Инженерный вестник Дона, №1 (2018)
ivdon.ru/ru/magazine/archive/n1y2018/4803

Подход к кластеризации угроз информационной безопасности предприятий

Д.Ю. Куринных, А.Р. Айдинян, О.Л. Цветкова

Донской государственный технический университет, Ростов-на-Дону

Аннотация: В результате реализации угроз информационной безопасности предприятия терпят существенные материальные и репутационные потери, поскольку на предприятиях хранится большое количество информации, в том числе конфиденциальной. В работе предлагается подход к кластеризации реализованных угроз информационной безопасности предприятий. Проведен анализ данных о реализованных угрозах путем кластеризации разными методами с различным количеством кластеров, для выявления наилучших результатов разделения угроз наилучшим образом. Реализованные угрозы описываются ущербом, который возник от реализации угрозы и длительности устранения последствий реализации угрозы. Кластеризация позволяет выявить общие характеристики угроз в каждой группе и определить возможность перевода возникающих угроз в группу с меньшим ущербом. Показано, что имеется возможность ликвидации последствий, возникших в результате реализации угроз информационной безопасности, путем снижения материальных потерь и уменьшения времени восстановления за счет введения организационных и технических мер.
Ключевые слова: информационная безопасность, угроза информационной безопасности, ущерб от реализации угрозы информационной безопасности, кластерный анализ.

Введение и постановка задачи

В настоящее время в информационных системах предприятий и организаций хранится и обрабатывается большое количество информации, которая подвержена воздействию различных факторов и условий, создающих опасность утечки и порчи конфиденциальной информации [1, 2]. Под угрозой информационной безопасности понимается потенциально возможное воздействие на информацию, которое прямо или косвенно наносит ущерб безопасности. Организация мероприятий по обеспечению информационной безопасности должна иметь комплексный характер и основываться на анализе возможных последствий от реализации потенциальных угроз [3, 4]. При этом необходимо выполнить ряд работ по выявлению актуальных угроз информационной безопасности, определению источников этих угроз и факторов, способствующих их проявлению, оценке вероятностей реализации

© Электронный научный журнал «Инженерный вестник Дона», 2007–2018

угроз [5]. Анализ результатов, полученных на этих этапах, позволит сформулировать рекомендации по внедрению организационных мер, технических и программно-аппаратных средств защиты информации.

Кластерный анализ используется при решении различных прикладных задач [6, 7]. В работе предлагается подход к проведению кластерного анализа угроз информационной безопасности, позволяющая получить группы сходных угроз и выявить возможность уменьшения ущерба от их реализации.

Описание подхода к кластеризации угроз информационной безопасности

Основными последствиями реализации угроз информационной безопасности являются материальный и моральный ущерб, и необходимость временных затрат на восстановление данных, во время которых функционирование бизнес-процессов предприятия может быть нарушено. В качестве ущерба, возникающего в результате реализации угрозы, рассматривается [8]:

— материальный ущерб, связанный с разглашением персональных данных;

— материальный и моральный ущерб от разглашения защищаемой информации;

— материальный ущерб от необходимости восстановления утраченной или модифицированной информации;

— материальный ущерб от невозможности выполнения деятельности организации;

— материальный и моральный ущерб от нарушения установленных связей и отношений, ухудшению репутации компании.

Пусть предприятие подверглось N реализованным угрозам в течение некоторого временного интервала. Информация о каждой i-ой угрозе описывается вектором $v_i = (t_i, u_i, \tau_i)$, где t_i — время, когда была реализована

© Электронный научный журнал «Инженерный вестник Дона», 2007–2018

угроза, u_i — ущерб, который возник от реализации угрозы, τ_i — длительность устранения последствий реализации угрозы.

В качестве объектов кластеризации предлагается использовать угрозы информационной безопасности, описываемые векторами $v_i = (u_i, \tau_i)$.

В результате решения задачи кластеризации множество угроз $G = \{g_i\}_{i=1}^{N}$ будет разделено на K кластеров. В качестве меры близости для определения схожести объектов и различия кластеров предлагается использовать декартово расстояние между объектами $d(g_i, g_j)$, $i, j = 1,..., N$.

Анализ полученного разбиения множества угроз информационной безопасности на кластеры позволит разделить угрозы на группы с выявлением тех угрозы, реализация которых приводит к наиболее негативным последствиям и наносит наибольший материальный ущерб. Таким образом, специалисты службы безопасности предприятия могут предпринять меры по защите информации, направить усилия на обеспечение защиты от угроз с наибольшими негативными последствиями.

Результаты реализации предлагаемого подхода

В качестве исходных данных рассматривались 523 угрозы, реализованные на анализируемом предприятии. Кластеризация осуществлялась методами k-means и k-medoids с различным количеством кластеров [9, 10]. Результаты кластеризации приведены на рис. 1 и таблице 1.

Из полученных результатов видно, что методы k-medoids и k-means при трех и четырех кластерах дают практически одинаковые результаты. Однако метод k-medoids является более предпочтительным в связи с меньшими вычислительными затратами.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2018

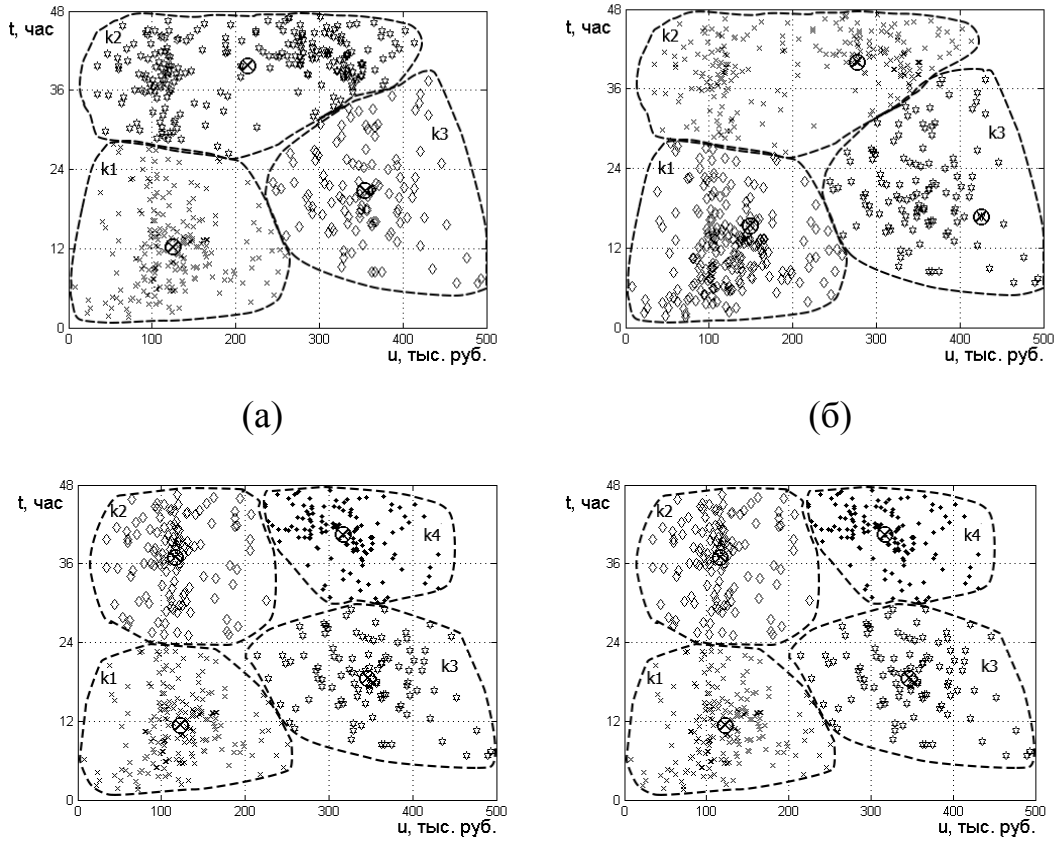

Рис. 1 — Результаты кластеризации: (а) — методом k-means, 3 кластера; (б) — методом k-medoids, 3 кластера; (в) — методом k-means, 4 кластера; (г) — методом k-medoids, 4 кластера

Таблица № 1

Результаты кластеризации

№ п/п	Метод кластеризации	Количество кластеров	Количество угроз в кластерах	Время кластеризации, с
1	k-means	3	193/208/122	0.921
2	k-medoids	3	193/210/124	0.126
3	k-means	4	179/127/101/116	0.853
4	k-medoids	4	180/127/101/115	0.106
5	k-means	5	172/114/73/66/98	0.785
6	k-medoids	5	117/71/105/123/107	0.123

© Электронный научный журнал «Инженерный вестник Дона», 2007–2018

Деление на четыре кластера позволило получить логичное распределение всех реализованных угроз на предприятиях на четыре группы:

1) Относительно небольшие потери от реализованных угроз с небольшим временем восстановления (k1);

2) Относительно небольшие потери от реализованных угроз с большим временем восстановления (k2);

3) Большие потери от реализованных угроз с небольшим временем восстановления (k3);

4) Большие потери от реализованных угроз с большим временем восстановления (k4).

В кластере k1 приблизительно в 1,5 раза больше угроз, чем в остальных. Это говорит о том, что большое количество реализованных угроз ликвидируется за небольшое время с относительно небольшими потерями. Однако имеется возможность улучшения ситуации путем переноса части реализованных угроз:

— из кластера k4 в k3 путем введения мер для уменьшения времени ликвидации реализованных угроз;

— переноса части реализованных угроз из кластера k4 в k2 путем введения мер повышения эффективности защиты информации и, соответственно, уменьшения потерь от реализованных угроз.

Заключение

Предложенная методика кластеризации угроз информационной безопасности позволила провести анализ системы защиты предприятий, выявить подходы к уменьшению потерь от уязвимости и выявить пути повышения уровня защиты.

Литература

1. Papadimitriou P., Garcia-Molina H. Data Leakage Detection. URL: il-pubs.stanford.edu:8090/839/1/2008-23.pdf.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2018

2. Айдинян А.Р., Цветкова О.Л. Подход к оценке DLP-систем с использованием средств нечеткой логики // Инженерный вестник Дона, 2017, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2017/4432.

3. Айдинян А.Р., Цветкова О.Л., Кикоть И.Р., Казанцев А.В., Каплун В.В. О подходе к оценке информационной безопасности предприятия // Системный анализ, управление и обработка информации: сб. тр. V Междунар. науч. семинара, п. Дивноморское, 2-6 окт. — Ростов н/Д: ДГТУ, 2014. — С. 109-111.

4. Цветкова О.Л., Заслонов С.А. Имитационное моделирование зависимости информационной безопасности организации от области деятельности // Вестник ДГТУ. — 2017. — Т. 17, № 4. — С. 116-121.

5. Цветкова О.Л., Айдинян А.Р. Интеллектуальная система оценки информационной безопасности предприятия от внутренних угроз // Вестник компьютерных и информационных технологий. — 2014. — № 8(122). — С. 48–53.

6. Гранков М.В., Аль-Габри В.М., Горлова М.Ю. Анализ и кластеризация основных факторов, влияющих на успеваемость учебных групп вуза // Инженерный вестник Дона, 2016, №4. URL ivdon.ru/ru/magazine/archive/n4y2016/3775

7. Голубева А.О., Виноградова Г.Л. Кластеризация процессов промышленного предприятия в методе их адаптации под заказ // Инженерный вестник Дона, 2012, №2. URL ivdon.ru/ru/magazine/archive/n2y2012/829

8. Артемов А.В. Информационная безопасность. Курс лекций. Орел: Литагент «МАБИВ», 2014. 51 с.

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

© Электронный научный журнал «Инженерный вестник Дона», 2007–2018

10. Hartigan J.A. Clustering Algorithms (Probability & Mathematical Statistics). John Wiley & Sons Inc. 1975. 369 p.

References

1. Papadimitriou P., Garcia-Molina H. Data Leakage Detection. URL: il-pubs.stanford.edu:8090/839/1/2008-23.pdf.

2. Ajdinyan A. R., Tsvetkova O.L., Inženernyj vestnik Dona (Rus), 2017, № 4 URL: ivdon.ru/ru/magazine/archive/n4y2017/4432.

3. Ajdinyan A.R., TSvetkova O.L., Kikot' I.R., Kazantsev A.V., Kaplun V.V. Sistemnyj analiz, upravlenie i obrabotka informatsii: sb. tr. V Mezhdunar. nauch. Seminara, Divnomorskoe, 2-6 okt, Rostov n/D: DGTU, 2014. pp. 109-111.

4. TSvetkova O.L., Zaslonov S.A. Vestnik DGTU. 2017. Vol. 17. № 4. pp. 116–121.

5. TSvetkova O.L., Ajdinyan A.R. Vestnik komp'yuternykh i informatsionnykh tekhnologiy. 2014. № 8(122). pp. 48–53.

6. Grankov M.V., Al'-Gabri V.M., Gorlova M.Yu. Inženernyj vestnik Dona (Rus), 2016, №4. URL ivdon.ru/ru/magazine/archive/n4y2016/3775.

7. Golubeva A.O., Vinogradova G.L. Inženernyj vestnik Dona (Rus), 2012, №2. URL ivdon.ru/ru/magazine/archive/n2y2012/829.

8. Artemov A.V. Informatsionnaya bezopasnost'. Kurs lektsiy [Information security. Course of lectures]. Orel. 2014. 51 p.

9. Madhulatha T.S. An overview on clustering methods. IOSR Journal of Engineering. Apr. 2012. Vol. 2. №. 4. pp. 719–725.

10. Hartigan J.A. Clustering Algorithms (Probability & Mathematical Statistics). John Wiley & Sons Inc. 1975. 369 p.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2018