УДК 656.072

МЕТОД НЕЧЕТКОЙ КЛАСТЕРИЗАЦИИ ДЛЯ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Курманбай Айгерим Кайраткызы, студент группы 17В41, II курс
Научный руководитель: Разумников С.В.
Юргинский технологический институт (филиал)
Томского политехнического университета

Для решения проблемы отсутствия готовых данных и сложности поиска оптимального значения оценки рисков информационной безопасности в данной статье рассматривается относительно новый метод информационной меры и нечеткой кластеризации в оценке рисков информационной безопасности. Новый метод определяет количество факторов риска всех данных и зависимость степени безопасности при вычислении взаимной информации. Затем поиск оптимального значения для каждой степени риска определяется как центр точек по K-means алгоритму кластеризации, используется K-means алгоритм кластеризации для классификации данных.

Этот метод прост в реализации, легко рассчитывается и позволяет избежать проблемы чувствительности к начальному значению, нелинейности и сложности оценки рисков информационной безопасности. Экспериментальные результаты показывают эффективность данного метода. Ключевые слова: информационная безопасность, оценка рисков, информационные измерения, нечеткая кластеризация.

С развитием Internet-технологий и электронной коммерции с каждым днем появляется все больше угроз безопасности информации. Сегодня организации все чаще используют информацию в бизнес-процессах, для облегчения управленческих решений и ведения бизнеса. Зависимость от информации в бизнес-среде крайне велика, где множество торговых операций осуществляется в электронном виде через Internet.

В информационной безопасности методики оценки рисков появились с целью прогнозирования возможного ущерба.

В настоящее время основные научные достижения в области оценки рисков информационной безопасности включают известные методы: OCTAVE-метод [1], CRAMM5 [2], PRA [3], и т. д. Но эти стандарты и методы имеют некоторые недостатки, некоторые из них являются только качественными методами анализа, некоторые — только количественными, громоздкими для реализации.

Оценка рисков информационной безопасности имеет некоторые характеристики, такие как нелинейность, сложность применения, характеристики, обусловленные некоторыми ограничениями на

использование традиционных моделей для проведения оценки рисков информационной безопасности [4].

Эти традиционные методы оценки массу субъективных проблем и неясностей, поэтому они более сложны в применении. В данной статья рассмотрен новый метод оценки рисков информационной безопасности, основанный на комбинации вычисления взаимной информации и K-means алгоритма кластеризации [5].

Для того чтобы добиться эффективной оценки уровня рисков информационной безопасности, новый метод определяет количество факторов риска всех данных и зависимость степени безопасности при вычислении взаимной информации.

Затем осуществляется поиск оптимального значения для каждой степени риска как центр точек K-means алгоритма кластеризации и используется K-means алгоритм кластеризации для классификации данных.

Риск информационной безопасности определяется как произведение финансовых потерь (ущерба), связанных с инцидентами безопасности, и вероятности того, что они будут реализованы. Данное определение подходит при рассмотрении различных архитектур информационных систем. Информация может существовать в различных формах. Она может быть написана на бумаге, храниться в электронном виде, пересылаться по почте или с использованием электронных средств, транслироваться на экране или обсуждаться в разговоре [6]. Какие бы формы информация ни принимала, она всегда должна быть защищена соответствующим образом. Оценка рисков информационной безопасности, с точки зрения управления рисками, анализ систематически подвергающихся угрозам и существующим уязвимостям информационных систем и технологий научными методами и средствами [4].

Оценка потенциального ущерба в случае угрожающих событий проведена и выдвинуты контрмеры против угроз для предотвращения и урегулирования рисков информационной безопасности, а также контроль рисков на приемлемом уровне таким образом, чтобы максимально обеспечить безопасность информации [5]. Оценка рисков информационной безопасности состоит из трех основных этапов:

- идентификация угроз,
- идентификация уязвимостей,
- идентификация активов

Элементы оценки рисков информационной безопасности. Процесс оценки риска информационной безопасности выглядит следующим образом:

определение информационных активов: установление ценности активов;

анализ угроз, определение вероятности угроз;

идентификация уязвимостей информационных активов, определение степени уязвимости;

вычисление вероятности наступления события по реализации угроз (использованию уязвимостей);

сочетание важности информационных активов и возможности возникновения инцидентов, выполняется расчет значения риска информационной безопасности для информационного актива.

Проиллюстрируем вычисление риска с помощью формулы:

Riskvalue = R (A, T, V) = R (L (T, V), F (Ca, Va)),(1)

где R — функция вычисления риска,

A — активы,

T — угрозы,

V — уязвимости,

Ca — стоимость активов, принесенная инцидентом,

Va — степень уязвимости,

L — возможность угрозы привести к инцидентам с помощью уязвимостей,

F — потери, вызванные событиями безопасности.

Определение значения риска связано с результатами оценки риска и выработкой мер по контролю риска, поэтому это является важным и сложным этапом в процессе оценки риска. Это основной вопрос этого исследования [7].

В целях предотвращения несанкционированного доступа организации используют различные контрмеры для защиты своих активов. Но даже благодаря применению контрмер и управлению информационной безопасностью активы зачастую не в полной мере защищены от угроз из-за недостатка контроля.

Таким образом, оценка рисков является одним из важнейших шагов в управлении рисками информационной безопасности. На практике оценка рисков информационной безопасности является довольно сложным и полным неопределенностей процессом. Неопределенности, существующие в процессе оценки, являются основным фактором, влияющим на эффективность оценки риска информационной безопасности. Поэтому они должны быть приняты во внимание при оценке рисков. Однако большинство существующих подходов имеют некоторые недостатки по обработке неопределённости в процессе оценки.

Для того чтобы решить проблему оценки рисков информационной безопасности, связанную со сложностью определения оптимальных значений предложен новый метод оценки рисков информационной безопасности, основанный на вычислении взаимной информации и K-means алгоритме кластеризации, позволяющем эффективно оценивать уровни риска информационной безопасности.

Метод определяет степень количественной зависимости между факторами риска и уровнем информационной безопасности с вычислением взаимной информации. На каждом уровне риска, определяются оптимальные точки как начальные центры кластеров по алгоритму K-means, затем алгоритм кластеризации K-means классифицирует данные.

Этот метод может динамически регулировать центр кластера в соответствии с результатами кластеризации и вычисление значения взаимной

информации. Этот метод легко применять, он имеет меньше вычислений, чем традиционные методы. Метод позволяет предотвратить чувствительность к входным данным, нелинейность, сложность и другие проблемы оценки рисков информационной безопасности.

Список литература:

1. А. Астахов. Искусство управления рисками. GlobalTrust. 2009.
2. Козлова Е. А. Оценка рисков информационной безопасности с помощью метода нечеткой кластеризации и вычисления взаимной информации // Молодой ученый. — 2013. — №5. — С. 154-161.
3. Мишурин А. О. Подход к определению потребности общества в специалистах информационной безопасности с помощью математической модели противоборства сторон // Молодой ученый. — 2010. — №5. Т.1. — С. 92-95.
4. Османов А. А., Юдин Д. Е., Тринкин М. Г., Науменко В. В. Анализ проблем обеспечения информационной безопасности электронной коммерции [Текст] // Технические науки: проблемы и перспективы: материалы III междунар. науч. конф. (г. Санкт-Петербург, июль 2015 г.). — СПб.: Свое издательство, 2015. — С. 99-101.
5. Разумников С.В. Анализ возможности применения методов Octave, RiskWatch, Cramm для оценки рисков ИТ для облачных сервисов //Современные проблемы науки и образования. -2014 -№ 1. -С. 1. - Режим доступа: http://www.science-education.ru/115-12197.
6. Разумников С.В. Моделирование оценки рисков при использовании облачных ИТ-сервисов//Фундаментальные исследования. -2014 -№ 5-1. -С. 39-43.
7. Разумников С.В. Интегральная модель оценки эффективности и рисков облачных ИТ-сервисов для внедрения на предприятии // Фундаментальные исследования. - 2015 - №. 2-24. - С. 5362-5366.