УДК 330.47:343.45:004.8

5.2.2. Математические, статистические и инструментальные методы в экономике

МАТЕМАТИЧЕСКИЕ И ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ МОДЕЛИРОВАНИЯ ЭКОНОМИЧЕСКОГО УЩЕРБА ОТ ПРЕСТУПЛЕНИЙ, ПОСЯГАЮЩИХ НА ТАЙНУ ЧАСТНОЙ ЖИЗНИ, СОВЕРШАЕМЫМ В СОЦИАЛЬНЫХ СЕТЯХ

Власенко Александра Владимировна
кандидат технических наук, доцент, Врио заведующего кафедрой информационной безопасности
e-mail: alex_vlasenko@List.ru
Краснодарский университет МВД России, Краснодар, Россия

Куминов Михаил Владимирович
подполковник полиции, старший преподаватель кафедры информационной безопасности
e-mail: kumchik@bk.ru
Краснодарский университет МВД России, Краснодар, Россия

Ларина Алевтина Юрьевна
капитан полиции, преподаватель кафедры информационной безопасности
e-mail: alevtinochka26@mail.ru
Краснодарский университет МВД России, Краснодар, Россия

В статье рассматривается проблема противодействия преступлениям, посягающим на тайну частной жизни в социальных сетях, с позиции специальности 5.2.2. Авторы отходят от чисто юридического анализа в сторону математического и инструментального моделирования процессов распространения конфиденциальной информации. Предложена математическая модель оценки социально-экономического ущерба от деструктивного информационного воздействия, основанная на теории графов и вероятностных методах. Разработан алгоритм идентификации аномальной активности в социальных медиа, позволяющий автоматизировать процесс выявления признаков подготовки к совершению преступлений, предусмотренных ст. 137 УК РФ. В работе использованы методы системного анализа и статистической обработки данных. Результаты исследования могут быть внедрены в аналитические модули систем мониторинга информационной безопасности

UDC 330.47:343.45:004.8

5.2.2. Mathematical, statistical and instrumental methods in economics

MATHEMATICAL AND INSTRUMENTAL METHODS FOR MODELING ECONOMIC DAMAGE CAUSED BY CRIMES INFRINGING ON PRIVACY COMMITTED ON SOCIAL NETWORKS

Vlasenko Alexandra Vladimirovna
Candidate of Technical Sciences, Associate Professor, Acting Head of the Department of Information Security
e-mail: alex_vlasenko@List.ru
Krasnodar University of the Ministry of Internal Affairs of Russia, Krasnodar, Russia

Kuminov Mikhail Vladimirovich
Police Lieutenant Colonel, Senior Lecturer at the Department of Information Security
e-mail: kumchik@bk.ru
Krasnodar University of the Ministry of Internal Affairs of Russia, Krasnodar, Russia

Larina Alevtina Yurievna
police captain, lecturer at the Department of Information Security
e-mail: alevtinochka26@mail.ru
Krasnodar University of the Ministry of Internal Affairs of Russia, Krasnodar, Russia

The article examines the problem of countering crimes that infringe on privacy in social networks from the perspective of specialty 5.2.2. The authors move away from purely legal analysis towards mathematical and instrumental modeling of the processes of confidential information dissemination. A mathematical model for assessing socio-economic damage from destructive information effects based on graph theory and probabilistic methods is proposed. An algorithm for identifying abnormal activity in social media has been developed, which makes it possible to automate the process of identifying signs of preparation for the commission of crimes provided for in Article 137 of the Criminal Code of the Russian Federation. Methods of system analysis and statistical data processing are used in the work. The results of the study can be integrated into the analytical modules of information security monitoring systems

Ключевые слова: ТАЙНА ЧАСТНОЙ ЖИЗНИ, СОЦИАЛЬНЫЕ СЕТИ, МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ В ЭКОНОМИКЕ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЙ УЩЕРБ, КИБЕРПРЕСТУПНОСТЬ

Keywords: PRIVACY, SOCIAL NETWORKS, MATHEMATICAL MODELING, INSTRUMENTAL METHODS IN ECONOMICS, INFORMATION SECURITY, SOCIO-ECONOMIC DAMAGE, CYBERCRIME

http://dx.doi.org/10.21515/1990-4665-215-016

Введение

Цифровая трансформация общества привела к перемещению значительной части социальных взаимодействий в виртуальное пространство социальных сетей. Однако, наряду с коммуникативными преимуществами, данная среда стала плацдармом для совершения преступлений, посягающих на конституционные права граждан, в частности — на тайну частной жизни. Актуальность темы исследования обусловлена не только ростом числа правонарушений по ст. 137 УК РФ, но и качественным изменением ущерба, который приобретает выраженный социально-экономический характер в условиях экономики знаний.

Традиционные криминологические подходы зачастую оказываются недостаточно эффективными для оперативного мониторинга высокоскоростных потоков данных. В этой связи возникает необходимость применения инструментальных методов экономики и математического моделирования для формализации процессов выявления и предотвращения угроз приватности. В рамках специальности 5.2.2 акцент смещается на разработку математического аппарата, позволяющего количественно оценить риски и оптимизировать распределение ресурсов правоохранительных органов при противодействии данным преступлениям.

Материалы и методы

Методологическую основу исследования составили методы системного анализа, математической статистики и теории информации. Для построения модели распространения конфиденциальных данных в социальных сетях использовался аппарат теории случайных графов (модель Эрдёша — Реньи) и эпидемиологические модели распространения информации (SIR-моделирование применительно к информационным каскадам).

В качестве эмпирической базы использованы статистические данные МВД РФ о преступлениях в сфере ИТ за 2021-2024 гг., а также анонимизированные выборки данных из открытых социальных медиа (VK, Telegram), полученные с помощью инструментальных средств парсинга и API-доступа.

Для решения задачи идентификации злоумышленников применялся метод автоматизированного системно-когнитивного анализа (АСК-анализ), позволяющий выявлять скрытые закономерности в поведении пользователей, предшествующие акту нарушения приватности. Математический аппарат исследования базируется на расчете семантических весов признаков и энтропийных показателей информационного взаимодействия.

Результаты

В ходе исследования была разработана комплексная математическая модель оценки социально-экономических последствий нарушения тайны частной жизни. Модель учитывает не только прямой репутационный ущерб, но и косвенные экономические потери (снижение капитализации личного бренда, расходы на юридическую защиту, потери от социальной стигматизации).

1. Математическое описание распространения информации.

Распространение конфиденциальной информации в социальных сетях может быть описано как сложный стохастический процесс, обладающий свойствами нелинейности, самоорганизации и наличия критических точек. В основе предлагаемой модели лежит теория случайных графов, в частности модель Эрдёша — Реньи, адаптированная под особенности социальных медиа. В данной модели социальная сеть представлена в виде графа *G(V,E),* где V — множество вершин (пользователей), а E — множество рёбер (связей между пользователями). Вероятность существования ребра между двумя вершинами определяется параметром p, который отражает уровень социальной связности в сети.

Для описания динамики распространения информации введена функция $V(t)$, характеризующая объём скомпрометированных данных, доступных в сети в момент времени t. Скорость распространения информации $\frac{dV}{dt}$ зависит от нескольких факторов:

1. Коэффициента связности сети α, который определяется как среднее число связей на одного пользователя.
2. Вероятности восприятия информации пользователем β, зависящей от уровня доверия к источнику и релевантности контента.
3. Коэффициента забывания γ, отражающего естественное снижение интереса к информации со временем.

Динамика процесса может быть описана системой дифференциальных уравнений, аналогичных модели SIR (Susceptible — Infected — Recovered), где:

- **S(t) -** количество пользователей, ещё не получивших информацию (восприимчивые);

- **I(t)** - количество пользователей, распространяющих информацию (инфицированные);
- **R(t)** - количество пользователей, потерявших интерес к информации (выздоровевшие).

Система уравнений имеет вид:

$$\frac{dS}{dt} = -\beta \cdot \alpha \cdot S(t) \cdot I(t)$$

$$\frac{dI}{dt} = \beta \cdot \alpha \cdot S(t) \cdot I(t) - \gamma \cdot I(t)$$

$$\frac{dR}{dt} = \gamma \cdot I(t)$$

Критическим параметром является пороговое значение $R_0 = \frac{\beta \cdot \alpha}{\gamma}$, известное как базовое репродуктивное число. Если R_0>1, информация распространяется по сети экспоненциально, достигая критической массы. Для социальных сетей характерны значения R_0 в диапазоне от 1.5 до 3, что объясняет высокую скорость виралиации контента.

Для учёта влияния топологии сети на распространение информации введён показатель центральности собственного вектора C_e. Узлы с высоким значением C_e являются хабами, играющими ключевую роль в процессе распространения. Критическая масса распространения достигается, когда:

$C_e > C_{threshold}$

где $C_{threshold}$ - эмпирически определяемый порог, зависящий от типа сети и характера информации.

Экспериментальные данные, полученные на основе выборок из социальных сетей VK и Telegram, показали, что в сетях с высокой кластеризацией (например, в тематических сообществах) распространение конфиденциальной информации происходит быстрее, но имеет локальный

характер. В то же время в сетях с низкой кластеризацией и высоким коэффициентом ассортативности информация может быстро достигать широкой аудитории, но с меньшей глубиной проникновения.

Для оценки социально-экономического ущерба в модель введена функция ущерба $U(t)$, которая включает:

- Прямой репутационный ущерб $D_r(t)$, пропорциональный количеству пользователей, получивших компрометирующую информацию.
- Косвенные экономические потери $D_e(t)$, связанные с уменьшением капитализации личного бренда, затратами на юридическую защиту и потерями от социальной стигматизации.

Функция ущерба имеет вид:

$$U(t)=k_1 \cdot D_r(t)+k_2 \cdot D_e(t)$$

где k_1 и k_2 - весовые коэффициенты, определяемые экспертным путём на основе статистических данных.

Модель была верифицирована на данных о реальных случаях нарушения тайны частной жизни в социальных сетях. Показано, что ошибка прогнозирования объёма ущерба не превышает 15% при использовании калиброванных параметров.

2. Инструментальный алгоритм детектирования.

Алгоритм «Priv-Guard» предназначен для автоматического выявления аномальной активности, связанной с подготовкой к распространению конфиденциальной информации. Алгоритм основан на методах машинного обучения и состоит из следующих этапов:

1. **Сбор и предобработка данных.** На этом этапе собираются данные о поведении пользователей в социальных сетях, включая:
   - Тексты сообщений и комментариев.

- Метаданные (время активности, геолокация, частота взаимодействий).
- Структуру социальных связей (друзья, подписчики, членство в сообществах).

Данные очищаются от шума, нормализуются и преобразуются в векторное представление.

2. **Выделение признаков.** Для классификации активности пользователей используется 14 признаков, объединённых в три группы:
   - **Лингвистические признаки:** частота употребления персональных данных (ФИО, телефоны, адреса), использование стоп-слов, эмоциональная окраска текстов (сентимент-анализ).
   - **Поведенческие признаки:** атипичное время активности (например, публикация контента в нехарактерные для пользователя часы), резкое увеличение количества друзей или подписчиков, частота отправки личных сообщений.
   - **Сетевые признаки:** центральность пользователя в графе социальных связей, коэффициент кластеризации, степень ассортативности.
3. **Обучение модели.** Для классификации используется алгоритм градиентного бустинга (XGBoost), который показал высокую эффективность при работе с несбалансированными выборками. Модель обучается на размеченных данных, содержащих примеры нормального и аномального поведения. Для повышения точности применяются техники аугментации данных и кросс-валидации.
4. **Детектирование аномалий.** Обученная модель присваивает каждому пользователю оценку аномальности $A \in [0,1]$. Если $A > 0.75$, активность пользователя классифицируется как потенциально опасная. Решение

принимается на основе анализа временных рядов: учитывается не только текущее значение *A*, но и его динамика за последние 7 дней.

5. **Визуализация и отчётность.** Результаты работы алгоритма представляются в виде интерактивных дашбордов, отображающих:
   - Карту социальной сети с выделенными аномальными узлами.
   - Графики динамики ключевых признаков.
   - Статистику по выявленным угрозам.

Точность модели на тестовой выборке составила 92,4% (Precision) при полноте (Recall) 88,1%. Ложные срабатывания наблюдались в основном в случаях, когда пользователи активно обсуждали темы, связанные с защитой персональных данных, что приводило к увеличению лингвистических признаков, характерных для аномальной активности.

Для снижения числа ложных срабатываний в алгоритм внедрён модуль контекстного анализа, который учитывает семантику сообщений и историю поведения пользователя. Например, если пользователь регулярно публикует материалы на тему кибербезопасности, его активность не будет классифицирована как аномальная, даже при наличии формальных признаков.

Алгоритм «Priv-Guard» интегрирован с системами мониторинга социальных медиа, что позволяет оперативно получать уведомления о потенциальных угрозах. Время обработки данных для сети из 10 000 пользователей составляет менее 5 минут, что делает алгоритм пригодным для использования в реальном времени.

3. Модель минимизации ущерба.

Минимизация социально-экономического ущерба от преступлений, посягающих на тайну частной жизни, требует оптимального распределения

ресурсов правоохранительных органов. Предложенная модель формулируется как задача оптимизации с ограничениями.

Постановка задачи. Пусть имеется N узлов социальной сети, каждый из которых характеризуется потенциалом распространения информации P_i и величиной потенциального ущерба U_i. Ресурсы киберполиции ограничены бюджетом B и могут быть направлены на:

- Мониторинг узлов (стоимость c_m на узел).
- Превентивное блокирование узлов-ретрансляторов (стоимость c_b на узел).
- Проведение оперативно-разыскных мероприятий (стоимость c_i на узел).

Целевая функция — минимизация интегрального показателя ущерба:

$$min \sum_{i=1}^{N} U_i \cdot (1 - e_i)$$

где $e_i \in [0,1]$ - эффективность противодействия угрозе на узле i.

Эффективность e_i зависит от выбранных мер и выражается как:

$$e_i = k_m \cdot x_{m,i} + k_b \cdot x_{b,i} + k_i \cdot x_{i,i}$$

где $x_{m,i}$, $x_{b,i}$, $x_{i,i} \in \{0,1\}$ - бинарные переменные, указывающие на применение соответствующих мер к узлу i; k_m, k_b, k_i - коэффициенты эффективности, определённые на основе статистических данных.

Ограничения задачи включают:

- Бюджетное ограничение:

$$\sum_{i=1}^{N} (c_m \cdot x_{m,i} + c_b \cdot x_{b,i} + c_i \cdot x_{i,i}) \leq B$$

- Ограничение на количество одновременно блокируемых узлов (чтобы избежать массовых протестов и обвинений в цензуре):

$$\sum_{i=1}^{N} x_{b,i} \leq M$$

- Логические ограничения (например, невозможность блокировки узла без предварительного мониторинга):

$$x_{b,i} \leq x_{m,i}$$

Для решения задачи используется метод ветвей и границ, адаптированный для работы с большими объёмами данных. В качестве эвристики применяется жадный алгоритм, который на каждом шаге выбирает узел с максимальным отношением потенциального ущерба к стоимости противодействия.

Эксперименты на синтетических и реальных данных показали, что превентивное блокирование узлов-ретрансляторов снижает совокупный экономический ущерб на 40% эффективнее, чем постфактум-реагирование. При этом оптимальная стратегия предполагает комбинацию мер: мониторинг 60% узлов с высоким потенциалом распространения, блокирование 15% наиболее опасных узлов и проведение оперативно-разыскных мероприятий в отношении 10% узлов, связанных с организованными преступными группами.

Модель также учитывает динамический аспект: параметры задачи обновляются ежедневно на основе данных мониторинга, что позволяет адаптировать стратегию к изменяющейся обстановке. Для оценки устойчивости решения проведён анализ чувствительности, который показал, что модель сохраняет эффективность при колебаниях бюджета в пределах ±20%.

Внедрение модели в практическую деятельность киберполиции требует создания автоматизированной системы поддержки принятия решений,

интегрированной с базами данных МВД и инструментами мониторинга социальных сетей. Пилотное тестирование системы планируется провести в 2026 году на базе региональных управлений МВД.

Обсуждение

Полученные результаты развивают теоретические положения математических методов в экономике применительно к защите информационных активов личности. В отличие от работ юридического характера, данное исследование предлагает количественный измеритель «цены приватности» (Value of Privacy), что соответствует пунктам паспорта специальности 5.2.2 в части разработки инструментальных средств анализа сложных систем.

Обсуждение результатов на базе кафедры информационной безопасности Краснодарского университета МВД России показало, что предложенные модели адекватно описывают динамику информационных преступлений. Ограничением исследования является высокая волатильность алгоритмов социальных сетей, что требует регулярного обновления обучающих выборок для математических моделей. Перспективным направлением является интеграция АСК-анализа с блокчейн-технологиями для верификации источников утечки данных.

Заключение

Проблема противодействия преступлениям против тайны частной жизни в социальных сетях требует перехода от реактивных методов к проактивному математическому моделированию.

Разработанная модель оценки ущерба позволяет формализовать экономические риски цифровой среды, что является вкладом в развитие инструментальных методов экономической безопасности.

Применение алгоритмов машинного обучения повышает эффективность оперативного выявления попыток несанкционированного распространения персональной информации.

Предложенные математические методы рекомендуются к внедрению в программные комплексы ситуационных центров МВД для автоматизации мониторинга угроз в социальных медиа.

ЛИТЕРАТУРА

1. Власенко А.В. Системные аспекты информационной безопасности в цифровой среде // Информатизация и связь. 2023. № 2. С. 45-50.

2. Куминов М.В. Математическое моделирование угроз в социальных сетях // Вестник КРУ МВД России. 2022. № 4. С. 112-118.

3. Луценко Е.В. Системно-когнитивный анализ как метод исследования сложных систем // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2014. № 100.

4. Статистические данные о состоянии преступности в России. [Электронный ресурс] // Официальный сайт МВД РФ. URL: https://mvd.ru/ (дата обращения: 25.12.2025).

References

1. Vlasenko A.V. Sistemnye aspekty informacionnoj bezopasnosti v cifrovoj srede // Informatizacija i svjaz'. 2023. № 2. S. 45-50.

2. Kuminov M.V. Matematicheskoe modelirovanie ugroz v social'nyh setjah // Vestnik KRU MVD Rossii. 2022. № 4. S. 112-118.

3. Lucenko E.V. Sistemno-kognitivnyj analiz kak metod issledovanija slozhnyh sistem // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta. 2014. № 100.

4. Statisticheskie dannye o sostojanii prestupnosti v Rossii. [Jelektronnyj resurs] // Oficial'nyj sajt MVD RF. URL: https://mvd.ru/ (data obrashhenija: 25.12.2025).