*Ф. Галиндо, Э. Гурски, Н. В. Дмитриенко, Д. А. Журавлев, Р. Лапорт, Ф. Ю. Линькова, Н. Л. Михайлов, А. Россодивита, Ч. Томлянович, А. И. Труфанов, Е. Фотиу, Е. В. Шубников*

# СТРАТЕГИИ СОТРУДНИЧЕСТВА В ПРОТИВОДЕЙСТВИИ ГЛОБАЛЬНЫМ УГРОЗАМ

**Введение.** Борьба с глобальными бедствиями и смягчение их последствий требуют совместных усилий различных национальных и международных организаций. Эффективность такой совместной работы зависит от среды информационного обмена, в которой учреждения находятся.

Существует большая потребность в надежной, производительной и устойчивой архитектуре информационного взаимодействия, которая отражается в ее сетевой топологии. Топология сети определяется только графическим отображением конфигурации соединений между узлами (узлами могут выступать учреждения и их сотрудники). Настоящее исследование направлено на топологические вопросы развития сетей информационного обмена в чрезвычайных ситуациях и создания устойчивых отношений между соответствующими национальными и международными учреждениями.

**Методы.** В рамках исследования использовалась агентная модель эволюции сетевого взаимодействия конкурирующих и кооперирующих участников для выполнения простого количественного анализа межведомственного и международного сотрудничества.

Для реализации модели нами: а) задействованы сети с существенно различными топологическими особенностями — случайные и безмасштабные, б) сделано предположение, что все агенты-участники (узлы сети) находятся не только в постоянном сотрудничестве, но и в конкуренции: эти процессы имеют как вертикальный (для агентов смежных уровней), так и горизонтальный (для агентов одного уровня), межкластерный характер, в) полагалось, что межведомственное и международное взаимодействие осуществляется только горизонтально, другими словами, между узлами одной степени, но разных кластеров; г) полагалось, что все угрозы безопасности и соответствующие им атаки являются внутренними — непреднамеренными и преднамеренными; д) полагалось, что поддержка сетевых связей и защищенность агентов ограничены имеющимися ресурсами.

В качестве основных метрик при сопоставлении различных топологий мы использовали параметры, характеризующие эффективность сети и ее надежность, такие как поток, мощность, центральность (betweenness centrality); относительный размер максимального кластера, связность и коэффициент кластеризации.

**Результаты.** Исследование привело к следующему результату: оптимальная топология для межведомственного и международного взаимодействия отвечает связям на высшем уровне при преобладании случайных атак и соответствует межкластерным связям среднего ранга в иных случаях. Аналогично: знание топологии взаимодействия позволяет атакующей стороне выбрать в качестве лучшего направления атаки на узлы агенты высокого ранга, не имеющие межкластерных связей.

**Выводы.** Работа продемонстрировала, что в интересах эффективного противодействия глобальным угрозам большое значение имеет поддержка не только контактов национальных и международных учреждений на высшем уровне, но и связей между агентами среднего ранга.

Как и в исследовании [1], нами обсуждается возможность временной перестройки сети для устойчивости к атакам с учетом характера последних. Данный подход изначально зарождался в рамках международного интернет-проекта Supercourse [2], являлся базовым в организации международной конференции NATO ASI «Preparing Regional Leaders with the Knowledge, Training

and Instruments for Information Sharing and Decision-Making against Biological Threats and Pandemics», проведенной 30 ноября — 8 декабря 2008 г. в Милане, Италия [3], и используется в политике междисциплинарной сети информационного обмена [4]. Перспективным представляется дальнейшее совершенствование модели для решения задачи оптимизации распределения средств, направляемых на межведомственное и международное сотрудничество. Обсуждается возможность применения данных техник расчетов для анализа цепей миграции радионуклидов в экосистемах.

## СПИСОК ЛИТЕРАТУРЫ:

1. http://www.cs.cmu.edu/~pkeyani/publications/peerpressure.pdf.
2. http://www.pitt.edu/~super1/disasters/disasters.htm.
3. http://www.pitt.edu/~super1/BH/Milan5.html.
4. *Trufanov A., Caruso A., Dmitrienko N., Galindo F., Guidotti M., Gursky E., Kolesnikov S., Laporte R., Linkov F., Ranghieri M., Rossodivita A., Shubnikov E.* Information — Sharing Networks for Global Emergency Medical Services // Abstr. of Scientific and Invited Papers: 16th World Congress for Disaster and Emergency Medicine. Prehosp Disast Med 2009. 24(2). S. 81.

*Ю. В. Гель, А. Г. Ростовцев*

## ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ В ГРУППЕ КЛАССОВ ИЗОГЕННЫХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Безопасность существующих криптосистем с открытым ключом базируется на двух обобщенных задачах: дискретное логарифмирование в группе вычислимого порядка (на этой задаче основывается криптосистема Эль-Гамаля, а также стандарт электронной цифровой подписи ГОСТ Р 34.10-2001) и определение порядка и структуры конечной группы (например, задача разложения на множители, на которой основана безопасность криптосистемы RSA).

Новый тип вычислительных машин, использующий квантово-механические взаимодействия, может преодолеть многие ограничения для обычных компьютеров. Существуют задачи, которые могут быть решены на квантовом компьютере принципиально быстрее, чем на классическом. Например, разложить число на простые множители или вычислить дискретный логарифм в циклической группе можно с полиномиальной сложностью алгоритмом Шора. Это ставит под угрозу безопасность большинства криптосистем с открытым ключом. В настоящее время компания D-Wave Systems разработала модель квантового компьютера на сверхпроводящих торах разрядностью 512 $q$-битов.

Таким образом, нужна новая задача, стойкая по отношению к квантовому компьютеру. Один из возможных вариантов решения — использование задачи поиска изогении между эллиптическими кривыми.

Изогения эллиптических кривых — бирациональный гомоморфизм, мощность ядра которого над алгебраически замкнутым полем равна степени изогении. Изогения между эллиптическими кривыми существует тогда и только тогда, когда эти кривые имеют одинаковое число точек, т. е. их инварианты являются корнями одного и того же полинома Гильберта, задающего поле классов мнимого квадратичного порядка для дискриминанта эндоморфизма Фробениуса.