Технологические основы построения интеллектуальных систем прогнозирования инцидентов информационной безопасности

В.Н. Соляной
Институт техники и цифровых технологий
Технологический университет
Г. Королев, МО, Россия
e-mail: solyanoy@ut-mo.ru

А.И. Сухотерин
Институт техники и цифровых технологий
Технологический университет
Г. Королев, МО, Россия
e-mail: sukhoterin@ut-mo.ru

Аннотация

Построение систем прогнозирования инцидентов информационной безопасности (ИБ) в настоящее время рассматривается как одна их сложных и важных задач стоящих перед руководством защищаемых информационных объектов в современных условиях ведения скрытой информационной войне как на межконтинентальных и континентальных пространств, так и в региональных и локальных сферах применения различных информационных систем. Системы прогнозирования, которые позволяют осуществлять сбор информации и по ключевым признакам ее анализировать с целью выявления инцидентов информационной безопасности в соответствии с заданным методом их обнаружения и реализуемой стратегии информационной безопасности, а также осуществлять ответные действия. Наличие разномасштабных защищаемых информационных систем требует выработки разных подходов по выбору технологических основ построения наиболее целесообразных систем прогнозирования инцидентов информационной безопасности. Целью данной статьи является обоснование технологических основ построения, прежде всего интеллектуальных систем прогнозирования инцидентов информационной безопасности как наиболее эффективных в постоянно усиливающихся скрытых угроз для критически важных информационных инфраструктур. В статье предложен интеллектуальный подход построения систем прогнозирования инцидентов информационной безопасности в интересах реализации на защищаемых информационных объектах упреждающей стратегии обеспечения ИБ [Малюк]. Использование методов интеллектуальной аналитики позволяет снизить вычислительную сложность построения систем прогнозирования инцидентов, возникающих в неизвестный момент времени и оперативно выработать ответные действия.

Ключевые слова: информационная безопасность; прогнозирование; интеллектуальные подходы; инциденты; информационная система; критическая инфраструктура; методы; модель.

1. Введение

Интеллектуальные системы прогнозирования инцидентов информационной безопасности представляют собой совокупность базы знаний и базы данных о произошедших инцидентов информационной безопасности, математических и логических методов работы и программных средств обеспечивающих сбор и обработку, анализ исходных данных в интересах прогнозирования инцидентов с целью выработки и принятия упреждающих управленческих решений по информационной безопасности. Поиск и своевременное выявление инцидентов информационной безопасности на основе предшествующих им возникновению различных аномальных активности рассматривается как одна из ключевых проблем в области информационной безопасности предприятий (организаций и учреждений). Такой поиск и выявление инцидентов в современных условиях реализуются различными подходами (методами). Используя новейшие информационные технологии обработки больших данных (Big Data) с различными методами обнаружения, распознавания и прогнозирования различных информационных ситуаций позволяют разрешать указанную выше проблему в области обеспечения информационной безопасности. Методы Big Data позволяют для анализа информационной обстановки задействовать и осуществлять сверку (на основе статистики) большого количества источников и прогнозировать возможные инциденты информационной безопасности с реализацией следующих технологий:

- обнаружения скрытых тенденций в больших наборах данных на основе их анализа;

-непосредственного прогнозирования различных ситуаций;

-вычислять вероятность любого возможного инцидента (исхода);

-оперативно получать желаемые результаты прогноза и др.

Наличия большого разнообразия в условиях и факторах защищаемых информационных системах для различных предприятий (организаций и учреждений) обуславливает привлечения разных алгоритмов построения целесообразных информационных систем прогнозирования инцидентов информационной безопасности.. Литература по данной тематике представлена многочисленными разработками и обуславливает актуальность исследований в современном мире В последнее время в сфере исследований были рассмотрены большое количество различных подходов для построения адаптированных информационных систем прогнозирования инцидентов информационной безопасности на основе: прогнозирования изменений параметров временных рядов [4] сигнатурный метод и поиск по ключевым признакам[15], нейронные сети автоматического распознавания ситуаций [4]. и др. Адаптивная информационная система прогнозирования при функционировании в недетерминированной среде позволяет подстраиваться под изменение условий и ограничения окружающей анализируемой информационной среды.

Анализ существующих решений отражает индивидуальность использования разработанных подходов под конкретную информационную ситуацию и используемые методы и системы прогнозирования. Следовательно, выявление и обоснование основ построения информационных систем прогнозирования инцидентов информационной безопасности с использованием различных условий и факторов функционирования защищаемых предприятий (организациях и учреждениях) является актуальной задачей.

2. Постановка задачи

Целью данной статьи следует рассматривать описание технологических основ построения интеллектуальных информационных систем прогнозирования инцидентов информационной безопасности для различных по масштабу деятельности предприятий (организаций и учреждений). Основной задачей работы является технологическое обоснование наиболее целесообразного подхода реализации с использованием метода интеллектуального анализа данных - нейросетевого прогнозирования.

Задачу исследования в данной постановке можно разделить на три уровня:

- стратегический уровень прогнозирования инцидентов. На данном уровне решается вопрос глобального прогнозирования (в интересах долгосрочного планирования информационной безопасности). Данная задача наиболее полно отражает потребности обеспечения информационной безопасности крупных распределенных предприятий (организаций и учреждений);
- тактический уровень прогнозирования инцидентов (в ходе краткосрочного планирования информационной безопасности). Данная задача прогнозирования тактического уровня сводится к решению задачи обеспечения информационной безопасности малых и средних предприятий (организаций и учреждениях) по масштабу своей деятельности;
- исполнительный (операционный) уровень прогнозирования инцидентов. Задача данного уровня прогнозирования наиболее характерна для обеспечения информационной безопасности отдельных защищаемых информационных объектов (комплексов) критически важной информационной инфраструктуры предприятий (организаций и учреждений).

В целом, для разрешения указанной задачи целесообразно рассмотреть с обоснованием наиболее возможные подходы реализации технологических основ формирования интеллектуальных систем прогнозирования инцидентов для сформулированных ранее уровнях информационной безопасности.

3. Структурные компоненты технологических основ построения систем прогнозирования инцидентов

Технологические основы построения интеллектуальных информационных систем прогнозирования инцидентов информационной безопасности предусматривают прежде всего обоснования: цели проектируемой системы; методов реализации; привлекаемых средств для построения и алгоритмы функционирования (рис.1).

Рисунок.1. Основы технологии (системы) прогнозирования инцидентов информационной безопасности

Прежде чем описывать каждый технологический компонент рассматриваемой интеллектуальной системы прогнозирования целесообразно сформулировать общую постановочную концепцию

разработки таких систем с учетом ключевых условий и факторов складывающейся информационной обстановки в интересах обеспечения информационной безопасности. Такой подход построения систем прогнозирования инцидентов базируется на вводимые в настоящее время понятия стратегий информационной безопасности с учетом рассматриваемых условий: оборонительная, наступательная и упреждающая стратегии [6].

Применительно к условиям реализации оборонительной стратегии информационной безопасности в качестве особенностей основ построения системы прогнозирования инцидентов следует рассматривать следующие положения (Табл.1).

Таблица 1. Особенности построения основ систем прогнозирования инцидентов при оборонительной стратегии информационной безопасности

Основы	**Особенности**	
Цели прогнозирования	Краткосрочное прогнозирование инцидентов (от суток до года)	
Возлагаемые функции	Внутренняя и внешняя оценка локальной и региональной информац. обстановки	Защита критического информац. ресурса локальных объектов
Решаемые задачи	Выявление нарушителей, угроз и рисков	
Методы прогнозирования	Регрессионный (трендовый) подход	
Виды моделей	Статистические	

Характерной особенностью реализации систем прогнозирования инцидентов для данного подхода являются рассмотрение прежде всего в качестве защищаемого информационного ресурса критических систем информационной инфраструктуры локальных и, в меньшей степени, региональных информационных объектов в пределах ареала функционирования конкретных объектов и обмена данными с другими взаимодействующими информационными объектами..

Применительно к условиям реализации наступательной стратегии информационной безопасности в качестве особенностей основ построения системы прогнозирования инцидентов следует рассматривать следующие положения (Табл.2).

Таблица 2. Особенности построения основ систем прогнозирования инцидентов при наступательной стратегии информационной безопасности

Основы	**Особенности**	
Цели прогнозирования	Среднесрочное прогнозирование инцидентов (от года до 3 лет)	
Возлагаемые функции	Внутренняя и внешняя оценка региональной информац. обстановки	Защита критического информац. ресурса регионально-распределенных объектов
Решаемые задачи	Выявление нарушителей, угроз и рисков	
Методы прогнозирования	Эвристический подход	
Виды интеллектуальных моделей	Экспертная система с обучением	

Характерной особенностью реализации систем прогнозирования инцидентов для данного подхода являются рассмотрение прежде всего в качестве защищаемого информационного ресурса критических систем информационной инфраструктуры региональных информационных объектов в пределах ареала функционирования этих объектов и обмена данными с другими взаимодействующими информационными объектами. Для данной экспертной системы была выбрана продукционная модель построения базы знаний, потому что она являются наиболее наглядным средствами представления знаний. Она близка к логическим моделям, что позволяет организовывать на ее базе эффективные процедуры вывода, и в то же время более наглядно (чем классические логические модели) отражает знания. Продукционная модель чаще всего применяется в промышленных экспертных системах. Она привлекает разработчиков своей наглядностью, высокой модульностью, легкостью внесения дополнений и изменений и простотой логического вывода.

Применительно к условиям реализации упреждающей стратегии информационной безопасности в качестве особенностей основ построения системы прогнозирования инцидентов следует рассматривать следующие положения (Табл.3).

Таблица 3. Особенности построения основ систем прогнозирования инцидентов при упреждающей стратегии информационной безопасности

Основы	Особенности	
Цели прогнозирования	Среднесрочное прогнозирование инцидентов (от 3 до 5 лет)	
Возлагаемые функции	Внутренняя и внешняя оценка континентальной информац. обстановки	Защита критического информац. ресурса континентально распределенных объектов
Решаемые задачи	Выявление нарушителей, угроз и рисков	
Методы прогнозирования	Методы Big Data	
Виды интеллектуальных моделей	Сетевая адаптивная модель. Модель интеллектуального анализа данных Data Mining	

Характерной особенностью реализации систем прогнозирования инцидентов для данного подхода являются рассмотрение прежде всего в качестве защищаемого информационного ресурса критических систем информационной инфраструктуры континентальных и межконтинентальных информационных объектов в пределах ареала их функционирования и обмена данными с другими взаимодействующими информационными объектами. В данных рассматриваемых условиях обеспечения информационной безопасности наиболее успешно реализуются прогнозирование инцидентов на основе использования моделей , воспроизводящих динамику временного ряда в форме искусственных нейронных сетей. Данный подход позволяет значительного увеличения возможного горизонта прогноза и минимизации погрешностей предсказаний. В интересах практического реализации прогнозирования инцидентов информационной безопасности целесообразно рассмотреть основы использования для этих целей модели интеллектуального анализа данных Data Mininq [15].

4. Основы технологии интеллектуального анализа данных Data Mininq по прогнозированию инцидентов информационной безопасности

Разработка данных (Data Mininq), это обнаружения знаний из баз данных в целях нахождения повторяющихся информационных элементов в анализируемых массивов информации из различных источников. Если повторяющихся сегментов информации выявлено достаточно много, то их анализ позволяет обнаруживать и прогнозировать неизвестные (новые) закономерности, т.е. извлекать новые знания. Основное отличие типовой статистической обработки данных от Data Mininq (разработка данных) от заключается в том, что первый подход позволяет пользователю делать собственные заключения и выводы на основе полученных результатов обычной статистической обработки исходных данных. При разработки данных (Data Mininq) компьютер предлагает пользователю свои выводы, сделанные относительно исходного набора данных на основе применяемых алгоритмов и моделей. В качестве одной из типовой задачи по прогнозированию появления инцидентов информационной безопасности реализуемой Data Mininq, приведенной в литературе [15]. описаны следующие технологии анализа:

-выявления подозрительной активности с банковскими картами (или слишком необычные для клиента выполнение различных покупок, нехарактерные для него). Выявление данной ситуации позволяют банкам не пропускать транзакции, пока они не получат письменного или устного разрешения клиента;

- решения вопроса о выдаче займа клиентам. Все клиенты характеризуются определенным набором исходных данных (зарплата, продолжительность работы на одном месте, возраст, семейное положение, наличие долгов и их величина, а также другие данные. Каждая характеристики клиента определяется некое количество баллов, которое суммируется для данного клиента. Далее полученный конечный результат сравнивается с определенным пороговым значением, которое аналитики банка считают безопасной величиной. При этом если количество очков клиента превышает пороговое значение, то клиенту выдается кредит, в противно случае ему будет отказано;

- выявления прогнозируемых видов нарушений и нарушителей информационной безопасности в сравнении с пороговыми значениями и оценки ожидаемых результатов опасности.

Рассматриваемая технология интеллектуального анализ данных Data Mininq позволяет решать следующие задачи:

- «Классификация объектов анализа» в виде разбиения их на заранее известные классы;

- «Кластеризация объектов анализа» в виде разбиения их на заранее неизвестные классы;

- «Регрессия» это поиск функций задаваемых параметров в интересах предсказания инцидентов;

-«Ассоциация» это анализ не отдельных объектов, а совокупности, т.е. набора связанных объектов;

- «Последовательность» эта задача позволяет находить временную закономерность между анализируемыми событиями;

- «Анализ отклонений и выбросов» позволяет обнаруживать в наборе анализируемых данных нехарактерные (наиболее отличающие) значения.

В интересах указанных задач интеллектуального анализа реализуются следующие алгоритмы Data Mininq:

- «Алгоритм Байеса» реализует задачу «Классификации»;

- «Деревья решений» также реализует задачу «Классификации»;

- «Алгоритм кластеризации» осуществляет итерационными шагами группировку исходных данных в кластеры, которые содержат подобные характеристики;

- «Алгоритм «нейронные сети» предназначенный для анализа сложных входных ситуаций (данных). При этом формируется сеть из двух или трех слоев (уровней) «нейронов»: входной, скрытый (необязательный) и выходной. Входные «нейроны» определяют вероятности различных входных параметров. Скрытый слой «нейронов» различным вероятностям входных данных назначает весовые коэффициенты важности. Выходные «нейроны» определяют значения выходных данных прогноза;

- «Временные ряды» представляют собой алгоритм реализации задачи «Регрессии», который оптимизирован для прогноза непрерывных значений во времени. Данный алгоритм проводит обучение на одинаковых данных по двум моделям: одна модель направлена на реализацию краткосрочного прогноза, а другая обеспечивает алгоритм долгосрочного прогноза. Далее осуществляется объединение результатов обоих моделей и формируется наилучший прогноз для переменного числа временных срезов;

- «Линейная регрессия» позволяет рассчитывать линейную зависимость между входными и прогнозируемыми параметрами;

- «Алгоритм кластеризации последовательностей» выявляет самые распространенные последовательности (ряд анализируемых событий или переходов между состояниями в наборе данных) и группирует идентичные последовательности в кластеры;

-«Логическая регрессия» является вариантом алгоритма нейронной сети и используется для моделирования непрерывных и дискретных результатов прогноза. При этом определяется вклад каждого входного параметра в виде наделения их весовыми коэффициентами.

Рассмотренный программный продукт революционной реализации технологий интеллектуального анализа данных Data Mining, разработанный компанией Microsoft, позволил его использовать в практической деятельности не только программистам, но и аналитикам, в частности, сферы информационной безопасности. Это достигается благодаря использования для реализации интеллектуального анализа приложений Excel и SQL-сервера. При этом аналитикам и программистам при реализации технологии (Data Mininq) не требуется углубленного знания SQL-сервера, даже можно обойтись лишь одной средой Excel. Непосредственно для работы по реализации технологией прогнозирования (Data Mininq) в среде Excel (версия 2007 и более позднего издания) необходимо установить бесплатную подпрограмму-надстройку Data Mininq Add-in. Загрузка осуществляется с сайта http://www.sqlserverdatamining.com. Данная программа нужна для коммуникаций между Excel и SQL-сервером. Инициирование подпрограмму-надстройку Data Mininq Add-in поможет осуществить специальный мастер установки конфигурации. Более подробное описание практического использования программного продукта Data Mininq можно ознакомиться в указанной литературе [15].

4. Результаты

В целях апробации рассмотренных основ технологии построения систем прогнозирования инцидентов информационной безопасности (на основе программного продукта Data Mininq) в настоящее время отрабатываются вопросы внедрения их в учебный процесс подготовки бакалавров информационной безопасности (направление подготовки 10.03.01) по профилю «Информационно-аналитические системы финансового мониторинга». Рассмотренные технологические основа практического построения таких систем интеллектуального анализа данных позволяют обнаруживать также новые знания в совершенно разных областях науки и бизнеса.

5. Заключение

В данной статье представлены теоретико-практические технологические аспекты основв построения интеллектуальных систем прогнозирования инцидентов информационной безопасности.

Теоретико-технологический ракурс статьи базируется, на вводимых в настоящее время понятий целесообразных стратегий информационной безопасности с учетом различных рассматриваемых условий их реализаций: оборонительная, наступательная и упреждающая стратегии. Именно вводимые стратегии информационной безопасности и определяют целесообразные технологические основы

построения интеллектуальных систем прогнозирования инцидентов информационной безопасности для различных объектов защиты.

Практико-технологический ракурс статьи предусматривает целесообразность рассмотрения в качестве основ построения современных интеллектуальных систем прогнозирования на основе применения нейросетевых моделей и , в частности, новейшей и простой среды разработки данных Data Mininq и которая не требует привлечения большого ресурса: финансового, людского и технического. Это особенно важно для использования данного подхода в ходе подготовки профессионалов в области информационной безопасности, прежде всего, в учбных заведениях.

Список используемых источников

1.Bogdanova E.M., Matveev A.V. The algorithm for predicting fires with the method of exponential smoothing // Security service in Russia: experience, problems, prospects. Ensuring complex safety of population: materials from Russian scientific conference, SPb.: Saint-Petersburg university of State fire service of EMERCOM of Russia, 2017. p. 94–97.

2.Bogdanova E.M. Algorithmic support of adaptive fire prediction: materials of II international scientific conference on international CD day. M.: Academy of State fire service of EMERCOM of Russia, 2018. p. 49–57.

3.Kindaev A.Y., Shishov V.F. Neural network as a forecasting tool for city fires // Mathematics application in economic and technical researchah. 2014. № 1 (4). p. 252–260.

4. Kropov Y.A. Proskuryakov A.Y., Belov A/A. Method of forecasting time series changes in digital instrumentation and control systems //computer optics-2018. -Chu 42, no. 6., p. 1093-1100.

5.Magliiec Y. A. Information systems analysis and requirements analysis M.: Internet University of Information Technologies BINOM. Knowledge Laboratory, 2008. p. 11.

6. Malyuk A. A. Security policy framework of critical information infrastructure systems. -M.: hotline-Telecom, 2018. -314.

7.Maksimov A.V., Matveev A.V., Popivchak I.I. Promising directions of information and analytical activities in the field of fire safety // Geopolicy and safety . 2015. № 2 (30). p. 113–117.

8.Matveev A.V., Bogdanova E.M. The classification for the methods of prediction emergency situations // National security and strategy. 2018. №4 (24). p. 61–70.

9. Eun Annalyn, Kenneth Su. Theoretical minimum for Big Data. Everything you need to know about Big Data-Spb.: Piter, 2019.p. 208.

10. Gost R ISO/MEC TO 18044-2007. Information technology. Methods and means of ensuring security. Management informacionnojs security incidents.

11. GOST 34-601–90. Information technology. Set of standards for automated systems. Automated systems. Stages of development. M.: Standartinform, 1990.

12. Novoselov S.V., Panihidnikov S.A. Problems in prediction of number of emergencies by statistical methods // mountain news and analytical bulletin (scientific and technical magazine). 2017. № 10. p. 60–71.

13. Problems of forecasting and monitoring of the critical situations by methods of the hydrogen theory of catastrophes / E.P. Burakovskij [i dr.] // Marine Intelligent Technology. 2012.№2 (16). p. 50–60.

14. Information Systems Design: textbook . / D.V. Chistov [i dr.]. M.: Yurajt, 2015.

15. Rafalovich in. Data Mininq, or data mining for busy-m. f Smartbook, 2014.-p. 96.

16. Solyanoy W.N. Features of construction expert system of evaluating economic efficiency of information security activities. Information technology bulletin . MGOTU. 2017. No. 3 (13), p. 127-136.

17. Solyanoy W.N. Information security management Organization in financial and credit institutions. Information security business and society. Compendium of selected articles. Russian State Social University. -M.: Publishing House «Pen». 2016.

18. Solyanoy W.N. Ppractice innovation scientific-educational complex for Bachelor and master courses in the field of information security. Scientific-practical magazine Informational counteraction to threats of terrorism, volume 1 2015 g. -Taganrog: IZD-vo Southern feleoalnyj University,2015.

19. Yakimenko K.W., Zhukov M. Creating detection methodology of information security incidents.//Reshetnevskie read. 2013. No. 17. p. 332-323.

20. Varnakov V.V., Varnakov D.V., Neberikutya I.A. Justification of methods for forecasting man-made emergencies // International Scientific Journal. 2011. № 1. p. 94–97.