СПОСОБ ПРОВЕДЕНИЯ КЛАСТЕРНОГО АНАЛИЗА УГРОЗ ИБ ПРЕДПРИЯТИЙ

Абзалов Вадим Шамилевич

магистрант, Казанский национальный исследовательский технологический университет, РФ, г. Казань

Ведение. Из-за реализованных угроз информационной безопасности предприятия часто могут потерять как материальные ресурсы, так и репутацию, поскольку на предприятиях хранится большое количество конфиденциальной информации. Под угрозой информационной безопасности понимается потенциально возможное воздействие на информацию, которое прямо или косвенно наносит ущерб безопасности [2]. Для уменьшения ущерба от угроз можно провести их кластеризацию.

С помощью разных методов кластеризации возможна группировка элементов наиболее оптимальным способом. Спектр применений кластерного анализа очень широк: его используют в различных дисциплинах и сферах деятельности, при решении разнообразных прикладных задач [1].

Кластеризацию угроз ИБ предприятий целесообразно проводить, опираясь на статистические данные по уже реализованным угрозам. Целью данной статьи является проведение анализа данных о реализованных угрозах ИБ путем кластеризации, позволяющей получить группы угроз, которые приводят к наиболее негативным последствиям, и уменьшить ущерб от их реализации.

Описание способа кластеризации угроз информационной безопасности. Основными последствиями инцидентов ИБ считаются моральный и материальный ущерб, а также затраченное время на восстановление данных, во время которых работа предприятия может быть нарушена.

Пусть на предприятии было выявлено N инцидентов ИБ во время некоторого интервала времени. В роли объектов кластеризации используются угрозы информационной безопасности. Каждая i – ая реализованная угроза описывается вектором $v_i = (u_i,\tau_i)$, где u_i – ущерб от реализации угрозы, τ_i – длительность устранения последствий.

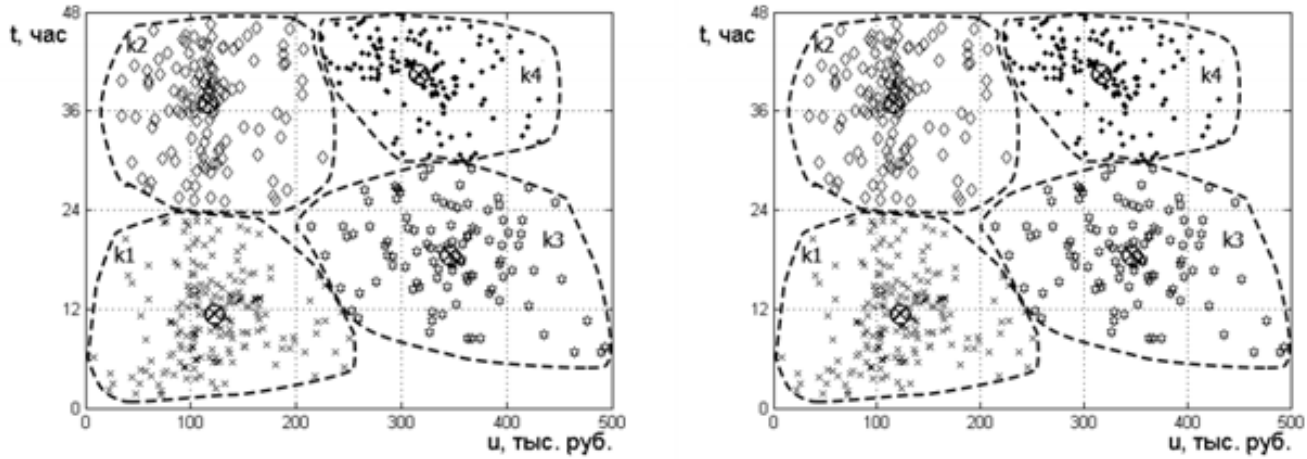
По окончании кластеризации множество угроз $G = \{v_i\}_{i=1}^{N}$ будет поделено на K кластеров.

Анализ полученного разбиения на кластеры дает возможность поделить угрозы на группы с установлением самых опасных угроз, которые при реализации приводят к наиболее негативным последствиям и наносят наибольший ущерб. Значит, специалисты по ИБ предприятия смогут направить все свои усилия на защиту от угроз с наибольшими негативными последствиями.

Результаты реализации. В качестве исходных данных были выбраны 409 инцидентов ИБ, произошедших на определенном предприятии. Кластерный анализ проводился с использованием методов k-means и k-medoids с различным количеством кластеров [3]. Результаты кластерного анализа приведены на рисунке и таблице.

По полученным результатам можно сделать вывод, что методы k-medoids и k-means при трех и

четырех кластерах дают одинаковое разбиение. Но наиболее предпочтительным является метод k-medoids, так как время кластеризации при его использовании меньше.



а) б)

Рисунок. Результаты кластеризации: (а) – методом k-means, 4 кластера; (б) – методом k-medoids, 4 кластера

Таблица.

Результаты кластеризации

Метод кластеризации	Количество кластеров	Количество угроз в кластерах	Время кластер
k-means	3	163/169/77	0.842
k-medoids	3	164/168/77	0.112
k-means	4	129/99/85/96	0.806
k-medoids	4	130/99/85/95	0.099

При четырех кластерах возможно распределение угроз на четыре группы:

1) Небольшие потери с быстрым устранением последствий (k1);

2) Небольшие потери с долгим устранением последствий (k2);

3) Большие потери с быстрым устранением последствий (k3);

4) Большие потери с долгим устранением последствий (k4).

Т.к. в кластере k1 намного больше угроз, чем в остальных, значит большое количество инцидентов ИБ ликвидируется за короткое время с небольшими потерями. Улучшить ситуацию можно переносом части реализованных угроз:

– из кластера k4 в k3, введя меры для ускорения ликвидации последствий;

– из k4 в k2 путем введения мер повышения эффективности защиты информации и

уменьшения потерь от реализованных угроз.

Заключение. Описанный способ кластеризации угроз информационной безопасности позволил провести анализ системы защиты предприятий, выявить подходы к уменьшению потерь от уязвимости и пути повышения уровня защиты.

Список литературы:

1. Зайцев А.С., Малюк А.А. Разработка классификации внутренних угроз информационной безопасности посредством кластеризации инцидентов // Безопасность информационных технологий. – 2016. – № 63. – С. 20-33.

2. Тюрин А.Г., Зуев И.О. Кластерный анализ, методы и алгоритмы кластеризации // Вестник МГТУ МИРЭА. – 2014. – № 2. – С. 86-97.

3. Madhulatha T.S. An overview on clustering methods // IOSR Journal of Engineering. – 2012. – Vol. 2. № 4. – P. 719–725.