# Метод выявления киберугроз в информационно-коммуникационных сетях транспорта

УДК 621.395.7

Валерий Лахно[1], Берик Ахметов[2]

*[1]Национальный университет биоресурсов и природопользования Украины, lva964@gmail.com*
*[2]Каспийский государственный университет технологий и инжиниринга, Казахстан,berik@yu.edu.kz*

**Введение**. Современные ИТ являются основой стремительного социально-экономического развития постиндустриального общества и требует внедрения и использования новейших достижений науки и техники для повышения эффективности бизнес процессов и, как следствие, повышения качества предоставляемых цифровых услуг. Отдельные характеристики сложных технических компьютерных систем (КС), такие как, кибербезопасность (КрБ), надежность, живучесть, отказоустойчивость, характеризуют многие параметры функционирования КС при воздействии отказов и повреждений. Но эти характеристики не позволяют в полной мере описать процессы функционирования в КС в условиях воздействия потоков отказов и неисправностей, вызванных возможными преднамеренными воздействиями, в том числе и террористическими. Также не всегда в системах кибербезопасности рассматривается влияние на характеристики КС преднамеренных деструктивных действий или ошибок обслуживающего персонала, а также других внутренних и внешних дестабилизирующих факторов.

Заметим, что исследования последних лет в области киберзащищенности КС, в том числе критически важных КС (КВКС) в основном велись в направлении изучения отдельных их свойств, например, надежность [1] или отказоустойчивость [2], или устойчивость к отдельным типам деструктивных воздействий [3,4]. Комплексный подход к решению проблемы обеспечения заданного уровня функциональной устойчивости КВКС исследован мало [3,5]. Поэтому актуальность темы нашего исследования обусловлена рядом причин.

Существует явное противоречие между принципиальной возможностью разработки высокоэффективных функционально устойчивых ИКСТ на базе использования перспективных ИТ и недостаточной эффективностью существующих технологий защиты, которые не обеспечивают заданный уровень КрБ и функциональной устойчивости. В частности, в условиях роста количества и сложности киберугроз (КрУг) для ИКСТ [3–5].

Для решения, указанного выше противоречия, в процессе наших исследований поставлена и решена новая научная задача, которая заключается в разработке моделей и методов построения функционально устойчивых киберзащищенных ИКСТ.

**Цель работы -** развитие моделей и методов, направленных на повышение степени киберзащищенности ИКСТ.

**Основной материал.** Выявление кибератаки или аномалии в сетевом трафике – состояние, при котором значение функции $F(t)$ в любой момент времени $t$, является отличимым от штатного [6–8].

Множества внутренних и внешних кибератак, направленных на ИКСТ, в проектируемой в ходе наших исследований СППР, можно представить в виде таких кортежей [18, 21]:

$$RCA = \langle EST, CE, SS_{ne}, SS_h, PP, O(NN) \rangle , \quad (1)$$

$$ICA_{l(m)} = \langle IST_l^{k-1}, CE, SS_{ne}, SS_h, PP, O^k(NN_m^k) \rangle , \quad (2)$$

где $RCA, ICA_{l(m)}$ – удаленные и внутренние атаки на ИКСТ, соответственно; *k* – уровень критичности ресурса; $EST$ – внешний источник КрУг; $IST_l^{k-1}$ – внутренний источник киберугроз (КрУг); *CE* – сетевое оборудование; $SS_{ne}, SS_h$ – сервисы КрБ на путях распространения атак; *PP* – протоколы и пакеты в ИКСТ; *O* – объекты доступа в ИКСТ; $NN_m^k$ – узел, на котором обрабатывается информация с наибольшим уровнем критичности (*k*); *l, m* – номера узлов.

В соответствии с ранее полученными результатами [3] в СППР задействованы процедуры с нечетким логическим выводом (НЛВ).

Базы продукционных правил, а также функции принадлежности, были сформированы на основе ранее полученных экспертных данных и результатов моделирования [3]. Для ИКСТ усовершенствован метод выявления киберугроз, который включает рекурсивные алгоритмы распределенного сетевого самообучения и выбора контрмер (стратегий) в зависимости от вида киберугроз. В основе метода лежит модель выявления киберугроз, которая была ранее описана в наших предшествующих исследованиях [3]. Концептуально и логически модель делится на следующие модули: модуль сбора трафика и формирования статистики, модуль обучения системы обнаружения киберугроз (КрУг), модуль обнаружения КрУг и модуль оповещения (рис. 1). В первом модуле осуществляется перехват всего трафика, который проходит через узлы ИКСТ и выделяет признаки КрУг, а затем формирует статистику, которую передает модулю обучения.

Основной задачей модуля обучения является построение графа выявления киберугроз (КрУг). Данный граф собирает информацию обо всех известных угрозах, в частности, тех, которые хранятся в базе знаний (БЗ) СППР или ЭС по распознаванию. Таким образом получается полная картина текущей ситуации в области КрБ ИКСТ.

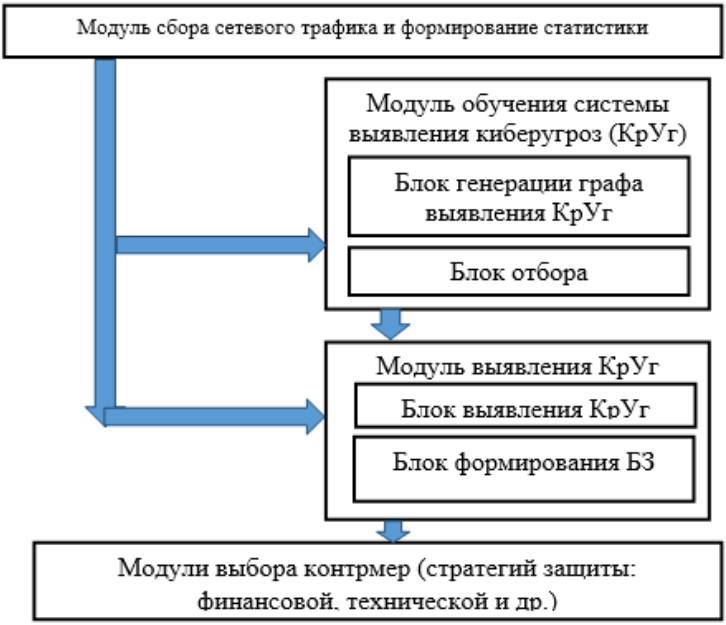


Рис. 1. Модель выявления киберугроз в ИКСТ

Благодаря этому появляется возможность спрогнозировать возможные новые КрУг и кибератаки (КрАт) путем определения взаимозависимости выявленных событий. Т.е. если событие распознается в качестве потенциальной кибератаки, то возможно применить конкретные меры для смягчения последствий ее воздействия (например, за счет задействования аппаратно-программных средств защиты) или выбрать соответствующую финансовую или организационную стратегию реагирования или предотвращения потенциально опасных угроз. Поэтому основной целью графа выявления киберугроз (ГВКрУг) является описание возможных кибератак (КрАт) и результатов их влияния на узлы сети.

Предложенный подход имеет следующие преимущества в сравнении с аналогичными решениями, используемыми в системах распознавания угроз [2, 9–12]: метод позволяет оценивать уровень защищенности информации на объекте защиты, состоящий из множества узлов, в которых обрабатывается информация разного уровня критичности; можно задавать исходные данные по количеству сегментов и узлов ИКСТ, учитывая уровни критичности информационных ресурсов; обеспечивается оперативность оценки контрмер для защиты.

Перспектива дальнейших исследований определяется возможностями применения полученных результатов для последующей алгоритмизации процессов, связанных с повышением киберзащищённости ИКСТ. Также

возможна программная автоматизация обработки данных о возможных киберугрозах.

**Выводы:** Получены такие результаты:

усовершенствован метод выявления киберугроз в ИКСТ. Усовершенствованный метод, в отличие от существующих, содержит рекурсивные алгоритмы распределенного сетевого самообучения и выбора контрмер (стратегий, в частности финансовых или технических для стороны защиты ИКСТ) в зависимости от вида киберугроз;

показано, что реализация предложенных дополнений к методам выявления киберугроз, позволит осуществлять вывод обоснованных решений о необходимых контрмерах для улучшения степени защищенности ИКСТ. При этом анализируется, поступающая от разных источников в ИКСТ информация об киберугрозах в условиях динамического изменения целей управления ИКСТ в реальном времени.

**Литература**

1. Petit, J., Shladover, S. E. Potential Cyberattacks on Automated Vehicles, *IEEE Transactions on Intelligent Transportation Systems*, 2015. Vol. 16, Iss. 2., P. 546 – 556. DOI: 10.1109/TITS.2014.2342271

2. Miao, F., Zhu, Q., Pajic, M. G., Pappas, J. Coding Schemes for Securing Cyber-Physical Systems Against Stealthy Data Injection Attacks, *IEEE Transactions on Control of Network Systems*, 2016, Vol. PP, Iss. 99, P. 1. DOI: 10.1109/TCNS.2016.2573039

3. Akhmetov, B. System of decision support in weaklyformalized problems of transport cybersecurity ensuring, Journal of Theoretical and Applied Information Technology, Vol. 96, Iss. 8, pp. 2184-2196.

4. Sawik, T. Selection of optimal countermeasure portfolio in it security planning, *Decision Support Systems*, 2013, Vol. 55, Iss. 1, P. 156–164. http://dx.doi.org/10.1016/j.dss.2013.01.001

5. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F. Decision support approaches for cyber security investment, *Decision Support Systems*, 2016, Vol. 86, P. 13–23. http://dx.doi.org/10.1016/j.dss.2016.02.012

6. Atymtayeva, L., Kozhakhmet, K., Bortsova, G. Building a Knowledge Base for Expert System in Information Security, *Chapter Soft Computing in Artificial Intelligence of the series Advances in Intelligent Systems and Computing*, 2014, Vol. 270, P. 57–76. DOI:10.1007/978-3-319-05515-2_7

7. Gamal, M.M., Hasan, B., Hegazy, A.F. A Security Analysis Framework Powered by an Expert System, *International Journal of Computer Science and Security (IJCSS)*, 2011, Vol. 4, No. 6, P. 505–527.

8. Dua, S., Du, X. Data Mining and Machine Learning in Cybersecurity, UK, CRC press, 2016, p. 225.

9. Buczak, A. L., Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, *IEEE Communications Surveys & Tutorials*, 2016, Vol. 18, Iss. 2. – P. 1153–1176. DOI: 10.1109/COMST.2015.2494502

10. Al-Jarrah, O., Arafat, A. Network Intrusion Detection System using attack behavior classification, 2014 5th International Conference on Information and Communication Systems (ICICS), 2014, DOI: 10.1109/iacs.2014.6841978

11. Ben–Asher, Gonzalez, N. C. Effects of cyber security knowledge on attack detection, *Computers in Human Behavior*, 2015, Vol. 48, P. 51–61. DOI: 10.1016/j.chb.2015.01.039

12. Nishanov, A. Kh, Kerimov, K.F. Methods of Counteraction from Attacks Carried out Against Users in a Network the Internet, ICEIC-Electronics, news and communications, IX-the conference, Tashkent, 2008, P. 298–299.