УДК 004.056.5:004.9:004.738.5

ПРОГНОЗУВАННЯ КІБЕРЗАГРОЗ ЧЕРЕЗ АНАЛІЗ “ЕМОЦІЙНИХ ПАТЕРНІВ” СОЦІАЛЬНИХ МЕРЕЖ

Полотай О.І.
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі розглянуто підхід до прогнозування кіберзагроз на основі аналізу емоційних патернів, що формуються у соціальних мережах під впливом суспільних подій та інформаційних хвиль. Показано, що різкі зміни емоційного фону, зокрема зростання негативу, паніки чи агресії, можуть передувати масштабним фішинговим, DDoS-атакам або інформаційним операціям.*

Ключові слова*: емоційні патерни; соціальні мережі; кіберзагрози; прогнозування; інформаційна безпека; машинне навчання; аналіз тональності; поведінкова аналітика; аномалії; кіберстійкість.*

Вступ. У сучасному цифровому середовищі соціальні мережі формують великий масив непрямої інформації, що відображає суспільні настрої, реакції на події, конфлікти та інформаційні коливання. Ці дані можуть бути не лише індикатором соціальної активності, але й потужним інструментом прогнозування кіберзагроз. Емоційні патерни – тобто зміни емоційного забарвлення контенту, реакцій, коментарів та поведінки користувачів – часто передують активізації кібератак, кампаній дезінформації та хвиль фішингових дій. Вивчення таких патернів дозволяє створити новий підхід до раннього попередження про можливі інциденти, особливо в умовах гібридних загроз.

Основні частина. Емоційний фон у соціальних мережах змінюється під впливом політичних криз, економічних новин, техногенних подій чи інформаційних кампаній. Для кіберзахисту важливо те, що різке зростання емоційної напруженості, агресивних повідомлень або одноманітності реакцій часто корелює з підготовкою цілеспрямованих цифрових атак. Наприклад:

- перед масовими DDoS-атаками спостерігається різкий сплеск токсичності в публічних коментарях;
- перед фішинговими розсилками – активне обговорення певної теми, яку зловмисники збираються використати як приманку;
- перед кібератаками на державні органи – збільшення кількості негативних емоційних хвиль у згадках про ці органи..

Для формування системи прогнозування необхідно аналізувати:

- семантику текстів (ключові слова, контекст, настрій);
- тональність (рівень негативу, агресії, паніки, ентузіазму);
- динаміку реакцій (раптові піки лайків, репостів, згадок);
- ритм комунікацій (частота постів у короткі проміжки часу);
- емоційні кластери (групи повідомлень з однотипним настроєм).

Дослідження показують, що інформаційні операції часто використовують три стадії:

1. Підготовка емоційного фону – невеликі вкиди інформації створюють напруження.

2. Ескалація емоцій – масові обговорення підсилюють увагу до теми.

3. Кіберудар – використання створеного емоційного стану для маскування атаки або підвищення її ефективності.

На основі аналізу емоційних патернів можна створити:

Модель короткострокового прогнозування (1–3 дні) – реагує на раптові зміни в негативі, сплески агресії чи масові обговорення новин.

Модель середньострокового прогнозування (1–2 тижні) – виявляє поступову ескалацію напруги та формування «інформаційних хвиль».

Модель подієвого прогнозування – передбачає кібератаку під час значимих подій (вибори, свята, кризи), якщо спостерігається аномальна концентрація емоційних реакцій.

Такі моделі можуть інтегруватися у SOC або системи моніторингу ризиків.

Підприємства та державні структури можуть використовувати аналіз емоційних патернів для:

- підсилення кіберстійкості перед кризами;
- передбачення хвиль фішингу, пов'язаних з резонансними новинами;
- ідентифікації інформаційних операцій, що супроводжують кібератаки;
- виявлення цілеспрямованої дискредитації, яка є частиною гібридних дій;
- коригування кіберзахисних сценаріїв відповідно до суспільних настроїв.

Інтеграція таких підходів у системи безпеки дозволяє не лише реагувати на інциденти, а й передбачати їх до фактичного прояву.

В якості прикладу можна навести таку ситуацію: під час загострення політичної ситуації в країні одна з великих фінансових установ помічає різке збільшення кількості негативних і панічних згадок у соціальних мережах. У короткий період стрімко зростає емоційна напруженість: користувачі поширюють повідомлення про нібито "масове блокування карток", активно коментують чутки про можливі технічні збої й висловлюють недовіру до банківської системи. Алгоритми аналізу емоційних патернів фіксують аномальну концентрацію негативного контенту, а тематика цих повідомлень збігається з популярними методами фішингових атак. Система попередження ризиків формує прогноз про ймовірну хвилю шахрайських розсилок, спрямованих на клієнтів та співробітників підприємства.

За кілька годин після піку емоційної хвилі зловмисники дійсно запускають масштабну фішингову кампанію, маскуючи свої повідомлення під офіційні попередження банку. Користувачі, які вже перебувають у стані підвищеної тривожності та очікують проблем, значно частіше переходять за шкідливими посиланнями, що збільшує ефективність атаки. Завдяки ранньому аналі-

зу емоційного фону організація отримує змогу швидко попередити клієнтів, посилити моніторинг транзакцій і внести корективи у політику кіберзахисту до того, як атака набула критичного масштабу. Такий приклад демонструє, як вчасне виявлення деструктивних емоційних патернів може стати дієвим інструментом прогнозування кіберзагроз.

Висновки. Аналіз емоційних патернів соціальних мереж відкриває новий напрям у прогнозуванні кіберзагроз. Емоційні хвилі часто передують активним фазам цифрових атак, а їх раннє виявлення дозволяє підприємствам і державним структурам підготуватися до можливих інцидентів. Застосування машинного навчання та моніторингу соціальних платформ дає можливість формувати динамічні моделі ризику, що відображають реальний емоційний стан суспільства. Це підвищує ефективність кіберзахисту, забезпечує перевагу у часі та зменшує ймовірність успішної реалізації атак.

Література

1. Полотай О.І., Кухарська Н.П. Прогнозування індексу захищеності комп'ютерних мереж за допомогою економетричних моделей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. Том 4 № 28: С. 365-374.

2. Сус В. Аналіз моделі прогнозування кіберзагроз "Cyber Kill Chain". Modeling, Control and Information Technologies: Proceedings of International Scientific and Practical Conference, (7), 2025, С. 210–211.

3. Яковів І. Модель чотирьох інформаційних середовищ кібератаки. Information Technology and Security. July-December 2023. Vol. 11. Iss. 2 (21). С.175-192.