1.3 ВЛИЯНИЕ СОЦИАЛЬНЫХ СЕТЕЙ НА КИБЕРПРЕСТУПНОСТЬ

Норкулова Гавхаршодбегим Алишер кизи

https://doi.org/10.5281/zenodo.8082066

ARTICLE INFO

Qabul qilindi: 20-June 2023 yil
Ma'qullandi: 23-June 2023 yil
Nashr qilindi: 26-June 2023 yil

KEY WORDS

Эволюция Интернета, наблюдаемая в течение последних нескольких лет, привела к росту сети социальных сетей. Фактом является то, что эти сети быстро меняют формы общения и взаимодействия между людьми по всему миру.

ABSTRACT

Социальные сети оказали значительное влияние на ситуацию с киберпреступностью. В то время как социальные сети предоставляют множество преимуществ, таких как объединение людей по всему миру, обмен информацией и развитие онлайн-сообществ, они также стали питательной средой для различных форм киберпреступности.

Социальные сети оказали значительное влияние на ситуацию с киберпреступностью. В то время как социальные сети предоставляют множество преимуществ, таких как объединение людей по всему миру, обмен информацией и развитие онлайн-сообществ, они также стали питательной средой для различных форм киберпреступности.

Эволюция Интернета, наблюдаемая в течение последних нескольких лет, привела к росту сети социальных сетей. Фактом является то, что эти сети быстро меняют формы общения и взаимодействия между людьми по всему миру. Все больше людей используют эти сети. Огромное количество пользователей социальных сетей является доказательством оперативного воздействия эволюции и появления этих сетей. И наоборот, каждая плодотворная деятельность имеет свой недостаток. Киберпреступность - одна из проблем, непосредственно связанных с социальными сетями. Киберпреступность относится к преступной деятельности, в соответствии с которой преступники используют компьютер в качестве инструмента, причины или цели преступления. Интернет также является важным путем к этому виду незаконной деятельности. Появление и развитие социальных сетей является основной причиной роста числа случаев киберпреступности, о которых сообщается каждый год. В этом документе основное внимание будет уделено влиянию социальных сетей на

киберпреступность.

Кража личных данных и неправильное использование являются значительным влиянием социальных сетей на кибернетику. Большинство платформ социальных сетей не уделяют особого внимания конфиденциальности пользователей. Кроме того, большинство платформ социальных сетей требуют, чтобы их пользователь ввел часть своей конфиденциальной информации для входа в систему. Значительное количество пользователей не знают о том, что информация может иметь отношение к киберпреступникам. Поэтому они охотно склонны входить. Поскольку большинство платформ не учитывают безопасность данных своего пользователя, информация остается доступной другим пользователям. Киберпреступник может легко получить доступ к этой информации о своей цели[1].

Киберпреступник может использовать эту информацию для осуществления другой преступной деятельности, такой как фишинг, для самостоятельного получения. Они также могут продавать или создавать новые личности для других преступников. Таким образом, другим преступникам легче совершать незаконную деятельность и скрываться от правоохранительных органов. По словам исследователя, с каждым годом наблюдается еще один рост числа случаев кражи личных данных и неправомерного использования. Социальные сети являются важной причиной этого роста.

Возможность отслеживать пользователей - еще один эффект социальных сетей на киберпреступность. Эволюция платформ социальных сетей привела к появлению функций, которые позволяют пользователям часто обновлять свой статус. Кроме того, большинство платформ просят пользователей добавить информацию о своем текущем и предыдущем проживании, а также о посещаемых школах. Пользователи также могут видеть и показывать свои эмоции на сообщениях других пользователей, независимо от знаний или дружбы. Если пользователь прикрепляет свое текущее местоположение и активность, любит и не любит, среди прочего, в своем статусе, киберпреступник может легко следить за ним. Кроме того, благодаря сообщениям пользователей, таким как фотографии, видео и контексты, а также эмоции, которые пользователь проявляет в постах других пользователей, компьютерные преступники могут легко собирать соответствующую информацию, анализировать ее и прогнозировать свои целевые следующие события. Используя эти прогнозы, преступники могут совершать другие более серьезные кибератаки. Они также могут продавать эту информацию другим преступникам. Таким образом, другие преступники могут угрожать безопасности либо пользователю, либо другим членам семьи и друзьям.

Кибертерроризм - еще одно серьезное влияние социальных сетей на киберпреступность. Социальные сети предназначены для объединения людей по всему миру. Тем не менее, социальные сети способствуют кибертерроризму. Террористы с помощью киберпреступников используют социальные сети для достижения нескольких целей, создают беспорядки единства, генерируют финансовый доход, приобретают новые личности и интеллектуальный анализ данных. Киберпреступники

[1] European Parliament, Citizens' Rights and Constitutional Affairs. (2016). Cyberbullying Among Young People. Directorate General For Internal Policies, Policy Department C (PE 571.367). http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf. (дата обращения: 25.02.2023)

создают новые учетные записи на платформах социальных сетей, таких как Facebook, используя поддельные удостоверения личности. Затем они отправляют запрос на добавление в друзья как можно большему количеству пользователей в области цели. Затем они могут использовать эти учетные записи для отправки графики и контекстов, которые могут вызвать панику и недоверие среди людей, тем самым отвлекая единство и способствуя террористическим атакам[2].

Кроме того, киберпреступники крадут личную информацию других пользователей социальных сетей и используют ее для создания новых личных данных для террористов. Они также используют свои компетенции по интеллектуальным данным для получения конфиденциальной информации, такой как информация о кредитных картах, и используют ее для подделки персонажей. Затем они могут использовать поддельные кредитные карты для совершения покупок и снятия наличных с банковских счетов других пользователей социальных сетей для финансирования терроризма.

Преследование имущества также является серьезной проблемой в социальных сетях, связанной с киберпреступностью. Социальные сети облегчают передачу вредоносных программ, таких как компьютерные вирусы и вредоносные программы, программы-вымогатели и другие. Киберпреступники создают такие программы и прикрепляют их к сообщениям и рекламе таким образом, что, если пользователь платформы социальных сетей нажимает, загружает или открывает ссылку с этими вредоносными файлами, его компьютер пострадает.

Преступники создают разные файлы с разными целями, саботажем, интеллектуальным анализом данных или финансовой выгодой. В большинстве случаев преступники используют программы-вымогатели для получения денежной выгоды. Вымогатели скрывает важную информацию от владельца компьютера. Поэтому владелец должен заплатить за расшифровку своих данных. С другой стороны, киберпреступники используют платформы социальных сетей для отправки вредоносного программного обеспечения, которое помогает им в интеллектуальном анализе данных и вандализме. Они используют программное обеспечение для взлома или взлома компьютеров своих целей.

Киберпреследование и клевета также являются киберпреступностью, которая тесно связана с социальными сетями. Люди рассматривают социальные сети как лучший способ высказать свое мнение. Тем не менее, киберпреступники воспринимают это как способ получения клеветнительного контента. В этом случае преступники используют клеветнические материалы для киберпреследия своих целей. Киберпреследование относится к использованию Интернета, социальных сетей в качестве средства отправки угрожающих материалов, чтобы напугать или преследовать получателя. Киберпреступники могут создавать клеветнические материалы для своей цели. Затем они могут связаться с целью, угрожая опубликовать этот контент на платформах социальных сетей. Здесь жертва вынуждена делать то, как

[2] Parkin, Simon. (2017). Keyboard warrior: the British hacker fighting for his life. The Guardian, 8 September 2017. https://www.theguardian.com/news/2017/sep/08/laurilove-british-hacker-anonymous-extradition-us.(дата обращения: 2.03.2023)

их инструктируют преступники. В основном эти преступники нацелены на авторитетных людей, таких как политики.

Угроза от использования сторонних приложений это влияние социальных сетей на киберпреступность, которая обычно затрагивает молодежь. В основном каждая платформа социальных сетей требует, чтобы их пользователи вводили свою личную информацию при входе в систему. Некоторые из этих платформ имеют безопасную конфиденциальность данных пользователей. Следовательно, злоумышленникам трудно получить доступ к этой информации. Киберпреступники используют сторонние приложения для доступа к необходимой им информации. Сторонние приложения могут включать в себя, среди прочего, игры, музыкальные приложения. Они запрашивают разрешение на доступ к данным пользователей с платформ социальных сетей. Некоторые из этих приложений могут загружать вредоносное ПО. Таким образом, киберпреступники могут использовать это вредоносное ПО для кражи соответствующей информации, необходимой им, когда пользователь предоставляет разрешение.

Нарушение конфиденциальности также влияет на киберпреступность. Большинство платформ социальных сетей предоставляют своим пользователям привилегию выбирать уровень конфиденциальности своей личной информации. Когда пользователь устанавливает настройку по умолчанию общедоступной, информация остается доступной для всех. Таким образом, преступникам легко получить доступ к этой информации[3].

Доверие пользователей к операторам сайтов социальных сетей и незнакомцам оказывает сильное влияние социальных сетей на киберпреступность. Личная информация и контент, публикуемый пользователем в социальных сетях, обычно доступны операторам. Ген может быть доступен операторам даже после удаления. Некоторые из этих операторов не заслуживают доверия. Они могут злоупотреблять или обмениваться данными пользователей. Некоторые пользователи также быстро доверяют незнакомцам. Принятие запроса на добавление в друзья от неизвестных людей подвергает пользователя киберпреступности,

В заключение, социальные сети являются основной причиной широко распространенной киберпреступности. Он переходит на золотой рудник киберпреступников. Это не только сайт интеллектуального анализа данных, но и рыночный сайт, где преступники незаконно обмениваются информацией. Уязвимость социальных сетей в аспекте безопасности и недостаточный уровень правосознания пользователей делают его более благоприятным для киберпреступности.

Список использованной литературы:

1. WIPO. What is Intellectual Property.
2. Закон о неправомерном использовании компьютерных технологий и киберпреступлениях 2018 года (Кения)
3. Конвенция о киберпреступности 2001 года (Совет Европы)
4. Закон о киберпреступлениях 2015 года (Ямайка)

[3] United Nations Commission on Crime Prevention and Criminal Justice. (2017). Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity. United Nations Economic and Social Council (2 April 2017). https://documents-ddsny.un.org/doc/UNDOC/GEN/V07/820/33/PDF/V0782033.pdf?OpenElement. (дата обращения: 2.03.2023)

5. Закон о предупреждении киберпреступности 2012 года (Республиканский закон №.10175; RA10175) (Флиппины)
6. ВОИС, Соглашение по торговым аспектам прав интеллектуальной собственности 1994 года 3.21. International Telecommunication Union (ITU). (2012). Understanding cybercrime: Phenomena, challenges and legal response (pp. 11-33).
7. D.S. (2017) 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing', pp. 1075-1096 in R. Brownsword, E. Scotford and K. Yeung (eds) The Oxford Handbook of the Law and Regulation of Technology, Oxford: Oxford University Press.
8. Schjølberg, Stein (Judge) and Amanda M. Hubbard. (2005). Harmonizing National Legal Approaches on Cybercrime. WSIS Thematic Meeting on Cybersecurity, ITU.