УДК 004.056.5

Жээналиева Назгуль Мидиновна,
ст. препод., заместитель зав. кафедры программной инженерии
Международного университета Кыргызской Республики
Аблабекова Чынара Азисовна,
к.ф.-м.н., доцент
кафедры программной инженерии Международного
университета Кыргызской Республики
Оморова Нургуль Амадалиевна,
ст. препод., кафедры обеспечение безопасности информационных систем
Институт информационных технологий КГТУ им. И. Раззакова

Жээналиева Назгуль Мидиновна,
улук окутуучу,
Кыргыз республикасынын эл аралык университети программалык
инженерия кафедрасы
Аблабекова Чынара Азисовна,
физика - математика илимдеринин кандидаты, доцент
Кыргыз республикасынын эл аралык университети программалык
инженерия кафедрасы
Оморова Нургул Амадалиевна,
улук окутуучу
Маалыматтык системалардын коопсуздук кафедрасы
И.Раззакова атындагы КМТУнун
Маалыматтык технологиялар институту

Jeenalieva N. M.,
Senior Lecturer, Deputy Head
of the department Software Engineering the
International University of the Kyrgyz Republic
Ablabekova Ch. A.,
Ph.D., Associate Professor
Department of Software Engineering from the
International University of the Kyrgyz Republic
Omorova N. A.,
senior lecturer
Department of Information Systems Security
Institute of Information Technologies of KSTU named after I. Razzakov

АНАЛИЗ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПРЕДСКАЗАНИЯ, ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ СБОЕВ РАБОТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

МААЛЫМАТ СИСТЕМАЛАРЫНЫН БОЛЖОМОЛОРУН АНЫКТОО ЖАНА АЛДЫН АЛУУ БОЮНЧА ИНТЕЛЛЕКТУАЛДУУ СИСТЕМАСЫН ТАЛДОО

ANALYSIS OF INTELLIGENT SYSTEM FOR PREDICTION, DETECTION AND PREVENTION OF FAILURES IN INFORMATION SYSTEMS

Аннотация: *Статья представляет собой обзорную работу, посвященную методам и технологиям, используемым при анализе интеллектуальной системы предсказания, обнаружения и предотвращения сбоев работы в информационных системах. В этой статье рассмотрены основы разработки интеллектуальной системы, способной выполнять эти задачи, а также ее ключевые компоненты и преимущества*

Ключевые слова: *безопасность данных, угрозы информационной безопасности, защита от атак, информационная безопасность, компьютерная безопасность, риск безопасности, система безопасности, защита.*

Аннотациясы: *Макала маалымат системаларындагы мүчүлүштүктөрдү алдын алуу, аныктоо жана алдын алуу үчүн интеллектуалдык системаны талдоодо колдонулган ыкмаларга жана технологияларга арналган обзордук иш. Бул макалада бул милдеттерди аткарууга жөндөмдүү интеллектуалдык системаны иштеп чыгуунун негиздери, ошондой эле анын негизги компоненттери жана артыкчылыктары талкууланат.*

Ачкыч сөздөр: *маалыматтардын коопсуздугу, маалыматтык коопсуздук коркунучтары, чабуулдан коргонуу, маалыматтык коопсуздук, компьютердин коопсуздугу, коопсуздук коркунучу, коопсуздук системасы, коргоо.*

Abstract: *This article is a review work devoted to the methods and technologies used in the analysis of an intelligent system for predicting, detecting and preventing failures in information systems. This article discusses the basics of developing an intelligent system capable of performing these tasks, as well as its key components and advantages.*

Key words: *data security, information security threats, attack protection, information security, computer security, security risk, security system, protection.*

Введение

Современные информационные системы становятся все более сложными и многоуровневыми, что делает их уязвимыми к различным сбоям и инцидентам. В условиях постоянного увеличения объемов данных и требований к их обработке, системы должны не только эффективно функционировать, но и уметь предсказывать, обнаруживать и предотвращать возможные сбои [2].

Стремительное развитие и внедрение предсказательного обслуживания основано на современных достижениях цифровизации и четвертой промышленной революции. В основе технологии лежит использование возможностей *Анализа Больших данных, Искусственного интеллекта, Интернета вещей, Облачных сервисов* [8].

Интеллектуальная система предполагает не только непрерывный сбор данных, но и их анализ с помощью алгоритмов машинного обучения, чтобы предсказывать потенциальные угрозы и автоматически принимать меры для предотвращения возможных аварий. Это включает в себя автоматическую систему оповещений, которая информирует ответственных

лиц о необходимости проведения ремонта или эвакуации в случае обнаружения критических изменений в параметрах мониторинга.

Современные кибератаки становятся все более изощренными, используя методы социальной инженерии, эксплуатацию неизвестных уязвимостей нулевого дня, распределенные инструменты для автоматического сканирования сетей. Традиционные средства защиты, основанные на сигнатурном анализе и правилах, зачастую оказываются неэффективными против новых, ранее неизвестных угроз. Возникает острая необходимость в более гибких и интеллектуальных системах обеспечения кибербезопасности, что обуславливает **актуальность** исследований в области применения интеллектуальных методов защиты в информационных системах.

Анализ интеллектуальной системы

Интеллектуальная система — это система, использующая алгоритмы машинного обучения, искусственного интеллекта и аналитики данных для обработки информации, принятия решений и автоматизации процессов [6]. В контексте предсказания и предотвращения сбоев в информационных системах, такая система может анализировать данные о работе сети, выявлять аномалии и предлагать меры по их устранению.

Интеллектуальная система может иметь средства в виде компьютерного приложения как базовый инструмент на объектно- ориентированном языке программирования C# [5].

Компоненты интеллектуальной системы

1. Сбор данных

Первый шаг в разработке интеллектуальной системы — это сбор и хранение данных. Ключевыми источниками данных могут быть:

- Логин серверов и приложений
- Метрики производительности (загрузка CPU, память, сеть)
- Информация о пользователях и их действиях
- Данные о конфигурациях оборудования и программного обеспечения

2. Обработка и анализ данных

Собранные данные должны быть обработаны и проанализированы для выявления паттернов и аномалий. Для этого используются методы статистического анализа, машинного обучения и обработки естественного языка. Важно выделить следующие этапы:

- Очистка данных: удаление шумов и некорректной информации.
- Анализ временных рядов: выявление трендов и сезонных колебаний.
- Моделирование: использование алгоритмов машинного обучения для построения предсказательных моделей.

3. Обнаружение аномалий

Система должна быть способна обнаруживать аномалии в реальном времени. Для этого применяются различные методы, такие как:

- Методы кластеризации: позволяют группировать данные и выявлять отклонения от нормального поведения.
- Нейронные сети: для сложных паттернов и многомерных данных.
- Правила и эвристики: на основе экспертных знаний.

4. Предсказание сбоев

Основной целью системы является предсказание сбоев до их возникновения. Для этого используются:

- Модели регрессии: для прогнозирования временных рядов.
- Алгоритмы классификации: для определения вероятности возникновения сбоя.
- Системы рекомендаций: для предложений по устранению потенциальных проблем.

5. Реакция на инциденты

После обнаружения потенциального сбоя система должна не только уведомить администраторов, но и предложить меры по его устранению [1]. Это может включать:

- Автоматизированные сценарии восстановления
- Уведомления и отчеты для администраторов
- Интеграция с системами управления инцидентами

Преимущества интеллектуальной системы

- Снижение времени простоя: благодаря раннему обнаружению и предотвращению сбоев.
- Оптимизация ресурсов: более эффективное использование вычислительных ресурсов и сетевой инфраструктуры.
- Улучшение качества обслуживания: повышение удовлетворенности пользователей за счет надежности систем.
- Аналитика и отчетность: возможность анализа исторических данных для улучшения бизнес-процессов.

Заключение

Разработка интеллектуальной системы предсказания, обнаружения и предотвращения сбоев в информационных системах — это сложная, но необходимая задача для обеспечения надежности и эффективности работы современных IT-структур.

Использование передовых технологий и методов анализа данных позволяет не только минимизировать риски, но и значительно повысить качество обслуживания пользователей. В условиях стремительного роста объемов информации и усложнения систем, внедрение таких решений становится критически важным для успешной деятельности организаций [5].

Рост новых информационных и телекоммуникационных технологии сильно повлияло на наше государство и частных организации, что привело к переходу цифровизации деятельности всех услуг. Соответственно вся информация хранятся, обрабатываются в электронном виде. Стоит отметить среди них особое значение имеют персональные данные (далее, ПДн), которые считается промежуточной для функционирования всех процессов как основной информационный ресурс. Вместе с этим следует, уделять особое внимание вопросам обеспечения защиты информации, чтобы предотвратить утечки и несанкционированного распространение персональных данных, последствия которого может привести к серьезному имиджевому и материальным потерям как в государственном, так и в частном организации [4].

С развитием технологий, таких как искусственный интеллект и большие данные, интеллектуальные системы будут становиться все более мощными и эффективными. Ожидается, что в будущем они смогут не только предсказывать и предотвращать сбои, но и самостоятельно обучаться на основе новых данных, что сделает их еще более адаптивными к изменениям в условиях работы.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Автоматизированная платформа информационной безопасности [Электронный ресурс]. – Режим доступа: https://www.securityvision.ru/blog/obzor-i-karta-rynkaplatform-dlya-zashchity-ml/

2. Артюшкина Е. С., Сафиуллин Дж. Ф., Использование интеллектуальных систем в защите информации. Вестник ПГУТиИ, г. —Самара, —№ 4 (69), 2023 https://cyberleninka.ru/article/n/ispolzovanie-intellektualnyh-sistem-v-zaschite-informatsii

3. Кадыров А.Р., Жээналиева Н.М. Критерии выбора средств защиты персональных данных // Современные проблемы механики. –Бишкек, 2019, № 38(4), —с.46-51

4. Кадыров А.Р., Жээналиева Н.М. Разработка программного модуля для определения актуальности угрозы безопасности персональных данных// Современные проблемы механики. –Бишкек, 2019, № 38(4),— с. 51-57.

5. Манапбаев И.К., Жээналиева Н.М., Осмонова Ж.Р. Инновационные технологии и цифровая трансформация в образовании: преобразование университета 4.0 для устойчивого развития. Вестник Международного университета Кыргызстана №4(56), 2024. —С.114-118 https://drive.google.com/file/d/1JqUKT_7tbzo3pI2TcVSnGOdPjCVnJ5Br/view?pli=1

6. Советов Б.Я. Интеллектуальные системы и технологии: учебник для студ. учреждений высш. проф. образования -М.: Издательский центр «Академия», 2013. - 320 с. https://academia-moscow.ru/ftp_share/_books/fragments/fragment_21887.pdf

7. Стратегия защиты киберпространства в Кыргызстане [Электронный ресурс]. – Режим доступа:https://digital.gov.kg/activities/strategiya-zashhity-kiberprostanstva-vkyrgyzstane/

8. https://rus.azattyk.org/a/32802618.html