## УДК 681.5

### Б. Ахметов

Казахский национальный педагогагический университет имени Абая E-mail:akmetov.b@iuth.edu.kz.

## МЕТОД ОПРЕДЕЛЕНИЯ ОБЪЕКТОВ НА ОСНОВЕ СОДЕРЖАТЕЛЬНОЙ

**ИДЕНТИФИКАЦИИ**

**Аннотация.** Рассматривается метод содержательной идентификации объектов при проектировании экспертных систем в задачах оценки киберугроз и рисков для информационной безопасности критически важных объектов информатизации.

**Ключевые слова.** Экспертные системы, силлогизмы, киберугрозы, кибербезопасность.

### Введение.

Организация системы информационной безопасности (ИБ) сегодня становится важным стратегическим фактором развития для многих компаний и предприятий, информационные системы которых попадают под определение критически важных объектов информатизации [1]. А поскольку сложность архитектуры большинства критически важных объектов информатизации (КВОИ) снижает результативность и достоверность обычной экспертной оценки угроз и рисков для информационной и кибербезопасности (КрБ) КВОИ, то, по мнению многих специалистов [2, 3], целесообразно для решения этой задачи использовать потенциал интеллектуальных систем поддержки принятия решений или экспертных систем (ЭС) [4].

### Материалы и методы.

При проектировании экспертных систем в задачах оценки киберугроз и рисков для ИБ КВОИ одним из естественных этапов является формирование аналитиками анкет или опросных листов, которые содержат типовые вопросы, задаваемые при аудите ИБ. Например, к таким вопросам можно отнести – имели ли место инциденты, располагает ли организация конфиденциальной информацией и т.п. [5, 6]. Далее эксперт или аналитик по ИБ формирует унарные и/или бинарные высказывания. Подобные высказывания позволяют строить так называемые сориты, т.е. цепь последовательных силлогизмов. В контексте проектирования базы знаний (БЗ) для ЭС в задачах ИБ, силлогизм – это двухпосылочное умозаключение, которое состоит из атрибутивных высказываний. Далее, используя аппарат исчисления предикатов и семантические сети, можно сформировать модели для актуальных киберугроз конкретному КВОИ. В общем, ключевые этапы алгоритма формирования перечня киберугроз для КВОИ можно представить в виде схемы, которая показана на рисунке 1.

|  |
| --- |
| Описание КВОИ путем компоновки унарныхвысказываний |
| Описание КВОИ путем компоновки бинарных высказываний |
| Формирование списка киберугроз для КВОИ путемкомпоновки силлогизмов |

Моделирование вероятностей реализации киберугроз (методы [1–4, 24–26])



Прогнозирование развитие ситуации при реализации киберугрозы (методы [4–7])

Оценка потенциального ущерба от реализации

киберугроз (методы [1, 12, 15])

Рисунок 1 – Общая схема взаимодействия алгоритмов оценки угроз и рисков ИБ

КВОИ

При проектировании баз знаний использовались такие базовые унарные высказывания: 0 – выполнение вредоносного ПО; 1 – использование входов USB; 2 – использование гибких дисков; 3 – наличие выхода в интернет; 4 – наличие выхода в локальную вычислительную сеть (ЛВС); 5 – наличие CD/DVD; 6 – отсутствие обновлений антивирусов и сигнатур; 7 – отсутствие системы комплексной ЗИ; 8 – отсутствие антивируса; 9 – отсутствие инструкций для ответственного за ИБ и КрБ; 10 – отсутствие в инструкциях для администратора ИБ; 11 - отсутствие технологических процессов ЗИ; 12 – отсутствие инструкций для средств антивирусной ЗИ; 13 – отсутствие акта по установке средств ЗИ; 14 – утечка ключей и атрибутов доступа; 15 – отсутствие файлов резервной копии; 16 - отсутствие элементов в инструкциях пользователям; 17 – факт разглашения информации; 18 – отсутствие договора о неразглашении информации сотрудниками; 19 – гроза заражения ЛВС вирусным ПО; 20 - угроза перехвата паролей в ЛВС; 21 – отсутствие файрвола; 22 – 100 и другое, включая резерв.

Данный подход рассмотрим на примере построения цепи последовательных силлогизмов, которые оперируют исходными высказываниями в области сетевой безопасности.

### Результаты исследования.

Составим простейшие унарные высказывания, которые описывают характеристики

объекта информатизации: 1)

*S*0 

анализируем КВОИ; 2)

*S*1 КВОИ использует

подключение к интернет; 3)

*S* 2 

КВОИ не имеет угроз хакерских атак; 4)

*S*3 

КВОИ

подвержен угрозам хищений информации; 5) *S* 4  КВОИ подвержен угрозам, связанным с

уничтожением информации; 6) *S*5  КВОИ подвержен угрозам, связанным с заражением вредоносным ПО.

Составим бинарные высказывания, которые будут описывать уязвимости КВОИ. Бинарные высказывания составлены на основе унарных высказываний и при этом также

применялась логика кванторов (рисунок 2): *A*, *S* 0, *S*1  анализируемый КВОИ – это КВОИ,

который использует подключение к Интернет. Или: *A*, *S*1, *S* 2  всякий КВОИ, использующий подключение интернет – это КВОИ, имеющий угрозы хакерских атаки;

*A*, *S* 2, *S*3  КВОИ, имеющий угрозы хакерских атак – это КВОИ, подверженный угрозам

хищения информации; *A*, *S* 2, *S* 4  КВОИ, имеющий угрозы хакерских атак – это КВОИ,

подверженный угрозам уничтожения информации; *A*, *S* 2, *S*5  КВОИ, подверженный

угрозам хакерских атак – это КВОИ, подверженный угрозам заражения вредоносным ПО.

### Выводы.

Таким образом, бинарные высказывания – это одна из посылок силлогизма с соответствующими кванторами. Силлогизмы можно сочетать в различных комбинациях. Каждое такое сочетание позволяет получать новое заключение. Аналогично можно сочетать между собой полученные заключения. Подобные операции можно продолжать до момента, пока переход от изменяющихся сильных свойств объекта анализа (или в терминах силлогизмов модусы) к слабым, не прервет процессы синтезы новых выводов.

Рисунок 2 – Пример бинарных высказываний в экспертной системе

Так пример, показанный на рисунке 2, позволяет сделать очевидный вывод. Если автоматизировать процесс синтеза связей между силлогизмами, то можно с помощью ЭС определять не только непосредственно перечень угроз для КВОИ, но и актуализировать их для текущего момента времени. А на выходе, получив перечень актуальных угроз, на основе применения уже имеющихся моделей или результатов наших предшествующих исследований [1–4], можем приступить к определению вероятностей реализации киберугроз для конкретного КВОИ.

Заметим, что в модели подачи знаний, представленной на рисунке 2, отсутствует семантическая метрика и не всегда может быть учтена внутренняя интерпретируемость знаний, касающихся новых угроз для ИБ и КрБ КВОИ.

## ЛИТЕРАТУРА

1. Davies J., Milward, D., Wang C. W., & Welch J. Formal model-driven engineering of critical information systems. /Science of Computer Programming. – 2015. –№103. P. 88-113.
2. Shahbazian E., Rogova G. Critical Aviation Information Systems Cybersecurity. In Meeting Security Challenges Through Data Analytics and Decision Support. / IOS Press. –2016. – Vol. 47. – P. 308.
3. Paradice D., Freeman D., Hao J., Lee J., & Hall D. A Review of Ethical Issue Considerations in the Information Systems Research Literature. / Foundations and Trends® in Information Systems. – 2018. – № 2(2). – P. 117-236.
4. Akhmetov B., Lakhno V., Malyukov V., Sarsimbayeva S., Zhumadilova M., Kartbayev

T. Decision support system about investments in smart сity in conditions of incomplete information. //International Journal of Civil Engineering and Technology. – 2019. – № 10 (2). –

P. 661-670.

1. Li K., Wen H., Li H., Zhu H., Sun L. Security OSIF: Toward Automatic Discovery and Analysis of Event Based Cyber Threat Intelligence. // In 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM /UIC/ATC/CBDCom/IOP/SCI) IEEE. – 2018. – P. 741-747.
2. Kashyap A. K., Wetherilt A. Some principles for regulating cyber risk. / In AEA Papers and Proceedings. – 2019. – Vol. 109. – P. 482-87.