ВЛИЯНИЕ СОЦИАЛЬНЫХ СЕТЕЙ НА НАЦИОНАЛЬНУЮ БЕЗОПАСНОСТЬ

Вахобов Муродилла

Независимый искатель

Аннотация: *Появление социальных сетей произвело революцию в способах общения, взаимодействия и обмена информацией. Эти платформы дали возможность людям из разных слоев общества и географических регионов общаться, способствуя созданию глобальных сообществ и облегчая обмен идеями. Однако рост социальных сетей также породил множество угроз, которые ставят под угрозу нашу безопасность, ставя под угрозу наше личное и коллективное благополучие. Цель этой статьи — углубиться в бесчисленные опасности, которые социальные сети представляют для нашей безопасности, и изучить способы, которыми эти платформы могут быть использованы для причинения вреда отдельным лицам, сообществам и обществам.*

Ключевые слова: *Социальные сети онлайн, Конфиденциальность, Безопасность, Решения для социальных сетей, Угрозы*

THE IMPACT OF SOCIAL NETWORKS ON NATIONAL SECURITY

Vakhobov Murodilla

Independent Seeker

Abstract: *The advent of social media has revolutionized the way we communicate, interact, and share information. These platforms have enabled people from different backgrounds and geographic regions to connect, fostering global communities and facilitating the exchange of ideas. However, the rise of social media has also given rise to a host of threats that threaten our safety, jeopardizing our personal and collective well-*

being. The purpose of this article is to delve into the myriad dangers that social media poses to our safety and explore the ways in which these platforms can be used to harm individuals, communities, and societies.

Keywords: *Online Social Networking, Privacy, Security, Social Media Solutions, Threats*

IJTIMOIY TARMOQLARNING MILLIY XAVFSIZLIKKA TA'SIRI

Vahobov Murodilla

Mustaqil qidiruvchi

Anotatsiya: *Ijtimoiy tarmoqlarning paydo bo'lishi biz bilan muloqot qilish, o'zaro aloqa qilish va ma'lumot almashish usullarini inqilob qildi. Ushbu platformalar turli kelib chiqishi va geografik mintaqalaridagi odamlarga ulanish imkonini berdi, global hamjamiyatlarni yaratishga yordam berdi va fikr almashishni osonlashtirdi. Biroq, ijtimoiy tarmoqlarning o'sishi bizning xavfsizligimizga putur etkazadigan, shaxsiy va jamoaviy farovonligimizni xavf ostiga qo'yadigan ko'plab tahdidlarni ham keltirib chiqardi. Ushbu maqolaning maqsadi ijtimoiy tarmoqlar bizning xavfsizligimiz uchun xavf tug'diradigan ko'p sonli xavflarni o'rganish va ushbu platformalardan odamlarga, jamoalarga va jamiyatlarga zarar etkazish uchun foydalanish usullarini o'rganishdir.*

Kalit so'zlar*: Onlayn ijtimoiy tarmoqlar, Maxfiylik, Xavfsizlik, Ijtimoiy tarmoq echimlari, tahdidlar*

Введение: Повсеместное использование онлайн-социальных сетей и сайтов с пользовательским контентом делает их местом для множества угроз и атак, начиная от простых готовых угроз и вредоносного ПО до сложных постоянных угроз. В этой статье будет проиллюстрирован размах этих угроз путем обсуждения использования этих сайтов ботнетом. Мы также покажем, как эти угрозы разработаны, чтобы

сделать их очень сложными для обнаружения. Более того, мы рассмотрим, что можно сделать для защиты пользователей этих сайтов от угроз, с которыми можно столкнуться, и возможные контрмеры, которые можно предпринять. Появление Web 2.0 позволяет все большую долю наших взаимодействий осуществлять в Интернете. Мы используем веб-электронную почту, используем представления знаний и используем сайты социальных сетей для поддержания связи. Однако виртуальный мир — это не утопия. Нас преследуют угрозы, начиная от простого спама, фишинга и фишинга до все более сложных вредоносных программ, ботнетов и сложных постоянных угроз. Широкое использование этих сайтов делает социальные сети особенно привлекательным предложением для злоумышленников, которые видят в них площадку для этих угроз и атак. По этой причине мы хотели выяснить, насколько серьезны эти угрозы на самом деле, что можно сделать для защиты систем от обнаруженных угроз и предоставить некоторые контрмеры против различных атак, которые можно было бы предвидеть.

Предыстория и значение

Всемирная паутина безвозвратно изменила деятельность организаций, в которых мы работаем, и то, как мы взаимодействуем друг с другом. Web 2.0 значительно увеличила возможности людей сотрудничать посредством использования социальных сетей. Благодаря использованию сложных приложений теперь можно создавать сети контактов, включающие доверенных лиц, распределенных по всему миру, и обмениваться информацией и создавать сообщества, которые предоставляют интеллектуальный контент, оставаясь анонимными для других членов сообщества. Созданные динамические инструменты также произвели революцию в способности злоумышленников охотиться на ничего не подозревающих членов сообщества. Фишинг стал распространенным способом для преступников использовать неосторожных в этих сетях. Распространились слухи о преимуществах, доступных

злоумышленникам, и множество создателей вредоносного ПО сосредоточили свои таланты на использовании потенциальных жертв.

Доступность подробных публичных профилей для большой части населения открывает дверь потенциальному злоумышленнику, который хочет нацелиться на часть сообщества. Например, информация об организации, полученная путем проникновения в ее социальную сеть, может быть использована для планирования и осуществления физической атаки на организацию. Очевидно, что доступность проверенной информации о лицах, составляющих сообщество, открыла многие сложные проблемы обороны и военной разведки. Эти проблемы обороны коренятся в преобразовании традиционных проблем обороны, которые по сути были национальными по своему масштабу. Эти проблемы теперь больше не могут быть решены исключительно с помощью тщательно контролируемого и проверенного контента, поскольку все большая и большая часть знаний и навыков, необходимых для смягчения этих угроз, принадлежит членам общества в целом.

Литературный обзор.

Исследование угроз безопасности, связанных с социальными сетями, привлекло значительное внимание в последние годы, что отражает растущую обеспокоенность, связанную с конфиденциальностью и безопасностью пользователей в цифровую эпоху. Эчаиз и Рауль Арденги (2012) заложили основу для понимания многогранных рисков, с которыми пользователи сталкиваются на сайтах социальных сетей. Их исследование подчеркивает тревожную тенденцию пользователей раскрывать личную информацию, часто не осознавая потенциальных последствий. Авторы подчеркивают необходимость разработки лучших практик для смягчения этих рисков, особенно уделяя внимание поведению, связанному с конфиденциальностью, которое может привести к уязвимостям.

Опираясь на эту основу, Альдхаффери и др. (2013) дополнительно исследуют последствия настроек конфиденциальности в онлайн-социальных сетях, особенно для пользователей мобильного Интернета. Их выводы показывают тревожную неосведомленность пользователей о рисках конфиденциальности, что может привести к значительному неправомерному использованию личной информации. Авторы выступают за усиление контроля пользователей над настройками конфиденциальности, подчеркивая, что способность управлять собственной информацией имеет решающее значение для укрепления доверия и безопасности пользователей. Они подчеркивают риски, связанные с воздействием несовершеннолетних на незнакомцев в сети, демонстрируя потенциал кражи личных данных и эксплуатации.

В более всестороннем анализе Саридакис и др. (2015) изучают взаимосвязь между индивидуальной информационной безопасностью, поведением пользователя и явлением кибервиктимизации. Их эмпирическое исследование подчеркивает растущую распространенность финансового мошенничества, преследования и шантажа, предполагая, что ответственность за защиту личной информации часто непропорционально ложится на пользователей. Авторы утверждают, что негативные аспекты социальных сетей недостаточно изучены, устанавливая связь между высоким использованием социальных сетей и повышенными рисками онлайн-виктимизации. Это исследование привлекает внимание к необходимости более широкого понимания последствий взаимодействия с социальными сетями для личной безопасности.

Y Alqubaiti (2016) вносит свой вклад в этот дискурс, исследуя парадокс безопасности социальных сетей через призму восприятия и поведения студентов ИТ-специалистов. Представленная тревожная статистика относительно эскалации преступности, связанной с социальными сетями, включая кражу личных данных и киберпреследование, подчеркивает значительные угрозы безопасности, создаваемые

этими платформами. Автор отмечает тревожную тенденцию пользователей пренебрегать управлением настройками конфиденциальности, что усугубляет их уязвимость к онлайн-угрозам. Это исследование подтверждает идею о том, что, хотя социальные сети предлагают многочисленные преимущества, они одновременно представляют существенные риски, с которыми пользователи должны справляться.

Наконец, Кириченко и др. (2018) дают обзор методологий, используемых в анализе социальных сетей для обнаружения киберугроз. В их обзоре излагаются различные задачи безопасности, имеющие отношение к социальным сетям, включая обнаружение сообществ и идентификацию ключевых лиц в сетях. Авторы утверждают, что быстрое развитие социальных сетей требует разработки новых методов для решения проблемы растущей сложности и частоты кибератак, которые создают значительные проблемы для ИТ-отделов.

В совокупности эти статьи иллюстрируют настоятельную необходимость в более глубоком понимании угроз безопасности, исходящих от социальных сетей. Они подчеркивают важность осведомленности пользователей, проактивного управления конфиденциальностью и внедрения надежных мер безопасности для защиты личной информации в условиях все более взаимосвязанного мира.

Обсуждение.

Одной из самых коварных угроз нашей безопасности в социальных сетях является распространение кибербуллинга и онлайн-преследований. Платформы социальных сетей стали рассадником вредоносного поведения, а преступники используют эти каналы для запугивания, унижения и унижения своих жертв. Согласно отчету Pew Research Center, 59% подростков подвергались онлайн-преследованиям, причем 47% из них сообщили, что подвергались серьезным формам преследований, включая физические угрозы. Психологические последствия кибербуллинга могут быть

изнурительными, приводя к депрессии, тревожности и даже суицидальным наклонностям.

Кража личных данных и утечка данных

Социальные сети также стали благодатной почвой для воров личных данных и хакеров, которые используют эти платформы для кражи конфиденциальной информации и нарушения безопасности пользователей. Фишинговые мошенничества, поддельные профили и вредоносные ссылки — вот лишь некоторые из тактик, используемых этими злонамеренными субъектами для кражи персональных данных, включая учетные данные для входа, информацию о кредитных картах и номера социального страхования. Последствия кражи личных данных могут быть ужасными, жертвы часто сталкиваются с финансовым крахом, репутационным ущербом и эмоциональным стрессом.

Дезинформация и пропаганда

Социальные сети стали мощным инструментом распространения дезинформации и пропаганды, что может иметь далеко идущие последствия для нашей безопасности. Фейковые новостные статьи, сфальсифицированные изображения и пропагандистские видеоролики могут распространяться в социальных сетях со скоростью лесного пожара, отравляя информационную экосистему и подрывая наше доверие к институтам. Преднамеренное распространение ложной информации может использоваться для влияния на общественное мнение, влияния на выборы и даже подстрекательства к насилию. Например, распространение фейковых новостей о вакцинации способствовало снижению показателей вакцинации, что поставило под угрозу общественное здоровье.

Терроризм и радикализация

Социальные сети также использовались террористическими организациями для распространения идеологии, вербовки членов и координации атак. Использование социальных сетей террористическими группами, такими как ИГИЛ, позволило им вербовать тысячи бойцов по всему миру, увековечивая цикл насилия и терроризма. Кроме того, платформы социальных сетей использовались для распространения радикальных идеологий, таких как превосходство белой расы и антисемитизм, что может привести к насилию и терроризму.

Последствия для психического здоровья

Постоянное воздействие курируемого и манипулируемого контента в социальных сетях также может оказывать разрушительное воздействие на наше психическое здоровье, способствуя возникновению тревожности, депрессии и социальной изоляции. Давление, направленное на то, чтобы представить идеальную онлайн-персону, может привести к чувству неадекватности и низкой самооценке, в то время как постоянный поток информации может увековечить чувство FOMO (страх упустить что-то) и беспокойство.

Государственное вмешательство и слежка

Наконец, социальные сети стали каналом для государственного вмешательства и слежки, угрожая нашей безопасности и свободе. Сбор метаданных и конфиденциальной информации правительствами может использоваться для профилирования лиц, подавления инакомыслия и подрыва демократии. Разоблачения Эдварда Сноудена о программе массового наблюдения Агентства национальной безопасности PRISM выявили риски злоупотребления властью со стороны правительства и продемонстрировали, как платформы социальных сетей могут использоваться для слежки и контроля за гражданами.

Заключение.

В заключение следует сказать, что социальные сети представляют собой множество угроз нашей безопасности: от кибербуллинга и онлайн-преследований до кражи личных данных, дезинформации, терроризма и вмешательства правительства. Эти риски могут иметь далеко идущие последствия, подвергая риску наше личное и коллективное благополучие и подрывая наше доверие к институтам. Чтобы смягчить эти угрозы, нам необходимо разработать надежные меры безопасности, включая надежное регулирование, образование и кампании по повышению осведомленности. Более того, компании социальных сетей должны уделять первостепенное внимание безопасности пользователей, инвестировать в модерацию контента и разрабатывать алгоритмы, которые продвигают надежную и достоверную информацию. Только признавая риски и работая вместе, мы можем создать более безопасную и защищенную экосистему социальных сетей, которая повысит нашу безопасность и будет способствовать нашему общему благу.

Список литературы:

1. Li, Yan & Deng (2015) Li Y, Yan Q, Deng RH. Анализ утечки конфиденциальной информации в социальных сетях. Computers & Security. 2015;49:239–254. doi: 10.1016/j.cose.2014.10.012.
2. Malenkovich (2012) Malenkovich S. Kaspersky Academy: атаки с использованием клонов идентификации. 2012. [15 мая 2020 г.]. https://usa.kaspersky.com/blog/identity-clone-attacks/648/
3. Mehmood et al. (2020) Mehmood E, Abid A, Farooq MS, Nawaz NA. Учебная программа, преподавание и обучение, а также оценки для вводного курса программирования. IEEE Access. 2020;8:125961–125981. doi: 10.1109/ACCESS.2020.3008321.
4. Norton (0000) Norton Kid’s Safety. Наиболее распространенные угрозы, с которыми сталкиваются дети в Интернете, NortonLifeLock. [15 мая 2020 г.].

https://hk-en.norton.com/internetsecurity-kids-safety-the-most-common-threats-children-face-online.html

5. Peng, Choo & Ashman (2016) Peng J, Choo KKR, Ashman H. Профилирование пользователей при обнаружении вторжений: обзор. Журнал сетевых и компьютерных приложений. 2016;72:14–27. doi: 10.1016/j.jnca.2016.06.012.
6. Ramalingam & Chinnaiah (2018) Ramalingam D, Chinnaiah V. Методы обнаружения поддельных профилей в крупных социальных сетях: всесторонний обзор. Computers & Electrical Engineering. 2018;65:165–177. doi: 10.1016/j.compeleceng.2017.05.020.