DOI 10.37882/2223-2966.2025.06.10

ПРОГНОЗИРОВАНИЕ ИНЦИДЕНТОВ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

FORECASTING INCIDENTS IN INFORMATION SECURITY SYSTEMS

D. Budnikov

Summary. The article is devoted to the topic of identifying incidents in information security systems. Special attention is paid to the effective identification of deviations and improving the quality of forecasts.

Keywords: information security, information security systems.

Будников Дмитрий Александрович
Аспирант, Финансовый университет при Правительстве РФ
devilrdie777@mail.ru

Аннотация. Статья посвящена теме выявления инцидентов в системах защиты информации. Особое внимание уделяется эффективному выявлению отклонений и повышению качества прогнозов.

Ключевые слова: информационная безопасность, системы защиты информации.

В статье рассмотрена методология, направленная на помощь в определении основных устройств и параметров, имеющих решающее значение для практических задач. Она способствует увеличению контрастности обнаруживаемых сигналов и актуализирует необходимость внедрения механизма, способствующего выявлению инцидентов. Обозначены требования к критериям, необходимым для обнаружения инцидентов. Использование предложенного метода в сочетании с наблюдаемыми характеристиками обеспечит эффективное выявление отклонений и повысит качество прогнозов.

Системы выявления инцидентов, работающие по сигнатурному принципу, служили основой защиты сетевых границ и находятся в центре активных исследований [5, 6]. Значительный интерес вызывают нейронные сети и машинное обучение, включая нечеткие логические методы, которые существенно способствуют выявлению аномалий в сетевом трафике [7–9]. Кроме того, получают заслуженное признание статистические методы анализа инцидентов [4, 10–13].

В своем научном исследовании Д.О. Ковалев [3] развил алгоритмические подходы для выявления инцидентов в текстах, полученных от систем мониторинга. Основой методики стало использование динамической таблицы показателей, демонстрирующей распределение сообщений, позволяя применять квадратичную интерполяцию для определения математического ожидания и дисперсии в рамках заданного временного интервала. Применение нечеткой логики стало центральным элементом анализа полученных данных.

Тем не менее, несмотря на достижения Ковалева, его методики инцидентного мониторинга не отвечают современным требованиям отслеживания состояния критически важных систем, поскольку изначально они разрабатывались для более простых систем.

Изучение внутреннего строения КССБ выявляет сложную архитектуру, обрабатывающую значительные объемы разнообразных данных. В структуре КССБ функционирует в пределах двадцати разновидностей узлов, осуществляющих взаимодействие друг с другом на аппаратном уровне, каждый из которых имеет индивидуальное программное обеспечение.

Временной ряд, отображающий динамику поведения КССБ, представляет собой зависимость количественного показателя от времени. Он отражает как положительные, так и отрицательные колебания. В функционировании КССБ выделяют несколько этапов: нормальный режим, отклонение от нормы, пред инцидентный этап и непосредственно сам инцидент. Каждый этап имеет собственные особенности и активно влияет на функционирование системы, что критично для анализа временных рядов. На момент инцидента отмечаются резкие колебания таких параметров, как скорость, напряжение и частота. Эти колебания поддаются оценке с применением различных статистических методов, что способствует созданию более точных моделей для прогнозирования динамики поведения системы. В связи с изменением статистического распределения показателей во время инцидента важно разработать соответствующие модели для анализа и предсказания последующего состояния системы.

Представленный метод обнаружения инцидентов основывается на формировании временных рядов, которые состоят из показателей КССБ. После этого полученные ряды подвергаются анализу с применением различных прогнозирующих методик. Основной принцип данного метода заключается в выявлении инцидентов путем сопоставления действительных значений исследуемого показателя с его прогностическими оценками.

Согласно [14], прогноз выступает в роли вероятностного предположения о будущем состоянии объекта исследования. Сам процесс прогнозирования представляет собой предсказание будущих событий на основании научных методов. Он охватывает комплексное исследование тенденций и ожидаемых изменений в анализируемом явлении. В современных научных исследованиях наблюдается широкий спектр прогнозных методов, а также разнообразие классификаций и подходов к ним.

На изображении 1 представлена система классификации прогнозирующих методов, созданная Э.Е. Тихоновым [15]. В соответствии с этой схемой выделяются две основные категории: интуитивные и формализованные подходы.

Интуитивные подходы, опирающиеся на мнения и оценочные суждения экспертов, находят широкое применение в таких областях, как экономика, политология и маркетинг. Наиболее очевидно в этих сферах проявляется недостаточная точность предсказания поведения систем при использовании математических моделей. В отдельных случаях системы оказываются элементарными, и использование сложных математических методов становится неоправданным.

Согласно авторитетным источникам, формализованные методы прогнозирования ассоциируются с созданием математических моделей, использующихся для предсказания будущих значений различных процессов. Эти методы позволяют достичь точных прогнозов на основе расчетов, основанных на анализе исторической информации.

Прогнозирование подразумевает применение различных технологий, охватывающих широкий спектр методов: экспертные, статистические (включая анализ временных рядов, корреляционно-регрессионный анализ и прочие), экономико-математические и аналогичные. Конкретный метод подбирается с учетом исследовательских целей, задач, которые необходимо решить, а также имеющихся ресурсов. Прогностическая модель характеризуется специализированной абстракцией, опирающейся на четко сформулированные концепции, которая минимизирует предпосылки и позволяет определить влияние отдельных факторов на итоговый показатель, даже в условиях неопределенности. Иными словами, прогностическая модель выступает в роли «интеллектуальной регрессионной формулы», адаптируемой к специфическим задачам.

Метод прогнозирования включает реализацию комплекса действий, необходимых для формирования модели, способной предсказать динамику или поведение определённого процесса.

Модель прогнозирования обязана достоверно отображать объект, подлежащий прогнозированию, и обеспечивать возможность генерации актуальных прогнозов.

Анализ исследований демонстрирует разнообразие методов, предназначенных для разработки прогнозных моделей [15]. В трудовой диссертации И.А. Чучуевой [16] предложена двухуровневая классификация методов, которая выделяет два базовых направления: модели, относящиеся к конкретным предметным областям, и временные модели.

Модели предметных областей представляют собой специализированные научные конструкции, отражающие закономерности, характерные для определённой сферы науки и техники. Формирование данных моделей основывается на изучении взаимосвязей ключевых категорий, свойственных конкретной области. При построении подобных моделей следует учитывать индивидуальные условия и уникальные особенности каждой предметной области.

Модели временных рядов, в отличие от прочих подходов, созданы с целью предсказания будущих показателей, на основе собранных данных, охватывающих предшествующие временные промежутки. Указанные модели обладают универсальным характером и могут интегрироваться в самые разнообразные сферы применения, при этом их основная структура остаётся неизменной вне зависимости от признаков анализируемых временных рядов.

Статья охватывает совершенствование методов обработки временных рядов в области обеспечения безопасности. Главная задача исследования заключается в создании алгоритмов предсказания, обеспечивающих оперативное выявление инцидентов, что является важным аспектом охраны объектов.

При выборе методов прогнозирования основным критерием служит срок предсказания, который должен быть согласован с циклом целевого объекта. Этого согласования достигают при помощи безразмерного прогностического коэффициента q [18].

$$q = \Delta w / w, \qquad (1.1)$$

где Δw — абсолютное время упреждения; w — величина эволюционного цикла объекта прогнозирования.

Формальные методы предсказания демонстрируют максимальную эффективность, когда $q << 1$ менее единицы, что подразумевает временной горизонт анализа до одного года. Способность этих методов обеспечивать точное отражение всех известных факторов, воздейству-

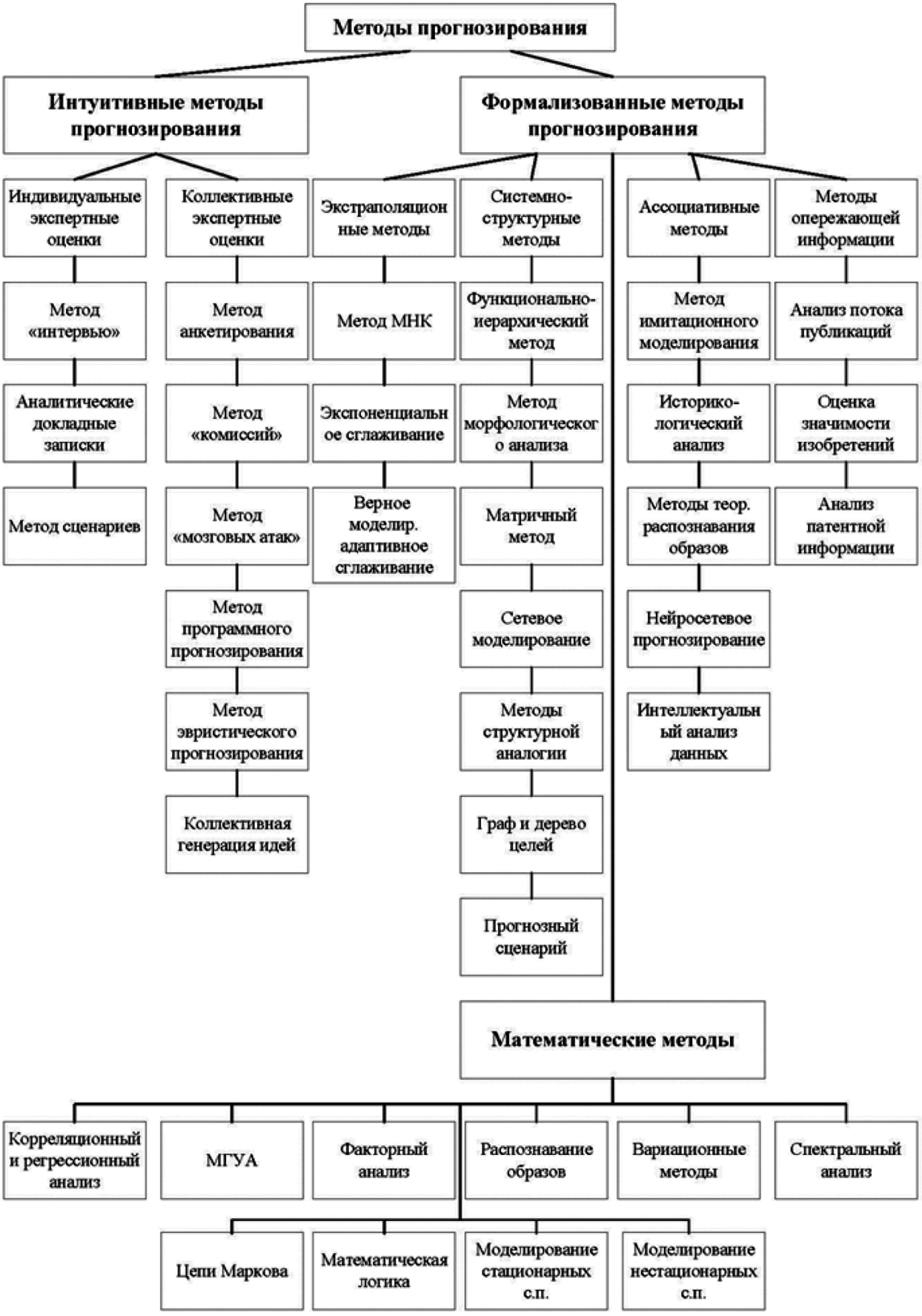

Рис. 1. Классификационная схема методов прогнозирования

ющих на прогнозируемые объекты, обусловливает такое положение дел. При необходимости выполнения долгосрочных предсказаний следует принимать во внимание вероятность значительных изменений в экономической и политической сфере, что существенно влияет на предсказательную точность.

В указанных условиях интуитивные подходы становятся востребованными для определения вероятных «скачков» и продолжительности их проявления. Обычно, когда значение ц превышает одну единицу — это может указывать на присутствие нескольких циклов роста.

Управление системами комплексного сбора и обработки данных (КССБ) в локальных сетях требует отказа от долгосрочных прогнозов на недели и месяцы, заменив их краткосрочными предсказаниями на весь эволюционный цикл. Использование актуальных данных позволяет формализованным методам предсказания стать действенным инструментом в данном направлении.

При составлении краткосрочных прогнозов ключевым моментом выступает изучение значений параметров, зафиксированных в течение определённого периода. На базе методик, рассмотренных в разделе, разрабатывается хранилище данных, состоящее из множества различных значений переменных, фиксируемых в разные временные моменты. Изменяющиеся во времени параметры позволяют получить временной ряд.

Методы анализа временных рядов предполагают набор последовательных наблюдений, собранных за определённый срок. Данный подход служит базой для предсказания и экстраполяции. В рамках предложенного исследования продемонстрирована одна из действенных методик предсказания, в состав которой входят алгоритмы наименьших квадратов [19], экспоненциальное сглаживание и вероятностное моделирование.

Метод наименьших квадратов (МНК), хотя и считается наилучшим средством для краткосрочного прогнозирования, требует соблюдения множества условий по нормальности ошибок. Кроме того, выбор соответствующей модели тенденции основывается на различных статистических критериях, что вызывает определённые затруднения.

Классические модели экстраполяции временных рядов фокусируются на выявлении закономерностей в прошлых данных с целью предсказания будущих значений. В противоположность им, вероятностные модели предоставляют более глубокий и комплексный метод, принимающий во внимание неопределенности и колебания в данных.

Модели временных рядов описываются функциями и коэффициентами, выведенными из собранных наблюдений, в то время как вероятностные модели сосредоточены на расчетах вероятностей. Следует подчеркнуть: вероятностные подходы оценивают последовательности наблюдений на основании их статистического распределения без учета временной зависимости. Указанное ограничение противоречит критериям и препятствует эффективному решению поставленных задач.

Экспоненциальное сглаживание, в отличие от ранее перечисленных методов, сосредоточено на выявлении параметров тренда, которые не только отображают средние значения, но и акцентируют внимание на актуальной динамике показателя в момент последнего измерения. Ключевыми преимуществами этого подхода выступают учет весов исходных данных, простота вычислений и высокая адаптивность к различным типам процессов.

В предложенном методе прогнозирования актуальные данные получают большее значение в сравнении с прошлыми, при этом величина этого значения увеличивается в соответствии с геометрической прогрессией. Экспоненциальное сглаживание соответствует установленным критериям, однако существует одна особенность.

Установление параметров сглаживания, начальных условий и порядка полинома выступает важной задачей в практическом применении указанных подходов в научной и инженерной сферах [15]. Исследования, изложенные в [18], продемонстрировали, что модели второго порядка не обеспечивают значительного прироста точности предсказаний по сравнению с моделями первого порядка, однако требуют более сложных вычислений.

В результате применения метода экспоненциального сглаживания он стал ведущим методом в среднесрочном прогнозировании.

ЛИТЕРАТУРА

1. Пустить в расход: как менялся бюджет России за десятилетие [Электронный ресурс] // Лента.Ру. — Электрон. дан. — [Б.м.], 2013. — URL: http://lenta.ru/articles/2013/10/08/budget (дата обращения: 18.02.2025).
2. Концепция построения и развития аппаратно-программного комплекса «Безопасный город»: утв. распоряжением Правительства Российской Федерации от 3 дек. 2014 г. № 2446-р [Электронный ресурс] // Правительство Российской Федерации: официальный сайт. — Электрон. дан. — М., 2014. — URL: http://government.ru/media/files/0apBppc8jyA.pdf (дата обращения: 06.02.2025).
3. Ковалев Д.О. Выявление нарушений информационной безопасности по данным мониторинга информационно — телекоммуникационных сетей: автореферат дис. ... канд. техн. наук / Д.О. Ковалев. — М., 2011. — 25 с.
4. Баранов В.А. Обнаружение инцидентов информационной безопасности как разладки процесса функционирования системы: дис. ... канд. техн. наук [Электронный ресурс] / В.А. Баранов // DisserCat: научная электронная библиотека. — Электрон дан. — СПб., 2013. — URL: http://www.dissercat.com/content/obnaruzhenie-intsidentov-informatsionnoi-bezopasnosti-kak-razladki-protsessa-funktsionirovan#ixzz3lXtMntrK (дата обращения: 05.02.2025).
5. Половко И.Ю. Анализ функциональных требований к системам обнаружения вторжений [Электронный ресурс] / И.Ю. Половко, О.Ю. Пескова // Известия ЮФУ. Технические науки. — 2014. — № 2 (151). — С. 8692. — Электрон. версия печатн. публ. — URL: http://cyberleninka.rU/article/n/analiz-funktsionalnyh-trebovaniy-k-sistemam-obnaruzheniya-vtorzheniy#ixzz3mejyq18n (дата обращения: 13.02.2025).
6. Камаев В.А. Методология обнаружения вторжений [Электронный ресурс] / В.А. Камаев, В.В. Натров // Известия ВолгГТУ. — 2006. — № 4. — С. 148–153. — Электрон. версия печатн. публ. — URL: http://cyberleninka.ru/article/n/metodologiya-obnaruzheniya-vtorzheniy#ixzz3mehexVma (дата обращения: 14.02.2025).
7. Слеповичев И.И. Обнаружение DDoS атак нечеткой нейронной сетью / И.И. Слеповичев, П.В. Ирматов, М.С. Комарова, А.А. Бежин // Известия Саратовского университета. Новая серия. Сер. Математика. Механика. Информатика. — 2009. — № 9:3. — С. 84–89.
8. Goyal A. GA-NIDS: A Genetic Algorithm based Network Intrusion Detection System [Electronic resource] / A. Goyal, Ch. Kumar // Northwestern University. — Electronic data. — Evanston, IL, [s.a.]. — URL: http://www.cs.northwestern.edu/~ago210/ganids/GANIDS.pdf (дата обращения: 14.02.2025).
9. Поздняков С.А. Использование схемы совпадений в системах обнаружения вторжений на основе нейронных сетей / С.А. Поздняков // Вестник Омского государственного университета. — 2012. — № 2 (64). — С. 189–190.
10. Баранов В.А. Оценка момента вторжения статистическими методами / В.А. Баранов // Проблемы информационной безопасности. Компьютерные системы. — 2011. — № 2. — С. 24–31.
11. Жуков В.Г. Модель синтеза коллективов интеллектуальных информационных технологий решения задачи обнаружения инцидентов информационной безопасности // В.Г. Жуков, В.В. Бухтояров // Программные продукты и системы: международный научно-практический журнал. — 2014. — № 1 (105). — С. 20–25.
12. Котов В.Д. Современное состояние проблемы обнаружения сетевых вторжений / В.Д. Котов, В.И. Васильев // Вестник УГАТУ. — 2012. — № 3 (48). — С. 198–204.
13. Исхаков С.Ю. Анализ трафика и моделирование сетевых атак с использованием методов прогнозирования / С.Ю. Исхаков, А.О. Шумская //Общество, современная наука и образование: проблемы и перспективы: сб. науч. тр. по матер. Межд. науч.-практ. конф., Тамбов, 30 нояб. 2012 г. — Тамбов: Бизнес-Наука-Общество, 2012. — Ч. 10. — С. 28–30.
14. Тихонов Э.Е. Прогнозирование в условиях рынка: учеб. пособие / Э.Е. Тихонов. — Невинномысск, 2006. — 221 с.
15. Сидоров С.Г. Анализ временных рядов как метод построения потребления электроэнергии / С.Г. Сидоров, А.В. Никологорская // Вестник ИГЭУ. — 2010. — Вып. 3. — С. 81–83.
16. Чучуева И.А. Модель прогнозирования временных рядов по выборке максимального подобия: дис. ... канд. техн. наук [Электронный ресурс] / И.А. Чучуева. — М., 2012 // Математические бюро. — Электрон. дан. — URL: http://www.mbureau.ru/sites/default/files/pdf/Chuchueva-Dissertation.pdf (дата обращения: 27.02.2025).
17. Широков Л.А. Исследование систем управления: учеб. пособие / Л.А. Широков. — М.: Изд-во МГИУ, 2010. — 168 с.
18. Галустян М.Ж. Проблемы использования метода наименьших квадратов при оценке и прогнозировании динамики фондовых рынков / М.Ж. Галучтян // Известия ТулГУ. Экономические и юридические науки. — 2015. — № 2–1. — С. 88–92.
19. Goodwin P. The Holt-Winters Approach to Exponential Smoothing: 50 Years Old and Going Strong [Electronic resource] / P. Goodwin // International Institute of Forecasters. — Electronic data. — [S.l.], 2010. — URL: http://forecasters.org/pdfs/foresight/free/Issue19_goodwin.pdf (дата обращения: 27.02.2025).

Журнал «Современная наука: актуальные проблемы теории и практики»