новление метрик взаимодействия пользователей с контентом. Применение стратегий шардирования и репликации позволяет достичь отказоустойчивости и гибкости системы при росте нагрузки, а использование кэширования существенно снижает задержку при формировании ленты. Рассмотренные алгоритмы ранжирования и рекомендательные подходы обеспечивают персонализацию контента с учётом социальных связей, истории взаимодействий и временных факторов. Полученные результаты подтверждают, что предложенная архитектура соответствует требованиям современных информационных платформ и может быть использована в качестве практической основы для построения высоконагруженных систем формирования новостных лент.

Список литературы

1. Kreps J., Narkhede N., Rao J. Kafka: A distributed messaging system for log processing, 2011.

2. Singh I., Vivek C. Real-time event joining in practice with Kafka and Flink // arXiv preprint arXiv:2410.15533, 2024.

3. Carbone P., Katsifodimos A. et al. Apache Flink: stream and batch processing in a single engine // Bulletin of the IEEE Computer Society Technical Committee on Data Engineering, 2015.

4. Алексеева К. А. Применение паттерна FAN-OUT для обновления лент в высоконагруженных веб-приложениях: выпускная квалификационная работа. Минск: БГУИР, 2025.

5. Davoudian A., Chen C., Liu M. A survey on NoSQL stores // ACM Computing Surveys (CSUR), 2018.

6. Megiddo N., Modha D.S. ARC: A self-tuning, low overhead replacement cache // Proceedings of the 2nd USENIX Symposium on File and Storage Technologies (FAST), 2003.

7. Ульянов М. В. Приближённые ближайшие соседи Москва, 2015.

8. Bailis P., Venkataraman S., Franklin M.J., et al. Probabilistically Bounded Staleness for Practical Partial Quorums, 2012.

ОБЗОР МЕТОДОВ ОЦЕНКИ ИНВЕСТИЦИЙ В КИБЕРБЕЗОПАСНОСТИ. ПРОЦЕСС УПРАВЛЕНИЯ РИСКАМИ

Романюк М. А., Мозговенко А.А.

ФГБОУ ВО «Мелитопольский государственный университет», Мелитополь, e-mail: ya@amozgovenko.ru

Задачи исследования:

1. Систематизировать основные виды угроз, связанных с распространением сообщений в социальных сетях.

2. Оценить масштаб и последствия угроз для отдельных пользователей и социума.

Материалы и методы исследования

Современные исследования в области цифровой безопасности выделяют несколько ключевых направлений анализа угроз в социальных сетях:

1. Киберпреступность и мошенничество. Работы последних лет (2022–2025 гг.) акцентируют внимание на эволюции фишинговых атак и методах социальной инженерии. Отмечается рост использования deepfake – технологий для создания поддельных сообщений и имитации доверенных источников.

2. Дезинформация и манипулирование. Исследования в области медиапсихологии и политической коммуникации фиксируют усиление роли соцсетей как каналов распространения фейков и пропаганды. Особое внимание уделяется алгоритмическому усилению дезинформации и её влиянию на общественное мнение.

3. Психологические угрозы. Публикации по киберпсихологии описывают рост случаев кибербуллинга, сталкинга и онлайн харассмента. Анализируются долгосрочные последствия для психического здоровья жертв, включая тревожные расстройства и суицидальные мысли.

4. Утечка данных и приватность. Исследования в сфере информационной безопасности демонстрируют, что сообщения в соцсетях часто становятся источником компрометации персональных данных через:

– скрапинг информации;

– анализ метаданных;

– эксплуатацию уязвимостей платформ.

5. Экстремистские угрозы. Работы по криминологии и противодействию терроризму отмечают использование соцсетей для вербовки и координации противоправной деятельности. Активно изучаются методы выявления и блокировки экстремистского контента.

Основная цель – создать типологию угроз, порождаемых сообщениями в социальных сетях.

Результаты исследования и их обсуждение

С увеличением использования социальных сетей многие пользователи стали уязвимыми к угрозам своей приватности и безопасности. Эти опасности могут быть разделены на 4 главные категории (рис. 1.1). Первая категория содержит классические угрозы, в частности, угрозы конфиденциальности и безопасности, которые не только угрожают пользователям соцсетей, но и пользователям Интернета, не использующим социальные сети. Вторая категория охватывает современные угрозы, то есть угрозы, в основном уникальные для среды социальных сетей, и которые используют инфраструктуру социальных сетей для угрозы конфиденциальности и безопасности пользователя. Третья категория состоит из комбинированных угроз, где мы описываем, как сегодняшние нападающие могут, и часто делают, совмещать разные типы атак для создания более сложных и летальных приступов. Четвертая и последняя категория включает в себя угрозы, специально ориентированные на детей, использующих социальные сети.

Классические угрозы, такие как вредоносное ПО, фишинг, спам и межсайтовый скриптинг (XSS), остаются актуальными в эпоху социальных сетей. Они быстро распространяются среди пользователей, используя их личные данные и доверие.

Вредоносное ПО, как Koobface, заражает компьютеры пользователей социальных сетей и создает бот-сети. Фишинговые атаки, например в Facebook(соцсеть признана экстремистской и запрещенной на территории России, заблокирована РКН), обманывают пользователей, заставляя их раскрывать конфиденциальную информацию. Спамеры используют фальшивые профили для распространения рекламы. XSS-атаки, такие как червь Mikeyy, распространяются через уязвимости в соцсетях.

Интернет-мошенники, используя соцсети, получают доверие жертв и крадут их данные. Например, в 2010 году мошенники взломали аккаунт Эбигейл Пикетт в Facebook (соцсеть признана экстремистской и запрещенной на территории России, заблокирована РКН), чтобы выманить деньги у ее друзей.

Современные угрозы часто нацелены на личную информацию пользователей и их друзей. Злоумышленники могут создавать поддельные профили, собирать данные через друзей или использовать атаки вывода для получения конфиденциальных сведений.

Примеры угроз

1. Clickjacking – обман, заставляющий пользователей нажимать не то, что они хотели.

2. Деанонимизация – раскрытие настоящей личности через файлы cookie, группы и топологию сети.

3. Распознавание лица – создание биометрической базы данных из публичных фото.

4. Поддельные профили – автоматизированные аккаунты для сбора личных данных.

5. Атаки клонирования личности – дублирование профиля для обмана друзей и сбора информации.

6. Атаки вывода – анализ общедоступных данных для получения скрытой информации.

7. Утечка локации – обмен данными о местонахождении через соцсети.

8. Socware – вредоносные сообщения и приложения, маскирующиеся под друзей.

Дети, как малые, так и подростки, подвергаются угрозам в социальных сетях, включая онлайн-хищников, рискованное поведение и кибербуллинг.

Онлайн-хищники: Педофилы в интернете могут использовать детей для производства и распространения детской порнографии, а также для онлайн- или оффлайн-эксплуатации. Исследования показывают, что контент, контакты с взрослыми и рискованное поведение детей могут привести к серьезным последствиям.

Рисковое поведение: Прямое общение с незнакомцами, интимные разговоры, предоставление личной информации и фотографий – все это увеличивает риск для детей. Комбинация этих действий может быть особенно опасной.

Кибербуллинг: Издевательства в интернете через электронные письма, чаты и соцсети, включающие публикацию оскорбительных материалов и угроз, особенно сильно влияют на детей. Опрос показал, что 12% родителей сталкивались с кибербуллингом своих детей, чаще всего на платформах вроде Facebook (соцсеть признана экстремистской и запрещенной на территории России, заблокирована РКН).

Радикализация: Террористические организации, такие как ИГИЛ, используют соцсети для вербовки и распространения информации о своих планах. Борьба с такими угрозами требует обнаружения и пресечения распространения вредоносных сообщений.

Заключение

Сообщения в социальных сетях выступают катализатором многообразных угроз: от индивидуального мошенничества до масштабных информационных кампаний. Их объединяет высокий уровень маскировки под легитимный контент.

Ключевые угрозы:

– фишинг и социальная инженерия (поддельные ссылки, имитация доверенных лиц);

– дезинформация (фейки, манипулятивные нарративы);

– кибербуллинг (травля, доксинг);

– утечка данных (скрапинг, анализ цепочек сообщений);

– экстремистская агитация (вербовка, координация незаконных действий).

Список литературы

1. Kotenko I., Vitkova L., Saenko I., Tushkanova O., Branitskiy A. The intelligent system for detection and counteraction of malicious and inappropriate information on the Internet // AI Communication. 2020. Vol. 33. № 1. P. 13-25. DOI: 10.3233/aic-200647.

2. Vitkova L., Kotenko I., Kolomeets M., Tushkanova O., Chechulin A. Hybrid Approach for Bots Detection in Social Networks Based on Topological, Textual and Statistical Features // Proceedings of the Fourth International Scientific Conference Intelligent Information Technologies for Industry. Springer. 2020. Vol. 1156. P. 412- 421. DOI: 10.1007/978-3-030-50097-9_42.

3. Liu L., Peng, T. Clustering-based method for positive and unlabeled text categorization enhanced by improved TFIDF // Journal of Information Science and Engineering. 2014. Vol. 30. P. 1463-1481.

4. Li X.L., Liu B., Ng S. K. Negative training data can be harmful to text classification // Proceedings of the 2010 conference on empirical methods in natural language processing. Association for Computational Linguistics. 2010. P. 218-228.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ИДЕНТИФИКАЦИИ ОБЪЕКТОВ ВОЗДУШНОГО ПРОСТРАНСТВА

Рукас М. К., Букреев Д. А.

ФГБОУ ВО «Мелитопольский государственный университет», Мелитополь, e-mail: dmitriy.bukreev@mel-su.ru

Научный руководитель: Букреев Д. А.

Введение

Современное воздушное пространство характеризуется высокой динамичностью, ростом плотности воздушного движения и быстрым