УДК 004.896

АНАЛИЗ ОБМЕНА ИНФОРМАЦИЕЙ В СОЦИАЛЬНЫХ СЕТЯХ С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ

Гасанова Гулумназ Заур кызы
hesenovagulumnaz02@gmail.com
Магистрант 1-го курса по специальности «Кибербезопасности» Сумгаитский государственный университет, г.Сумгаит, Республика Азербайджан
Научный руководитель – к.т.н.,доцент **Ахмедова С.М.**

Социальные сети — это совокупность электронных коммуникационных платформ, которые пользователи используют для создания онлайн-сообществ. Через эти платформы пользователи обмениваются информацией, идеями и личными сообщениями. Социальные сети предоставляют публичный доступ к информации профилей пользователей и информации, которой они делятся. Однако эта открытая среда может привести к раскрытию профилей пользователей или их захвату хакерами. В настоящее время большинство пользователей социальных сетей привыкли делиться своими мыслями, чувствами и переживаниями с широким кругом друзей с помощью видео и фотографий. При обмене информацией в Интернете отдельные лица могут не учитывать риски безопасности, связанные с такой деятельностью. Однако этот шаг может привести к раскрытию большего объема личной информации неизвестным лицам, чем ожидалось. Сотрудникам следует быть более осторожными с тем, чем они делятся в социальных сетях, поскольку в наше

время растет число случаев мошенничества с использованием социальной инженерии. Эта информация может быть использована против них и компании, в которой они работают, а также может быть объединена с другой личной информацией, собранной киберпреступниками посредством других утечек данных потребителей [1].

Когда пользователи раскрывают на платформах социальных сетей информацию, которую они считают менее конфиденциальной, это также может привести к нарушению конфиденциальности. Однако осведомленность пользователей в этой области все еще недостаточно развита. Например, предоставление информации о текущем местоположении пользователя через GPS может послужить ворам сигналом к атаке на дом или квартиру этого человека. Другим примером является раскрытие информации о семейных отношениях в социальных сетях, что может создать проблемы с конфиденциальностью, такие как преследование, клевета и киберугрозы в адрес членов семьи. Более высокий уровень осведомленности о конфиденциальности обеспечит более надежную информационную безопасность. Однако большинство пользователей социальных сетей сталкиваются с этими угрозами только в реальной жизни и поэтому не осознают опасности и уязвимости платформ социальных сетей [3].

В ходе опроса большинство участников старшего и младшего возраста признались, что они делятся большим количеством личной информации, такой как номера телефонов и адреса, в социальных сетях; Опасность такого поведения заключается в том, что большинство из них не проверяют настройки конфиденциальности своих аккаунтов в социальных сетях. В

другом исследовании большинство студентов бакалавриата сообщили, что используют платформы социальных сетей для общения с семьей и друзьями, завязывания и поддержания отношений, проведения времени, развлечения и самовыражения. Исследование показало, что наибольшему риску подвержены студенты в возрасте от 18 до 30 лет. Основной причиной этого является активное использование Интернета и социальных сетей. В целом, использование социальных сетей снижается с возрастом, но по мере роста уровня дохода и образования использование социальных сетей увеличивается [1].

Развитие киберпреступности берет свое начало в конце 1970-х годов в сфере информационных технологий (ИТ). Киберпреступность, которая в то время заключалась только в рассылке спама, сегодня приобрела более сложные формы, такие как вирусы и вредоносное ПО. Термин «киберпреступность» охватывает широкий спектр противоправных действий, осуществляемых киберпреступниками с помощью любого электронного устройства, подключенного к Интернету. По словам экспертов, киберпреступники, несмотря на высокий уровень знаний о принципах работы и уязвимостях технологий, часто выбирают легкие цели, которые оказывают наименьшее сопротивление. Причина этого в том, что, воздействуя на таких пользователей, они могут легко инициировать хакерскую деятельность, прилагая меньше усилий [4].

Доверчивые пользователи часто становятся мишенью хакеров, и киберпреступники прибегают к креативным и разнообразным способам сбора их личной информации. Интернет стал неотъемлемой частью общества и превратился в основное средство общения и обмена информацией в современную эпоху. Это сделало Интернет мишенью для различных киберугроз [2].

Список использованных источников

1. Lana Kemal A., Rasber Dhahir R. 'Advanced security: The application social media and their security', (2024).

2. Etuh, E., Bakpo, F. S., and Agozie, H. E. 'Social Media Network Attacks and Their Preventive Mechanisms: A Review', Science Direct, səh. 140,14 (2022).

3. Shevchuk, R. and Pastukh, Y. 'Improving the security of social media accounts', Journal Title in Italics, səh. (Issue), 5 (2019).

4. Thuraisingham, B. 'The Role of Artificial Intelligence and Cyber Security for Social Media', Science Direct,səh. issues, 3 (2020).