурам[4].

Существуют различные типы методов социальной инженерии, которые могут использовать киберпреступники, в том числе:

1. Фишинг: Как было описано ранее, фишинг - это форма социальной инженерии, которая использует электронную почту, текстовые сообщения или телефонные звонки, чтобы обманом заставить жертв предоставить конфиденциальную информацию, такую как пароли, номера кредитных карт или реквизиты банковского счета.

2. Травля: При использовании этого метода злоумышленник предлагает что-то заманчивое, например бесплатный подарок или рекламный товар, чтобы заставить жертв предоставить свою личную информацию.

3. Предлог: Предлог включает в себя создание ложного сценария или предлога, чтобы завоевать доверие жертвы и убедить ее разгласить свою конфиденциальную информацию. Например, злоумышленник может выдавать себя за авторитетное лицо или сотрудника доверенной компании, чтобы получить информацию.

4. Точечный фишинг: это целенаправленная форма фишинга, при которой личная информация используется для придания фишинговому сообщению более легитимного вида. Например, злоумышленник может указать в сообщении имя жертвы, должность или другую информацию.

5. Тайный ход: При этом методе злоумышленник следует за уполномоченным лицом в зону ограниченного доступа, выдавая себя за курьера, специалиста по ремонту или другого поставщика услуг, чтобы получить доступ в зону ограниченного доступа.

Чтобы предотвратить атаки социальной инженерии, важно быть осведомленным о методах, которые используют киберпреступники, и принимать меры для защиты вашей личной информации. Некоторые советы включают в себя:

1. Быть осторожным с незапрашиваемыми запросами о предоставлении личной информации, особенно если они исходят из неизвестного источника.

2. Подтверждать личность любого, кто запрашивает личную информацию, связавшись с ним напрямую или запросив его учетные данные.

3. Быть осторожным с любым сообщением, которое создает ощущение срочности или пытается посеять панику.

[4] Цифровая компетентность подростков и родителей (под ред. Г.У. Солдатовой, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова). 2013. М.: Фонд развития Интернет, 144 с.

4. Внедрение политики и процедуры безопасности, которые могут помочь защитить от атак социальной инженерии, например, требуйте от сотрудников использования надежных паролей, включите двухфакторную аутентификацию и проведите обучение по вопросам безопасности.

Киберзапугивание - это форма издевательств, которая осуществляется онлайн с использованием цифровых технологий, таких как социальные сети, текстовые сообщения, обмен мгновенными сообщениями и электронная почта. Это включает в себя использование технологий для преследования, смущения или запугивания кого-либо, часто неоднократно и в течение длительного периода.

Примеры киберзапугивания включают отправку сообщений с угрозами или оскорблениями, публикацию смущающих или уничижительных комментариев или изображений в социальных сетях, распространение слухов или лжи о ком-либо и выдачу себя за кого-то другого в Интернете. Киберзапугивание может вызвать у жертвы эмоциональный стресс, тревогу, депрессию и другие проблемы с психическим здоровьем[5].

Киберзапугивание может случиться с кем угодно, но дети и подростки особенно уязвимы. Анонимность и дистанция, обеспечиваемые цифровыми технологиями, могут облегчить хулиганам преследование своих жертв, не опасаясь последствий. Киберзапугивание может иметь серьезные и долговременные последствия, такие как социальная изоляция, трудности в учебе, членовредительство и даже самоубийство.

Чтобы предотвратить киберзапугивание, важно:

1. Рассказывать детям, подросткам и взрослым о последствиях киберзапугивания и важности уважения к другим людям в Интернете.

2. Поощрять жертв высказываться и обращаться за помощью к взрослым, которым они доверяют, таким как родители, учителя или консультанты.

3. Поощрять прохожих высказываться и сообщать о киберзапугивании, когда они становятся его свидетелями.

4. Учить детей и подростков быть ответственными и уважительными цифровыми гражданами и использовать технологии в позитивном ключе.

5. Внедрять политику и процедуры в школах, на рабочих местах и в других организациях для предотвращения киберзапугивания и борьбы с ним.

Кража личных данных - это вид киберпреступления, при котором личная и финансовая информация человека похищается злоумышленником, который затем использует эту информацию в мошеннических целях. Это может включать в себя кражу информации о кредитной карте или банковском счете жертвы, номера социального страхования и других конфиденциальных личных данных.

Злоумышленник может использовать эту украденную информацию для открытия новых учетных записей на имя жертвы, совершения мошеннических покупок и подачи заявок на получение займов или кредитных карт. Жертва может даже не подозревать о краже до тех пор, пока не получит счета за счета, которые она не открывала, или пока это не повлияет отрицательно на ее кредитный рейтинг.

[5] Giddens A. 1991. Modernity and Self-Identity. Self and Society in the Late Modern Age. Stanford University Press, 257 p.

Кража личных данных может происходить различными способами, включая фишинговые атаки, утечку данных и физическую кражу личной информации. Киберпреступники могут также использовать тактику социальной инженерии, чтобы обманом заставить жертв раскрыть свою личную информацию, например, выдавая себя за представителя законной компании или государственного учреждения.

Чтобы предотвратить кражу личных данных, важно принять меры для защиты личной и финансовой информации. Это может включать:

1. Использовать надежные и уникальные пароли для всех учетных записей и регулярно менять их.

2. Быть осторожным при разглашении личной информации, особенно по телефону или онлайн.

3. Поддерживать свой компьютер и мобильные устройства в актуальном состоянии с помощью новейшего программного обеспечения для обеспечения безопасности и исправлений.

4. Регулярно отслеживать свои банковские счета и счета по кредитным картам на предмет любых необычных действий.

5. Ежегодно проверять свой кредитный отчет на предмет любых подозрительных действий или ошибок[6].

Вредоносное ПО, сокращенно от вредоносного программного обеспечения, - это тип программного обеспечения, предназначенный для повреждения или сбоя в работе компьютерных систем, сетей и устройств. Вредоносные программы могут принимать различные формы, включая вирусы, червей, троянские программы, программы-вымогатели и шпионские программы.

Вредоносное ПО может распространяться различными способами, такими как вложения электронной почты, вредоносные веб-сайты, загрузки зараженного программного обеспечения и тактики социальной инженерии. Как только устройство заражено вредоносным ПО, оно может выполнять широкий спектр вредоносных действий, таких как:

1. Кража конфиденциальной информации, такой как пароли, номера кредитных карт и другие личные данные.

2. Захват устройства или сети и использование их для незаконных действий, таких как распределенные атаки типа "отказ в обслуживании" (DDoS).

3. Шифрование файлов и требование оплаты (часто в криптовалюте) в обмен на ключ расшифровки (известный как программа-вымогатель).

4. Нарушение или отключение нормальной работы устройства или сети, приводящее к сбоям системы или потере данных.

Чтобы предотвратить заражение вредоносными программами, важно принять несколько мер предосторожности, таких как:

1. Установка и регулярных обновлений антивирусного и вредоносного программного обеспечения.

[6] Barclay, Corlane. (2017). Cybercrime and legislation: a critical reflection on the Cybercrimes Act, 2015 of Jamaica. Commonwealth Law Bulletin, Vol. 43(1), 77-107.

2. Избегать перехода по ссылкам или загрузки вложений из неизвестных или подозрительных источников.

3. Поддерживать операционную систему и программное обеспечение в актуальном состоянии с помощью последних исправлений безопасности.

4. Быть осторожным при разглашении личной или финансовой информации онлайн.

5. Регулярно создавать резервные копии важных данных, чтобы предотвратить потерю данных в случае заражения вредоносным ПО.

Для решения растущей проблемы киберпреступности в социальных сетях были приняты различные меры на организационном, правительственном и индивидуальном уровнях. Сами социальные сети внедрили различные функции безопасности для защиты своих пользователей, такие как двухфакторная аутентификация, шифрование и контроль конфиденциальности. Правительства также приняли законы и подзаконные акты для борьбы с киберпреступностью в социальных сетях.

На индивидуальном уровне пользователи могут предпринять шаги для защиты от киберпреступности, такие как использование надежных паролей, отказ от перехода по подозрительным ссылкам или вложениям и осторожность при обмене личной информацией в Интернете.

В целом, киберпреступность в контексте социальных сетей - это сложная проблема, требующая многогранного подхода. Это предполагает сотрудничество между социальными сетями, правительствами и отдельными лицами для предотвращения киберпреступности в этом цифровом ландшафте и борьбы с ней[7].

В дополнение к мерам, принимаемым платформами социальных сетей для повышения кибербезопасности, правительства и правоохранительные органы также работают над борьбой с киберпреступностью в социальных сетях. Например, во многих странах приняты законы и подзаконные акты по борьбе с киберпреступностью, а правоохранительные органы создали специализированные подразделения для расследования и судебного преследования киберпреступников.

Однако задача борьбы с киберпреступностью в социальных сетях осложняется несколькими факторами. Во-первых, социальные сети глобальны по своей природе, а это означает, что киберпреступники могут действовать через границы, что затрудняет правоохранительным органам их выслеживание и привлечение к ответственности. Кроме того, огромный объем данных, генерируемых социальными сетями, может затруднить своевременное выявление киберугроз и реагирование на них

Для решения этих проблем правительствам, правоохранительным органам и платформам социальных сетей необходимо сотрудничать в целях повышения кибербезопасности и борьбы с киберпреступностью в социальных сетях. Это может включать обмен информацией и опытом, разработку новых технологий для

[7] Davies, Caroline. (2018). ‘Sadistic’ paedophile Matthew Falder jailed for 32 years. The Guardian, 19 February 2018. https://www.theguardian.com/technology/2018/feb/19/dark-web-paedophilematthew-falder-jailed-for-32-years. (дата обращения: 25.02.2023)

обнаружения и предотвращения киберугроз, а также информирование пользователей о рисках, связанных с использованием социальных сетей.

В конечном счете, ключом к борьбе с киберпреступностью в социальных сетях является многогранный подход, который включает в себя сочетание технических, юридических и образовательных мер[8].

References:

1. Алоева А. А., Алоев И. А., Жуков А. З. Информационный терроризм – угроза национальной безопасности в условиях цифровизации // 2020. Т. 13. № 6. С. 197-201.
2. Дерендяева Т. М., Мухина Г. А. Противодействие киберпреступности в аспекте обеспечения безопасности информационного общества. 2022. № 1 (67). С. 85-89.
3. Козячая А. В. Политический аспект киберпреступлений // В мире научных открытий. Материалы IV Международной студенческой научной конференции. Ульяновск, 2020. С. 39-42.
4. Крупенникова К. К. Формы проявления киберпреступности в современном мире // Эволюция государства и права: проблемы и перспективы: сборник научных трудов 3-й Международной научной конференции с включением материалов XI-ого круглого стола «Ценности и нормы правовой культуры в России». Курск, 2021. С. 221-225.
5. Парамонов А. В. Противодействие киберпреступности как деятельность по обеспечению национальной безопасности // Проблемы экономики и юридической практики. 2019. Т. 15. № 2. С. 244-247.
6. Решетова В. А., Шарыпова Т. Н. Вопросы противодействия киберпреступности // Инновации. Наука. Образование. 2022. № 56. С. 60-64.
7. Цифровая компетентность подростков и родителей (под ред. Г.У. Солдатовой, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова). 2013. М.: Фонд развития Интернет, 144 с

[8] Там же.