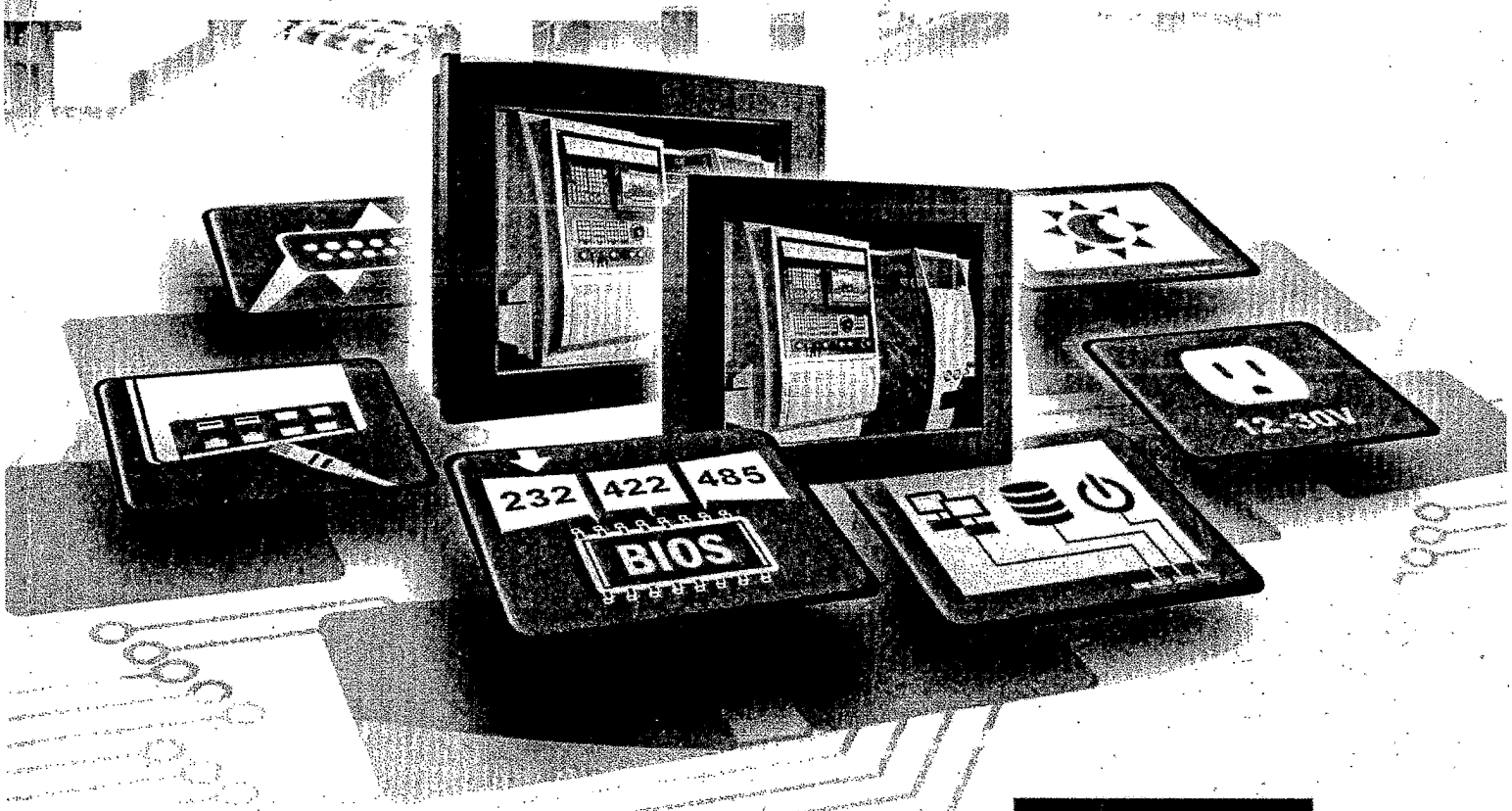
41 19 8-9

Промышленные Контроллеры

8.2013
ISSN: 1561-1531
Industrial Automatic Control Systems and Controllers

PPC-3120 / 3100 Безвентиляторный панельный компьютер с процессором Intel® Atom™ D2550

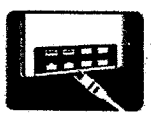
Спроектировано для машиностроения



PPC-3120/3100 12.1"/10.4"-дюймовый безвентиляторный панельный компьютер с процессором Intel® Atom™ D2550

ADVANTECH
Enabling an Intelligent Planet

- Процессор Intel Atom D2550 с низким энергопотреблением
- Поддержка питания DC 12~30V input support
- Безвентиляторное исполнение с диапазоном рабочих температур 0~50°
- Встроенный интерфейс mSATA, 4 COM порта, 4 порта USB



Легкодоступные порты ввода-вывода

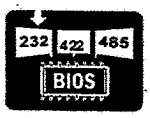
Порты ввода/вывода сзади, легкий монтаж в панель, ничто не мешает.

Автоматическая регулировка яркости

Светодиодный дисплей с автомати-ческой регулировкой яркости, два режима работы, устанавливаемые BIOS или ПО.

Питание через COM-порт

Последовательный порт с возможностью подачи 5V/12V, выбираемой через BIOS, повышает эффективность системной интеграции.



Управление портами в BIOS

Режимы RS-232/422/485 выбираются в BIOS.

Широкий диапазон напряжений питания

Поддерживает питание 12-30V для надежной работы в промышленных средах.

Светодиодные индикаторы

Светодиодный индикатор на передней панели отображает состояние системы включая наличие питания, доступ к накопителю и сети.

Windows Embedded

http://www.advantech.ru/applied-computing-systems/panel-pc/

Advantech Россия
Ул.Профсоюзная,108, 6 этаж, оф.648
Москва, 117437, Россия
Тел.: +7 (495) 232-16-92
Email: info@advantech.com
Web: www.advantech.ru

Промышленные Контроллеры АСУ

8/2013

ООО ИЗДАТЕЛЬСТВО «НАУЧТЕХЛИТИЗДАТ» ISSN 1561-1531

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ПРОИЗВОДСТВЕННЫЙ ЖУРНАЛ

СОДЕРЖАНИЕ

АСУ ДЛЯ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

Чистякова М.А.
Автоматизированная система управления запасами готовой продукции 3

ООО "КРУГ-Софт"
SCADA/HMI DataRate в системе управления линии экспандирования комбикормов Челябинского комбината хлебопродуктов им. Григоровича 12

НОВОСТИ СИСТЕМОСТРОЕНИЯ 15

НОВЫЕ ТЕНДЕНЦИИ И ТЕХНОЛОГИИ В ЭФФЕКТИВНОЙ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ

Коршаков А.В., Шатерников В.Е.
Идентификация и определение достоверности принятых решений по вызванной энцефалографической активности 20

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Пилипенко А.В.,. Пилипенко А.П, Абашин В.Г.
Исследование и модернизация математической модели работы гидропрессового оборудования 26

Интеллектуальные системы

Игнатов А.С., Круг П.Г., Лупачев А.А.
Структура и принципы построения аппаратно-программного комплекса интеллектуального управления движением автомобильных потоков 34

Программное обеспечение

Мезенцев К.Н.
Системный подход и имитационное моделирование 40

ТЕХНИЧЕСКИЕ СРЕДСТВА АСУТП

ЗАО "РТСофт"
Когда все должно быть готово вчера... 45

Волошин Е.В.
Анализ и разработка программных средств мониторинга и диспетчеризации для регулятора тепловой энергии Danfoss ECL 210/310 51

Emerson Process Management
WirelessHART, пожалуй, единственный беспроводной протокол связи, удовлетворяющий требованиям рынка АСУТП 58

Сетевые многофункциональные контроллеры

Сенина Т.Е., Сенин Л.Н.
Модуль аудиосообщений в составе переносной сейсмической станции "Синус" 62

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Лось А.Б., Кабанов А.С., Трунцев В.И.
Особенности использования кластерного анализа в системе менеджмента информационной безопасности 67

ХРОНИКА 73

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ ЖУРНАЛА
ООО "САТАГЕ"
ООО Издательство
«НАУЧТЕХЛИТИЗДАТ»

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций
Свидетельство о регистрации
ПИ № 77-1141
Подписной индекс 79216

Подписано в печать 22.07.2013.
Формат 60×88 1/8. Бумага кн.-журн. Печать офсетная.
Усл.-печ. л. 8,7. Усл. кр.-отт. 13,74. Уч.-изд. л. 13,48. Зак. 535.
Тираж 5400 экз.

Адрес редакции: Москва, 107258, Алымов переулок, дом 17, строение 2. Тел.: +7(499) 168-23-28, +7(916) 008-23-28.
E-mail: promasu@mail.ru. www.tgizd.ru

По вопросам приобретения журнала обращаться в бухгалтерию издательства по тел.:
Тел./факс: +7 (499) 168-13-69. *E-mail: buchnauch@mail.ru*

Оригинал-макет и электронная версия подготовлены ООО Издательство «Научтехлитиздат»
Отпечатано в ООО Издательство «Научтехлитиздат».
107258, Москва, Алымов пер., д. 17, стр. 2

А.Б. Лось
канд. техн. наук, доцент
E-mail: alos@hse.ru
А.С. Кабанов
канд. техн. наук, доцент
E-mail: kabanov_as@mail.ru
В.И. Трунцев
(Московский институт электроники и математики Национального исследовательского университета "Высшая школа экономики")
Москва, Российская Федерация

Особенности использования кластерного анализа в системе менеджмента информационной безопасности

В статье обсуждаются вопросы применения методов кластерного анализа в системе менеджмента информационной безопасности. Описаны принципы и классификация методов кластерного анализа данных. Приведен пример работы иерархического алгоритма кластеризации. Рассмотрен метод кластеризации применительно к информационной системе, каждый элемент которой описываются двумя параметрами – вероятностями реализации угроз. Исследуются преимущества методов кластерного анализа в системе менеджмента информационной безопасности. Отмечены особенности использования кластерного анализа для оценки рисков информационной безопасности.

Ключевые слова: *менеджмент информационной безопасности; кластерный анализ; риски информационной безопасности; классификация рисков.*

A.B. Los
Cand. of Techn. Sciences, Associate Professor
E-mail: alos@hse.ru
A.S. Kabanov
E-mail: kabanov_as@mail.ru
V.I. Truntsev
(Moscow Institute of Electronics and Mathematics National Research University "Higher School of Economics")
Moscow, Russian Federation

The Features of Cluster Analysis Application in the Information Security Management System

The article discusses the application of the methods of cluster analysis in the information security management system. It describes the principles and classification of methods of cluster analysis of the data. An example of hierarchical clustering algorithm. The method of clustering in relation to the information system, each element of which are described by two parameters - the probabilities of threats. Explores the advantages of the methods of cluster analysis in the system of information safety management. Marked by features of the use of cluster analysis for the assessment of information security risks.

Keywords: *management of information security; cluster analysis; risks information security; risk classification.*

В условиях увеличивающейся сложности и интеграции информационных систем вопросы информационной безопасности (ИБ) приобретают все большее значение. С одной стороны, требуется построение единого информационного пространства предприятия, быстрой интеграции имеющихся и вновь внедряемых информационных систем и комплексов в единое решение, позволяющее осуществлять оперативное и стратегическое управление компанией и производством. С другой стороны, крайняя неравномерность развития ИТ-служб и инфраструктуры и разнородность эксплуатируемых информационных систем препятствуют обеспечению требуемого уровня ИБ. Обеспечение ИБ становится одной из приоритетных задач предприятий и организаций с целью поддержания ее нормальной деятельности, устойчивости на рынке и успешного развития. В сложившихся условиях необходимо построение действительно комплексной корпоративной системы менеджмента информационной безопасностью (СМИБ), являющейся одной из наиболее важных

составляющих в общей системе менеджмента компании.

Для современного менеджмента ИБ характерен проактивный подход. В отличие от реактивного он предполагает решение проблем не "по мере их поступления", когда бывает уже слишком поздно ими заниматься, а предусматривает заблаговременный анализ и упреждение возможных проблем, на основе оценки возможных рисков ИБ, руководствуясь при этом соображениями экономической целесообразности [4]. Поэтому фундаментом для успешного внедрения и функционирования СМИБ является оценка и анализ рисков ИБ.

Анализ рисков – это процедуры выявления факторов рисков ИБ и оценки их значимости. Анализ рисков ИБ включает оценку рисков и методы снижения рисков или уменьшения связанных с ними неблагоприятных последствий. При анализе вначале производится выявление соответствующих факторов и оценка их значимости, полнота выявленных факторов увеличивает качество и точность прогнозируемых рисков [1]. К таким факторам относятся множество активов, уязвимостей и угроз. Основная цель создания классификации угроз ИБ – полная, детальная классификация, описывающая все существующие угрозы ИБ и которая наиболее применима для анализа рисков реальных информационных систем [6].

При исследовании множества факторов порождающих риски ИБ возникает задача сведения множества параметров и характеристик к небольшому ряду обобщающих итогов, выражающему действительно существенное. Такую задачу решают методы *кластерного анализа.*

Кластерный анализ широко используется в прогнозировании поведения того или иного объекта по набору признаков, определяющих поведение этого объекта. В экономике, к примеру, кластерный анализ может быть использован при исследовании сегментации рынков [10].

Основа кластерного анализа состоит в делении множества точек группы таким образом, чтобы каждая точка принадлежала только одному выделенному подмножеству. При этом в каждом подмножестве деления точки расположены достаточно плотно друг к другу и являются сходными по определенным признакам, в то время как точки, принадлежащие разным подмножествам, разнородны. Эти точки могут быть переменными, объектами, индивидуумами и другими величинами, которые содержатся в матрице исходных данных. Таким образом, с помощью кластерного анализа осуществляется группировка первичных данных, что составляет основу дальнейшей работы с полученной информацией [4].

Методы кластерного анализа классифицируются по следующим признакам [10]:

- способу обработки данных (иерархические, неиерархические);
- способу анализа данных (четкие и нечеткие);
- количеству применений алгоритмов кластеризации (с одноэтапной, многоэтапной кластеризацией);
- объему данных (масштабируемые, не масштабируемые);
- времени выполнения кластеризации (потоковые, не потоковые).

Применение кластерного анализа в общем виде сводится к следующим этапам:

1. Отбор выборки объектов для кластеризации.
2. Определение множества переменных, по которым будут оцениваться объекты в выборке. При необходимости – нормализация значений переменных.
3. Вычисление значений меры сходства между объектами.
4. Применение метода кластерного анализа для создания групп сходных объектов (кластеров).
5. Представление результатов анализа.

Рассмотрим пример иерархического кластерного анализа.

Исходным шагом при практической реализации кластерного анализа является формирование матрицы наблюдений.

Допустим, у нас имеется множество объектов $(X_1,X_2,..,X_n)$. Каждый из n объектов описывается некоторым множеством наблюдаемых и измеряемых показателей или характеристик.

Вышеуказанную матрицу наблюдений, обозначив ее через X, можно представить следующим образом:

$$X = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ x_{21} & x_{22} & \dots & x_{2m} \\ \dots & \dots & \dots & \dots \\ x_{n1} & x_{n2} & \dots & x_{nm} \end{bmatrix},$$

где n – число объектов, m – число показателей.

Задача кластерного анализа заключается в том, чтобы на основании данных, содержащихся в матрице X, разбить множество объектов $(X_1,X_2,..,X_n)$ на подмножества так, чтобы каждый объект принадлежал одному и только одному подмножеству разбиения и чтобы объекты, принадлежащие одному и тому же подмножеству, были сходными, в то время как объекты, принадлежащие разным подмножествам, были разнородными. Стоить отметить, что признаки включенные в матрицу наблюдений могут совершенно различными, поскольку описывают разные свойства объектов. Кроме того, различаются их единицы измерения, что еще более затрудняет их сопоставление.

Важнейшим понятием для количественного отражения сходства пары объектов является показатель (метрика) близости между ними. С учетом особенности информационных систем и простоты вычисления евклидово расстояние (квадрат евклидова расстояния) является наиболее удобной метрикой. Квадрат евклидова расстояния между объектами может быть рассчитан по формуле [8]:

$$d(X_i, X_j) = \sum_{l=1}^{k} \left(x_{il} - x_{jl}\right)^2,$$

где x_{il}, x_{jl} – величина компоненты с показателем l i-го и j-го объекта (l=1,2..,k; i,j=1,2,..,n); $d(X_i,X_j)$ – расстояние между любой парой исследуемых объектов (X_1,X_2,..,X_n).

Результаты расчетов мер близости могут быть представлены в виде симметричной матрицы расстояний D^2 [9]:

$$D^2 = \begin{bmatrix} 0 & d_{12}^2 & d_{13}^2 & \dots & d_{1n}^2 \\ d_{21}^2 & 0 & d_{23}^2 & \dots & d_{2n}^2 \\ d_{31}^2 & d_{32}^2 & 0 & \dots & d_{3n}^2 \\ \dots & \dots & \dots & 0 & \dots \\ d_{n1}^2 & d_{n2}^2 & d_{n3}^2 & \dots & 0 \end{bmatrix}.$$

При этом вначале элементы разбиваемого множества рассматриваются как отдельные кластеры, то есть все множество (X_1,X_2,..,X_n) рассматривается как множество кластеров $\{X_1\},\{X_2\},\dots,\{X_j\},\dots,\{X_n\}$.

Далее объединяются два самых близких кластера. Близость определяется в смысле минимума квадрата евклидова расстояния между объектами:

$$\min\left\{d_{ik}^2\right\}, j \neq k.$$

Пусть это будут кластеры $\{X_j\}$ и $\{X_k\}$. С помощью объединенных кластеров образуется новый кластер. Таким образом, новое множество кластеров, состоящее уже из (n – 1) элементов, будет $\{X_1\},\{X_2\},\dots,\{X_j+X_k\},\dots,\{X_n\}$. Повторяя процесс, получим последовательные множества кластеров, состоящие из (n – 2), (n – 3) и т. д. кластеров. По завершению этой процедуры получится кластер, состоящий из n объектов и совпадающий с первоначальным множеством $\{X_1\},\{X_2\},\dots,\{X_j\},\dots,\{X_n\}$.

Выбор числа кластеров, на котором прекращается работа алгоритма, может быть осуществлен лицом, принимающим решение. Основным соображением при выделении какой-либо группы в качестве кластера является ее устойчивость на протяжении нескольких шагов алгоритма. Целесообразно принимать во внимание расстояние между объединяющимися группами. Если для нескольких шагов расстояние между объединяющимися группами остается примерно одинаковым, а затем резко увеличивается, то это может быть признаком того, что объединяются два самостоятельных кластера [6].

Приведем пример вышеописанного алгоритма.

Для простоты возьмем информационную систему, каждый элемент которой описываются двумя параметрами. Этими параметрами могут быть, к примеру, вероятности реализации двух угроз информационной безопасности, выраженные в процентах. Предположим, что матрица наблюдений для 10 объектов имеет вид:

$$X = \begin{bmatrix} 12 & 10 \\ 3 & 43 \\ 14 & 8 \\ 33 & 4 \\ 28 & 7 \\ 10 & 11 \\ 33 & 9 \\ 5 & 35 \\ 9 & 8 \\ 1 & 51 \end{bmatrix}.$$

Пронумеруем объекты информационной системы от 1 до 10 в соответствии с исходной матрицей. Матрица квадратов евклидовых расстояний D_1^2 соответствующая первой итерации расчетов (исходя из ее симметричности), будет следующей:

	1	2	3	4	5	6	7	8	9	10
1	0	1170	8	477	265	5	442	674	13	1802
2		0	1346	2421	1921	1073	2056	68	1261	68
3			0	377	197	25	362	810	25	2018
4				0	34	578	3233	1745	592	3233
5					0	340	29	1313	362	2665
6						0	533	601	10	1681
7							0	1460	577	2788
8								0	745	272
9									0	1913
10										0

Результатом работы алгоритма кластеризации для приведенных 10-ти элементов информационной системы будет является разбиение на 3 кластера, а именно: {1,3,6,9},{2,8,10},{4,5,7}. Из этого следует, что данные группы объектов обладают сходными характеристиками, а это играет важную роль при решении задачи оценки и управления рисками информационной системы.

Вообще, рассматривая различные методы кластерного анализа, можно выделить общий ряд преимуществ для его использования применительно к анализу и оценке рисков в СМИБ.

Кластерный анализ позволяет разбить исследуемое пространство на подпространства (кластеры), где параметры выбранной модели статистически однородны [4]. Данное свойство полезно при сегментации рисков в кластер (рис. 1). Это позволяет выделить однородные группы рисков с различными показателями, а также выделить существенные риски, что будет полезно для анализа развития динамики рисков на предприятии. Выделение классов по уровню риска

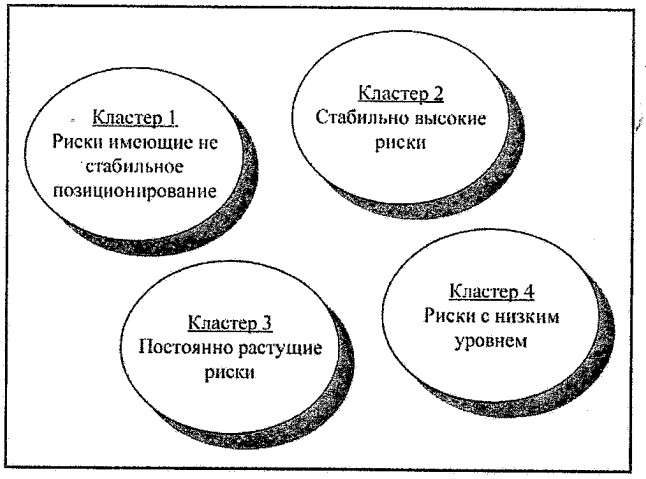


Рис. 1. Пример разбиения на кластеры информационных рисков

будет способствовать адекватному выбору стратегии управления рисками для различных классов.

Достоинство кластерного анализа применительно к СМИБ в том, что он позволяет производить разбиение объектов не по одному параметру, а по целому набору признаков. Данное свойство полезно, так как информационные риски зависят от большого множества факторов (источники угроз, уязвимости, вероятность угрозы, ценность актива и т. д.). При оценке рисков информационных систем в ряде случаев возникает задача деления элементов систем на классы в зависимости от значений, выбранных в качестве классифицирующих характеристик. Такими характеристиками, например, может стать время эксплуатации элемента и величина ущерба при его отказе и т. д.

Кроме того, кластерный анализ позволяет рассматривать достаточно большой объем информации и резко сокращать, сжимать большие массивы информации, делать их компактными и наглядными [2]. Поэтому, его целесообразно применять в достаточно крупных организациях и компаниях, где процесс анализа и управлениями рисками довольно трудоемок.

Кластерный анализ в отличии от большинства математико-статистических методов не накладывает никаких ограничений на вид рассматриваемых объектов, и позволяет рассматривать множество исходных данных практически произвольной природы. Это свойство полезно при применении комбинированных методов оценки рисков, где используется качественные и количественные показатели. Например, в методике OCTAVE применяются опросные листы для составления проблемно-ориентированных таблиц, где используются различные типы данных. Анализ будет особенно полезен для разбиения мнений экспертов при отсутствии их согласованности. Группировка таких данных кластерным методом, позволит повысить объективность полученных результатов.

Данный вид анализа также позволяет проводить изучение вероятностных характеристики процесса переходов из кластера в кластер. Это свойство особенно ценно при выборе стратегии обеспечения ИБ на предприятии, а также при анализе эффективности внедрённых контрмер. Например, эффективность можно оценить, рассматривая вероятности перехода рисков из кластера "высокие риски" в кластер "низкие риски" и т. д. Следует отметить, что кластерный анализ можно использовать циклически, что согласуется с принципом цикличности процесса анализа рисков по модели PDCA.

При применении кластерного метода в оценке рисков СМИБ следует учитывать следующие особенности:

1. Состав и количество кластеров зависит от выбираемых критериев разбиения. Следует учесть, что состав и количество кластеров для различных типов предприятий будет различно. Поэтому целесообразно предусмотреть так называемые "профили" для различных типов предприятий с характерными отличительными признаками.

2. Основным критерием качества и обоснованности полученного разбиения является содержательный анализ результатов, основанный на осмыслении исследователем возможных причинных механизмов обособления полученных групп объектов. Для оценки рисков информационной безопасности может использоваться подход, в котором каждая итерация кластеризации должна быть оценена экспертом.

3. Признаки, включенные в матрицу наблюдений, неоднородны, поскольку описывают разные свойства объектов. Необходимо выполнять предварительное преобразование, которое заключается в стандартизации признаков. Стандартизация, таким образом, представляет собой переход к некоторому единообразному описанию для всех признаков, к введению новой условной единицы, допускающей формальное сопоставление объектов.

4. При сведении исходного массива данных к более компактному виду могут возникать определенные искажения, а также могут теряться индивидуальные черты отдельных объектов за счет замены их характеристиками обобщенных значений параметров кластера. Например, при оценке различных активов в денежном выражении объекты могут быть сгруппированы по финансовому ущербу, при этом не будут учтены различия влияния на безопасность других объектов и т. д. По мнению авторов, данный недостаток является неизбежной "жертвой" при использовании данного метода. Задача разработчика системы минимизировать эти потери.

5. Задача кластеризации относится к статистической обработке. При этом основным недостатком является зависимость от объема накопленной статистики в виде экспертных или количественных оценок.

Приведенный анализ указывает на тот факт, что при "поверхностном" рассмотрении конкретной системы (предприятия) велика вероятность неточной кластеризации для оценки рисков ИБ. Поэтому универсальные программные продукты, используемые для оценки рисков ИБ с использованием кластеризации, предположительно могут иметь много неточностей, которые будут

негативно отражаться на конечном результате. Целесообразно использование кластерного анализа в крупных организациях, где существуют схожие по типам риски в различных информационных системах. Для извлечения максимального эффекта от использования кластерного анализа необходимо предусмотреть так называемые "профили" для различных типов предприятий с характерными отличительными признаками группируемых показателей.

Список литературы

1. Астахов А.М. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.
2. Барсегян А. и др. Анализ данных и процессов: Учебное пособие. СПб: БВХ-Питербург, 2009.
3. Бериков В.С., Лбов Г.С. Современные тенденции в кластерном анализе / Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению "Информационно-телекоммуникационные системы", 2008. 26 с.
4. Доценко К.А., Пшенецкий С.П. Подход к построению модели систем менеджмента информационной безопасности // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. Электронный ресурс: http://ej.kubagro.ru/2009/09/pdf/05.pdf
5. Кунакова Н. Описание классификации угроз. Электронный ресурс: http://www.dsec.ru /about/articles/dsecct/
6. Кластерный и факторный анализ. Электронный ресурс: http://www.dea-analysis.ru/clustering-7.htm
7. Сайт Банковского обозревателя. Электронный ресурс: http://bankibank.ru/publication/ 295.html
8. Берсегян А.А., Куприянов М.С., Степаненко В.В., Холод И.И. Технологии анализа данных: *Data Mining, Visual Mining, Text Mining, OLAP* / 2-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2007. 384с.
9. Шмойлова Р.А., Минашкин В.Г., Садовникова Н.А., Шувалова Е.Б. Теория статистики. Учебник / 5-е изд. М.: Финансы и статистика, 2011. 656 с.
10. Шимко П.Д. Оптимальное управление экономическими системами: Учеб. пособие. СПб.: Издательский дом "Бизнес-пресса", 2004. 240 с.

References

1. Astakhov A.M. Iskusstvo upravleniya informatsionnymi riskami [The art of managing information risk]. M.: DMK Press [Moscow: Publishing House "DMK Press"]. 2010. 312 p.
2. Barsegyan A. i dr. Analiz dannykh i protsessov: Uchebnoe posobie [Analysis of the data and processes: Textbook]. SPb: BVKh-Piterburg [St. Petersburg: Publishing House "BVKh-Piterburg"]. 2009.
3. Berikov V.S., Lbov G.S. Sovremennye tendentsii v klasternom analize [Current trends in the cluster analysis]. *Vserossiyskiy konkursnyy otbor obzorno-analiticheskikh statey po prioritetnomu napravleniyu "Informatsionno-telekommunikatsionnye sistemy"* [All-competitive selection of an overview and analytical articles on the priority area of "Information systems"]. 2008. 26 p.
4. Dotsenko K.A., Pshenetskiy S.P. Podkhod k postroeniyu modeli sistem menedzhmenta informatsionnoy bezopasnosti [The approach to the construction of a model of information security management systems]. *Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta* [Polythematic power electronic scientific journal of the Kuban State Agrarian University]. *Available at:* http://www.dsec.ru /about/articles/dsecct/
5. Kunakova N. *Opisanie klassifikatsii ugroz* [Description of the classification of threats]. *Available at:* http://www.dsec.ru / about/articles/dsecct/
6. *Klasternyy i faktornyy analiz* [Cluster and factor analysis]. *Available at:* http://www.dea-analysis.ru/clustering-7.htm
7. *Sayt Bankovskogo obozrevatelya* [Banking's browser]. *Available at:* http://bankibank.ru/publication/ 295.html
8. Bersegyan A.A., Kupriyanov M.S., Stepanenko V.V., Kholod I.I. *Tekhnologii analiza dannykh* [Data mining technology]. SPb.: BKhV-Peterburg [St. Petersburg: Publishing House "BKhV-Peterburg"]. 2007. 384 p.
9. Shmoylova R.A., Minashkin V.G., Sadovnikova N.A., Shuvalova E.B. *Teoriya statistiki. Uchebnik, 5-e izd.* [Theory of Statistics. Textbook]. M.: Finansy i statistika [Moscow: Publishing House "Finance and Statistics"]. 2011. 656 p.
10. Shimko P.D. *Optimalnoe upravlenie ekonomicheskimi sistemami*: Ucheb. posobie. SPb.: Izdatelskiy dom "Biznes-pressa", 2004. 240 p.

Информация об авторах

Лось Алексей Борисович, канд. техн. наук, доцент
E-mail: alos@hse.ru
Кабанов Артем Сергеевич, канд. техн. наук, доцент
E-mail: kabanov_as@mail.ru
Трунцев Вадим Игоревич
Московский институт электроники и математики Национального исследовательского университета "Высшая школа экономики"
109028, Москва, Российская Федерация, Трехсвятительский пер., дом 3

Information about the authors

los Aleksey Borisovich, Cand. of Techn. Sciences, Associate Professor
E-mail: alos@hse.ru
Kabanov Artem Sergeevich, Cand. of Techn. Sciences, Associate Professor
E-mail: kabanov_as@mail.ru
Truntsev Vadim Igorevich
Moscow Institute of Electronics and Mathematics National Research University "Higher School of Economics"
109028, Moscow, Russian Federation, Trehsvyatitelsky per., 3