УДК 681.518.5:004.7

МЕТОДИКА КЛАССИФИКАЦИИ АКТИВОВ ПО КИБЕРБЕЗОПАСНОСТИ

В.Г. Промыслов
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: v1925@mail.ru

К.В. Семенков
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: semenkovk@mail.ru

А.С. Шумов
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: mau17@list.ru

Ключевые слова: кибербезопасность, формальные методы, классификация активов, кластеризация, модель “take-grant”, иерархические системы.

Аннотация: В работе предложена методика классификации активов по кибербезопасности. Проблема решается в рамках решения задачи кластеризации. Определены состав и форма представления исходных данных. Предложен алгоритм классификации активов по кибербезопасности в системах с произвольным числом подсистем.

1. Введение

Решение проблемы обеспечения кибербезопасности (защищенности) систем управления на АЭС тесно связано с задачами выявления критически важных активов в защищаемой системе и назначения мер защиты этих активов [1]. Сложилась следующая практика обеспечения защищенности сложных программно-технических комплексов: уровни кибербезопасности назначаются активам в соответствии с критичностью этих активов для общей безопасности [2, 3]. Степень защиты каждого из активов должна соответствовать присвоенному для него уровню кибербезопасности. Между классифицированными активами устанавливаются соответствующие барьеры, препятствующие распространению угрозы; с каждым активом должен быть связан набор мер для предупреждения кибератак, их выявления и реагирования на них [1]. На сегодня не известно подхода, формализующего задачу классификации активов для систем управления (АСУ ТП), учитывающего специфику систем управления АЭС и предлагающего подход сверху вниз.

Мы предлагаем рассмотреть задачу классификации активов как классическую задачу кластеризации [4, 5], связанную с построением отношения порядка на множестве активов кибербезопасности. Представленный подход полностью учитывает сложившуюся практику классификации активов по кибербезопасности для АЭС, изложенную в профильных документах МАГАТЭ и МЭК.

2. Кластеризация в задаче классификации

Для выбора представления данных необходимо идентифицировать активы, определить значения признаков на активах, шкалы измерений. Для задания отношений между признаками и активами предлагается использовать таблицу вида «актив–признак». В Таблице 1 приведен пример формы представления исходных данных для задач классификации активов АСУ ТП АЭС по кибербезопасности, где признаки — столбцы 2–4 данной таблицы.

Таблица 1. Признаки активов АСУ ТП АЭС..

Актив	**Класс по ядерной безопасности (ЯБ)**	**Функциональное свойство актива**	**Информационные свойства актива**		
			Конфиденциальность	**Целостность**	**Доступность**
1	2	3	4		

Число признаков может быть произвольным, но в данной работе для наглядности мы ограничились тремя признаками.

Функциональными свойствами актива могут быть любые характеристики, имеющие значимость для кибербезопасности. В качестве примера рассмотрим такое свойство: назначение актива состоит либо в обработке данных по определенным алгоритмам, либо в хранении данных (буфер).

Информационные свойства актива по отношению к кибербезопасности определяются уровнем конфиденциальности, целостности и доступности информации, ассоциированной с активом. Основное внимание уделяется сохранению доступности и целостности информации, данные свойства доминируют над принципом сохранения конфиденциальности информации. В данной работе мы рассматриваем только статические системы, и свойство доступности нас интересовать не будет. Тогда мы можем сосредоточиться только на целостности информации.

Представим модель системы в виде графа (графа безопасности), отражающего физическую природу описываемых систем и обозначим его $G = G(X, E)$, где X – множество вершин, E – множество ребер.

Воспользуемся широко применяемой дискретной моделью распространения прав доступа, или моделью take-grant («брать-давать») [6]. Она использует теорию графов для описания отношений доступа между объектами и субъектами политики безопасности. Рассматриваемый в настоящей работе вариант модели take-grant основан на подходе, описанном в работе [7].

Из существования отношения порядка на подмножестве вершин следует, что на этом подмножестве мы можем ввести порядковую функцию $R(x)$. Мы будем использовать следующую порядковую функцию графа безопасности: количество исходящих из вершины ребер после транзитивного замыкания графа безопасности по выбранному отношению доступа. Это соответствует тому, что более важным с точки зрения организации защиты мы будем считать элемент системы, который передает информацию большему числу абонентов.

После приведения всех признаков к численному виду каждому активу будет соответствовать вектор порядковых функций, задающих численное значение соответствующего признака для актива $\{R_1(x), \ldots, R_n(x)\}$, где n — номер признака в таблице признаков.

Для приведения признаков к сопоставимому виду проводится перенормировка значений: у каждого признака изменяют точки отсчета и масштаб шкалы. Начало координат лучше всего помещать где-то в районе центра множества точек, представляющих признак для активов [5]. Коэффициенты нормирования следует выбирать, исходя из идеи выравнивания относительных шкал признаков.

Для разбиения активов на классы кибербезопасности мы предлагаем использовать метод кластеризации разбиения с центроидами по методу k-средних [8].

3. Пример кластерного анализа и верификация результатов

Рассмотрим пример сегмента АСУ ТП АЭС, состоящего из рабочей станции (РС) оператора, РС начальника смены блока (НСБ), РС архива, архива хранилища данных,

сервера обработки информации и шлюза, обеспечивающего взаимодействие с механизмами АЭС.

Признаки системы сведены в таблицу признаков 2. Граф безопасности системы, отображающий информационные связи в рамках модели take-grant, представлен на рис. 1.

Таблица 2. Таблица признаков.

Имя системы	Класс ЯБ	Доп. признак	РС Оператора	РС НСБ	РС Архив	Сервер	Шлюз	Архив хранилище
РС Оператора	2	1	1	0	0	1	0	0
РС НСБ	2	1	0	1	0	0	0	0
РС Архив	3	1	0	0	1	0	0	0
Сервер	2	2	1	1	0	1	1	1
Шлюз	2	1	0	0	0	1	1	0
Архив хранилище	3	0	0	0	1	0	0	1

На рис. 1 незакрашенным кружком обозначен актив «хранилище данных», серыми кружками – все остальные активы, красными линиями – информационные связи по отношению w (write), коричневыми линиями – информационные связи по отношению r (read).

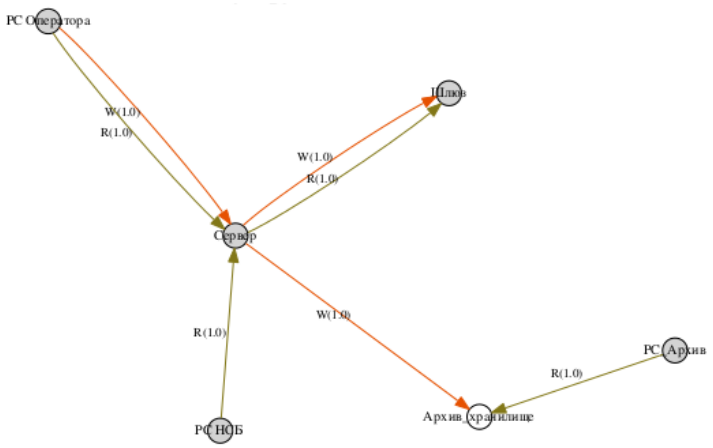

Рис. 1. Граф безопасности системы в рамках модели take-grant.

Определим уровни безопасности для активов, входящих в систему, по отношению записи (*w*). Для этого следует выполнить транзитивное замыкание графа по отношению *w*.

После кластеризации было получено разделение всего множества активов на 3 непересекающиеся подмножества, где активы сгруппированы по сходству признаков. Графическое отображение этого разделения приведено на рис. 2, где оси на графике представляют собой шкалы соответствующего пространства признаков.

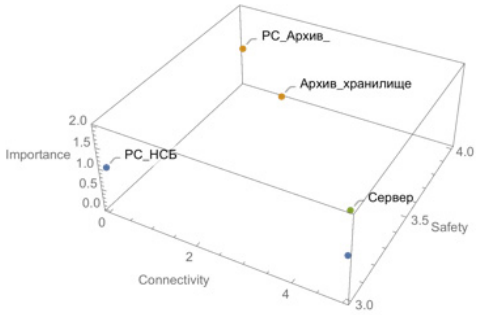

Рис. 2. Графическое отображение разделения активов по уровням кибербезопасности.

Заметим, что метод кластеризации не предполагает упорядочения полученных кластеров. Чтобы получить упорядоченное множество кластеров, до начала кластеризации к каждому из уровней кибербезопасности был отнесен один актив, который использовался в дальнейшем для задания центроида соответствующего кластера. В результате был получен набор упорядоченных кластеров (см. Таблицу 3).

Таблица 3. Разделение активов по уровням кибербезопасности.

Уровни кибербезопасности		
S1	**S2**	**S3**
Сервер	РС Оператора	РС архива
	РС НСБ	Архив хранилища
	Шлюз	

Если в исследуемой системе нет подсистем (активы атомарны), то предложенный метод дает полный формальный подход классификации активов по кибербезопасности. Для классификации систем с произвольным количеством уровней вложенности мы предлагаем использовать следующий алгоритм:

1) Проектировщик системы строит граф безопасности, вершинами которого являются подсистемы, и проводит на нем классификацию активов. В результате каждой подсистеме назначается определенный класс безопасности.
2) Проектировщик каждой из подсистем строит граф безопасности своей подсистемы и проводит классификацию активов с наложенными дополнительными условиями: максимальный класс безопасности актива равен классу безопасности подсистемы. Для корректной классификации необходимо, что бы хотя бы один их активов подсистемы имел уровень кибербезопасности, назначенный для всей подсистемы. Данный актив должен использоваться как центроид для задания соответствующего кластера при кластеризации.
3) Проектировщик подсистемы второго уровня (подсистемы внутри подсистемы) проводит классификацию активов своей подсистемы в соответствии с п. 2, и т.д.

4. Выводы

В работе предложен формальный метод классификации активов АСУ ТП АЭС по кибербезоасности. Рассмотрена проблема классификации иерархических систем и показана применимость индуктивного подхода к ее решению.

В заключение отметим, что основная проблема кластерного анализа в нашем случае — отсутствие четкой математической связи результатов кластеризации с искомыми уровнями кибербезопасности для активов. Поэтому необходима верификация результата: либо через анализ внутренних свойств полученного результата классификации, либо

через сопоставление результата, полученного методами кластеризации, с результатами, полученными другими методами и подходами.

Список литературы

1. IEC 62645 ed 1. Атомные электростанции. Системы контроля и управления. Требования к программам обеспечения безопасности для компьютерных систем. 2014.
2. Computer Security at Nuclear Facilities Technical Guidance Reference Manual IAEA. Nuclear Security Series. 2011. No. 17.
3. ФСТЭК России от 14.03.2014 № 31 (ред. от 23.03.2017) «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющую повышенную опасность для жизни и здоровья людей и для окружающей природной среды». Зарегистрировано в Минюсте России 30.06.2014, № 32919.
4. Kaufman L., Rousseeuw P.J. Finding Groups in Data: An Introduction to Cluster Analysis. New York: Wiley, 1990.
5. Mirkin B. Mathematical Classification and Clustering, Dordrecht-Boston-London, Kluwer Academic Publishers, 1996.
6. Bishop M. Computer Security: Art and Science. Boston: Addison Wesley, 2003.
7. Промыслов В.Г., Полетыкин А.Г. Формальная иерархическая модель безопасности верхнего уровня АСУТП АЭС // Ядерные измерительно-информационные технологии. 2012. Т. 4 (44). С. 39-53.
8. Bishop C.M. Neural Networks for Pattern Recognition. Oxford, England: Oxford University Press, 1995.