НАУЧНЫЙ АСПЕКТ

na-journal.ru

2024

№4

ТОМ 48

УДК 001.8(082)

ББК 1
Н 34

Периодичность – 12 раз в год

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

Свидетельство ПИ № ФС 77-84349

ISSN 2226-5694

Учредитель, главный редактор – Хасиятуллов Марат Габделахатович

Состав ред. коллегии представлен на сайте https://na-journal.ru

Адрес редакции:
443125, г. Казань, ул. Азата Аббасова, д. 21А, кв. 149

Издатель ООО «Аспект»

Адрес издательства:
443068, г. Самара, ул. Николая Панова, д. 16, оф. 34

Н 34 НАУЧНЫЙ АСПЕКТ № 4 2024. – Самара: Изд-во ООО «Аспект», 2024 . – Т48 . – 140 с.

Журнал «Научный аспект» является научным изданием и отражает результаты научной деятельности авторов по различным дисциплинам в области гуманитарных, естественных и технических наук.

УДК 001.8(082)
ББК 1

Почтовый адрес: 420100 г. Казань а/я 9
Официальный сайт: https://na-journal.ru
Электронная почта: public@na-journal.ru

Подписано к печати 20.05.2024
Дата выхода в свет 28.05.2024
Цена свободная

Бумага ксероксная. Печать оперативная. Заказ № .
Формат 60×84 /16. Объем 8,4 п.л. Тираж 100 экз.

Отпечатано в типографии «Куранты»
г. Казань, Сибирский тракт, 34к14, оф. 317, тел. +7 (843) 216-12-71

Содержание

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004

Будущее искусственного интеллекта

Чумаев Данил Михайлович

студент Поволжского государственного университета телекоммуникаций и информатики

***Аннотация**: Статья освещает разнообразные аспекты влияния искусственного интеллекта (ИИ) на современное общество, от его применения в журналистике и обслуживании клиентов до революционных изменений в транспорте и проблемах, связанных с рабочими местами. Особое внимание уделяется рискам, связанным с предвзятостью в алгоритмах, которые могут усугублять социальное неравенство, проблемам конфиденциальности данных и угрозам от дипфейков и дезинформации. Подчеркивается сложность вопросов, стоящих перед обществом, и необходимость в балансе между инновациями и этическими соображениями при разработке и внедрении ИИ.*

***Abstract**: This article highlights the diverse aspects of the impact of artificial intelligence (AI) on modern society, ranging from its application in journalism and customer service to its provision of revolutionary changes in transportation and workplace issues. Particular attention is paid to the risks of biases in algorithms that may exacerbate social inequalities, data privacy issues, and threats from deepfakes and misinformation. The complexity of the issues facing society and the need to balance innovation and ethical considerations in the design and implementation of AI are emphasized.*

***Ключевые слова**: искусственный интеллект, ИИ.*

***Keywords**: artificial intelligence, AI.*

Введение

Инновации в области искусственного интеллекта продолжают определять будущее человечества практически во всех отраслях. ИИ уже является основной движущей силой таких развивающихся технологий, как большие данные, робототехника и IoT (интернет вещей), а генеративный ИИ еще больше расширил возможности и популярность ИИ.

По данным исследования IBM 2023, 42% предприятий корпоративного уровня интегрировали ИИ в свою деятельность, а 40% рассматривают возможность внедрения ИИ в своих организациях. Кроме того, 38% организаций внедрили генеративный ИИ в свои рабочие процессы, а 42% рассматривают такую возможность.

Вот что могут означать изменения в области ИИ для различных отраслей промышленности и общества в целом, учитывая столь стремительные темпы развития.

Как искусственный интеллект повлияет на будущее

Повышение уровня автоматизации бизнеса

Около 55% организаций в той или иной степени внедрили искусственный интеллект, что позволяет предположить, что в ближайшем будущем многие предприятия смогут повысить уровень автоматизации. С появлением чат-ботов и цифровых помощников компании могут полагаться на ИИ в простых разговорах с клиентами и ответах на основные вопросы сотрудников.

Способность ИИ анализировать огромные объемы данных и преобразовывать полученные результаты в удобные визуальные форматы также может ускорить процесс принятия решений. Руководителям компаний не нужно тратить время на самостоятельный анализ данных, вместо этого они могут использовать мгновенные выводы для принятия обоснованных решений.

Сокращение рабочих мест

Автоматизация бизнеса, естественно, привела к опасениям по поводу потери рабочих мест. На самом деле работники считают, что почти треть их задач может выполнять искусственный интеллект. Несмотря на то что искусственный интеллект добился успехов на рабочем месте, он оказывает неодинаковое влияние на различные отрасли и профессии. Например, ручные работы, такие как секретарь, находятся под угрозой

автоматизации, но спрос на другие профессии, такие как специалисты по машинному обучению и аналитики по информационной безопасности, вырос.

Работники, занимающие более квалифицированные или творческие должности, скорее всего, будут дополнены ИИ, а не заменены. Независимо от того, заставляет ли ИИ сотрудников осваивать новые инструменты или берет на себя их функции, он будет стимулировать повышение квалификации как на индивидуальном, так и на корпоративном уровне.

Проблемы изменения климата

В гораздо более широком масштабе ИИ способен оказать значительное влияние на устойчивое развитие, изменение климата и экологические проблемы. Оптимисты могут рассматривать ИИ как способ повышения эффективности цепочек поставок, проведения прогнозируемого технического обслуживания и других процедур, направленных на сокращение выбросов углекислого газа.

В то же время ИИ можно рассматривать как одного из главных виновников изменения климата. Энергия и ресурсы, необходимые для создания и поддержания моделей ИИ, могут увеличить выбросы углекислого газа на 80%, что нанесет сокрушительный удар по всем усилиям в области устойчивого развития в технологиях. Даже если ИИ будет применяться в климатически безопасных технологиях, затраты на создание и обучение моделей могут привести к тому, что общество окажется в худшей экологической ситуации, чем раньше.

На какие отрасли промышленности ИИ окажет наибольшее влияние

Практически нет ни одной крупной отрасли, которую бы не затронул современный ИИ. Вот несколько отраслей, которые претерпевают наибольшие изменения благодаря ИИ.

ИИ в производстве

Производство уже давно извлекает выгоду из ИИ. Роботизированные руки и другие производственные роботы с поддержкой ИИ появились еще в 1960-х и 1970-х годах, поэтому эта отрасль хорошо адаптировалась к возможностям ИИ. Эти промышленные роботы обычно работают вместе с людьми, выполняя ограниченный круг задач, таких как сборка и штабелирование, а датчики предиктивного анализа обеспечивают бесперебойную работу оборудования.

ИИ в здравоохранении

Это может показаться маловероятным, но ИИ в здравоохранении уже меняет способ взаимодействия людей с медицинскими работниками. Благодаря возможностям анализа больших данных ИИ помогает быстрее и точнее выявлять заболевания, ускорять и оптимизировать процесс поиска лекарств и даже следить за состоянием пациентов с помощью виртуальных помощников.

ИИ в финансах

Банки, страховые компании и финансовые учреждения используют ИИ для решения различных задач, таких как выявление мошенничества, проведение аудита и оценка клиентов для получения кредитов. Трейдеры также используют способность машинного обучения оценивать миллионы точек данных одновременно, что позволяет им быстро оценивать риски и принимать разумные инвестиционные решения.

ИИ в образовании

ИИ в образовании изменит способы обучения людей всех возрастов. Машинное обучение, обработка естественного языка и распознавание лиц с помощью ИИ помогают оцифровывать учебники, выявлять плагиат и оценивать эмоции студентов, чтобы определить, кто испытывает труд-

ности, а кто скучает. Как в настоящее время, так и в будущем ИИ адаптирует процесс обучения к индивидуальным потребностям учащихся.

ИИ в СМИ

Журналистика тоже использует ИИ и будет продолжать получать от него пользу. В качестве примера можно привести использование "Associated Press" системы "Automated Insights", которая ежегодно готовит тысячи репортажей о заработке. Однако по мере появления на рынке генеративных инструментов для написания статей с использованием ИИ, таких как ChatGPT, возникают вопросы об их использовании в журналистике.

ИИ в обслуживании клиентов

Большинство людей боятся получать звонки от роботов, но ИИ в сфере обслуживания клиентов может предоставить отрасли инструменты, основанные на данных, которые принесут значимые знания как клиенту, так и поставщику услуг. Инструменты ИИ в сфере обслуживания клиентов представлены в виде чат-ботов и виртуальных помощников.

ИИ в транспорте

Транспорт — одна из отраслей, которую, безусловно, ждет радикальное изменение благодаря ИИ. Самоуправляемые автомобили и планировщики поездок с искусственным интеллектом — это лишь несколько аспектов того, как мы добираемся из пункта А в пункт Б, на которые повлияет ИИ. Несмотря на то что автономные автомобили далеки от совершенства, в один прекрасный день они будут перевозить нас из одного места в другое.

Риски и опасности искусственного интеллекта

Несмотря на положительные изменения во многих отраслях, искусственный интеллект все еще имеет недостатки, которые оставляют место для беспокойства. Вот несколько потенциальных рисков искусственного интеллекта.

Потеря рабочих мест

По данным Всемирного экономического форума (ВЭФ) в период с 2023 по 2028 год 44% рабочих мест будут утрачены. Не все работники будут затронуты одинаково — женщины чаще, чем мужчины, сталкиваются с искусственным интеллектом в своей работе. В сочетании с тем фактом, что между мужчинами и женщинами существует огромный разрыв в навыках работы с ИИ, женщины оказываются гораздо более подверженными риску потерять работу. Если компании не примут меры по повышению квалификации своего персонала, распространение ИИ может привести к росту безработицы и сокращению возможностей для маргинализированных слоев населения попасть в сферу технологий.

Человеческие предубеждения

Репутация искусственного интеллекта запятнана привычкой отражать предвзятость людей, которые обучают алгоритмические модели. Например, известно, что технология распознавания лиц предпочитает светлокожих людей, дискриминируя людей с более темным цветом кожи. Если исследователи не позаботятся об искоренении этих предубеждений на ранних стадиях, инструменты ИИ могут закрепить их в сознании пользователей и увековечить социальное неравенство.

Дипфейки и дезинформация

Распространение дипфэйков грозит размыть границы между вымыслом и реальностью, заставляя широкую общественность задаваться вопросом, что реально, а что нет. А если люди не смогут распознать дипфэйки, то влияние дезинформации может оказаться опасным как для отдельных людей, так и для целых стран. Дипфэйки использовались, в частности, для политической пропаганды, финансовых махинаций и постановки студентов в опасное положение.

Конфиденциальность данных

Обучение моделей ИИ на открытых данных повышает вероятность нарушения безопасности данных, что может привести к раскрытию личной информации потребителей. Компании также вносят свой вклад в эти риски, добавляя свои собственные данные. Исследование Cisco 2024 показало, что 48% компаний ввели непубличную информацию о компании в инструменты генеративного ИИ, а 69% опасаются, что эти инструменты могут нанести ущерб их интеллектуальной собственности и юридическим правам. Одна-единственная утечка может раскрыть информацию миллионов потребителей и в результате сделать организацию уязвимой.

Список литературы

1. Гудфеллоу Я., Бенджио И. Глубокое обучение: учеб. пособие: 2017. 652 с.
2. Брокман Д. CRM: Искусственный интеллект — надежды и опасения: учеб. пособие 2019. 400 с.

УДК 004.7

Программно-конфигурируемая сеть

Токмаков Данил Александрович

аспирант Отдела аспирантуры и докторантуры Поволжского государственного университета телекоммуникаций и информатики

Научный руководитель **Карташевский Вячеслав Григорьевич**

доктор технических наук, профессор кафедры Информационной безопасности Поволжского государственного университета телекоммуникаций и информатики

***Аннотация**: В статье рассматриваются основные этапы развития программно-конфигурируемых сетей. В частности, речь пойдет об основных годах, в которых были переломные моменты в области исследования данной сети. Также будут представлены несколько документов, согласно которым требуется проводить построение ПКС. Отдельное внимание уделяется протоколу OpenFlow, который на данный момент*

представляет из себя неотъемлемую часть любой ПКС. Также в статье рассматриваются несколько структур построения ПКС. Будут рассмотрены различные структуры программно-конфигурируемых сетей и их уровни.

***Abstract**: The paper discusses the main stages of development of software-configurable networks (SCN). In particular, it will discuss the main years in which there were turning points in the research field of this network. Several documents, according to which it is required to conduct the construction of SCN will also be presented. Special attention is paid to the OpenFlow protocol, which is currently an integral part of any SCN. Also, the article considers several structures of SCN. Different structures of software-configurable networks and their layers will be considered.*

***Ключевые слова**: программно-конфигурируемые сети, концепции, интерфейсы прикладного программирования, протокол OpenFlow, ПКС-контроллер, архитектура ПКС, уровень управления, уровень приложений, сетевые ресурсы, маршрутизация, интерфейсы.*

***Keywords**: software-defined networks, concepts, application programming interfaces, OpenFlow protocol, PKS controller, PKS architecture, control level, application level, network resources, routing, interfaces.*

В конце прошлого столетия стали возникать абсолютно новые тенденции в развитии сетей связи. Они, в первую очередь, были нацелены на возможность быстрого и простого способа смены конфигурации сети, которые реализуются посредством программируемости и централизованного управления. По истечении некоторого времени стало проводиться все больше исследований в данной области, что привело к формированию одной из новых концепций, суть которой заключается в разграничении области управления и передачи данных. Это позволило приложениям и сетевым службам управлять абстрагированной сетевой инфраструктурой непосредственно через интерфейсы прикладного программирования (API — Application Programming Interface).

Важным этапом в развитии программно-конфигурируемых сетей явилась разработка первых версий протокола OpenFlow в 2008 году. Если дать краткое определение, то протокол OpenFlow представляет из себя процесс управления обработкой запросов, которые передаются по сети посред-

ством сетевых устройств, представляющие из себя маршрутизаторы и коммутаторы. Вся эта совокупность технологий и процессов позволяет реализовать технологию программно-конфигурируемой сети. Данный протокол позволяет управлять сетевыми устройствами с центрального устройства, называемого контроллером сети, который представлен в виде некоторого сервера. Появление протокола OpenFlow наряду с появлением ПКС-контроллеров послужило мощным толчком к развитию программно-конфигурируемых сетей.

Тестирование первых версий протокола OpenFlow проводилось на базе сети университетских городков. Главной площадкой в конце 2000-х годов стал Стэнфордский университет.

В 2011 году организована некоммерческая организация Open Networking Foundation (ONF) при поддержки таких крупных организаций как Google, Verizon, Deutsche Telekom, Microsoft, Facebook, и Yahoo и др. И уже в 2014 году эта организация определила в документе ONF TR-502: SDN Architecture, свои перспективы развития ПКС и видение архитектуры ПКС. Также стоит обратить внимание, что достаточно длительное время протокол OpenFlow рассматривался как экспериментальная площадка.

Стоит сделать небольшую ремарку, что в материалах ONF TR-502, где представлены рекомендации, не регламентируется внутренняя структура или реализация ПКС-контроллера. Вообще контроллер представляется как «черный ящик».

Первые разработки в области стандартизации ПКС в Международном Союзе Электросвязи были начаты 2009 году. В 2014 году МСЭ-Т Y.3300 была выпущена рекомендация «Framework of Software-Defined Networking», в ней приведено описание эталонной архитектуры программно-конфигурируемых сетей. Если кратко описать архитектуру, предложенную МСЭ-Т, то она обладает следующими уровнями: уровень ресурсов (Resource layer), уровень управления ПКС (SDN control layer) и уровень приложений (Application layer).

В 2015 году Исследовательская группа интернет-технологий предложила свое представление архитектуры программно-конфигурируемых сетей в документе RFC 7426 «Software-defined networking (SDN): Layers and Architecture Terminology».

В ходе разработки ПКС были предусмотрены концепции мониторинга и измерений. Эти функции стали неотъемлемой часть ПКС, т.к. они необходимы для обеспечения возможности сетевого управления контроллером. Полученная в результате измерений и мониторинга информация используется для программной обработки и получения данных о состоянии сети. Кроме того, в ПКС легко реализуется функция зеркалирования трафика, при этом зеркалирование возможно и на плоскость управления, и на какое-либо внешнее устройство.

Программно-конфигурируемая сеть представляет собой набор методов, позволяющих значительно облегчить проектирование, развертывание и функционирование сетевых служб динамическим и масштабируемым образом. Пользователям данные возможности предоставляют оперативно и эффективно реализовывать функции программирования, организации, контроля и управления сетевыми ресурсами.

В ПКС управление сетевыми ресурсами выполняет выделенный сетевой элемент — контроллер, который чаще всего из себя представляет центральный сервер сети. При помощи контроллера проводиться выполнение функций программирования и с помощью плоскости приложений реализуется возможность по сетевому управлению ресурсами и их контролю. При этом централизованное сетевое управление в рассматриваемой модели сети осуществляет через интерфейсы.

Для управления и настройки распределенных сетевых ресурсов контроллер ПКС взаимодействует с интерфейсом управления приложениями. Контроллер может предоставить различные типы интерфейсов для приложений ПКС.

В ПКС на первый план выходит программируемость управления сетью и абстракция основных сетевых элементов. Сетевыми элементами в данном случае могут быть представлены такие устройства как маршрутизаторы и коммутаторы.

Для того чтобы была возможность соблюдения концептуальных возможностей программно-конфигурируемых сетей, а в первую очередь это является программное управление, которое включает поддержку абстракции сетевых ресурсов требуется обеспечение выполнения следующих требований: программируемость, оркестровка, наличие интер-

фейсов управления для настройки различных ресурсов сети, возможности логического централизованного управления, разделение функций управления и сетевых элементов, использование абстракций для сетевых элементов, управление физическими устройствами, управления виртуальными ресурсами.

Для выполнения требований, которые были представлены в рекомендациях ITU-T Y.3302 и ITU-T Y.3320 была предложена архитектура ПКС, которая включается в себя несколько уровней. Рассмотрим каждый их них.

Прикладной уровень. На данном на программном уровне определяются правила, согласно которым проводится управление приложений ПКС посредством поведения сетевых элементов. Для обеспечения возможности автоматической настройки свойств сетевых элементов и их поведения приложения ПКС взаимодействуют с уровнем управления при помощи интерфейса управления приложениями. Модели информации и данных позволяют использовать абстрактное представление сетевых элементов, которое предоставляется уровнем управления.

Уровень управления. Согласно правилам, которые были сформированы на прикладном уровне программно-конфигурируемой сети предоставляются инструменты для управления поведением сетевых ресурсов. Способы контроля и распределения сетевых ресурсов определяют приложения ПКС, посредством взаимодействия с уровнем управления. Это достигается благодаря использованию интерфейсов управления приложениями. Настройки, предоставляемые приложениям, абстрагируются с помощью моделей. Абстракция будет различаться в зависимости от приложений и особенностей услуг, которые используются при этом.

Функция маршрутизации данных обеспечивает управление сетью и услуги на уровне ресурсов согласно правилам маршрутизации, которые могут быть определены на уровне управления ПКС для приложений ПКС. Пути, по которым осуществляется пересылка данных, определяются на уровне ресурсов и задаются при помощи управлением распределенной маршрутизации. Маршруты перенаправления данных определяются механизмами распределенной маршрутизации. При этом на уровне ресурсов может осуществляться как простая пересылка, так и маршрутизация данных. Помимо прочего имеется возможность реализовать другие функ-

ции в соответствии с требованиями приложений ПКС, к которым можно отнести сжатие данных, транскодирование мультимедийных данных и т.д.

Имеется два интерфейса, управление ресурсами и управления приложениями. Они предоставляют возможность программного управления сетевыми элементами, а также обеспечения доступа к контроллеру и сетевым ресурсам. При этом интерфейс управления ресурсами также служит для обеспечения согласованности работ уровня управления и ресурсов. А интерфейс управления приложениями для обеспечения согласованной работы между уровнями прикладным и управления.

Организация Open Networking Foundation в свою очередь архитектуру программно-конфигурируемых сетей представляет в виде трех плоскостей (уровней): данных (data plane), управления (control plane) и приложений (application). Взаимодействие плоскостей между собой реализуется с помощью интерфейсов и имеет следующий вид: интерфейс D- CPI (Data-Control Plane Interface) позволяет взаимодействовать уровню данных и управления, интерфейс A-CPI (Application-Control Plane Interface) позволяет взаимодействовать уровню приложений и управления. Для архитектуры ONF характерной чертой является выделение в отдельный блок функций, отвечающих за менеджмент. Данная возможность позволяет блоку менеджмента взаимодействовать с каждой плоскостью архитектуры отдельно. т.к. это связано с тем, что функции менеджмента индивидуальны.

Основа любой услуги состоит из определенного набора ресурсов, что позволяет функциям и интерфейсам обеспечивать возможность предоставления пользователю услуг в соответствии с его запросами.

Список литературы

1. Recommendation ITU-T Y.3302 «Functional architecture of software-defined networking». ITU-T, Geneva, January,2014.
2. Recommendation ITU-T Y.3320 «Requirements for applying formal methods to software-defined networking». ITU-T, Geneva, August, 2014.
3. ONF TR-502. SDN architecture. [Электронный ресурс] / Режим доступа: https://www.opennetworking.org/wp-content/uploads/2013/02/TR_SDN_ARCH_1. 0_06062014.pdf

4. ONF TR 521 [Электронный ресурс] / Режим доступа: https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR-521_SDN_Architecture_issue_1.1.pdf
5. Ksentini, A. Toward enforcing network slicing on RAN: Flexibility and resources abstraction / A. Ksentini, N. Nikaein // IEEE Communications Magazine.— 2017. — Vol. 55. — No. 6. — P. 102–108.
6. Benzekki, K. Software-defined networking (SDN): a survey / K. Benzekki, A. El Fergougui, A. Elbelrhiti Elalaoui // Security and Communication Networks.— 2016. — V. 9(18). — P. 5803–5833.

УДК 004.5

Принципы психологии цвета в дизайне интерфейса

Правдин Денис Сергеевич

студент факультета Кибербезопасности и управления Поволжского государственного университета телекоммуникаций и информатики

Елисеев Илья Денисович

студент факультета Кибербезопасности и управления Поволжского государственного университета телекоммуникаций и информатики

Научный руководитель **Коваленко Татьяна Анатольевна**

кандидат технических наук, доцент кафедры Информатики вычислительной техники Поволжского государственного университета телекоммуникаций и информатики

***Аннотация**: В статье дается описание основных принципов психологий цвета и их применения в дизайне интерфейса. Авторы статьи исследуют влияние цветовой гаммы на эмоциональное восприятие пользователя и акцентируют внимание на выборе правильных цветовых комбинаций для достижения определенных целей: улучшения удобства использования, увеличения конверсии и удержания внимания пользователя. Статья представляет ценную информацию для дизайнеров и разработчиков, которые стремятся создать интерфейсы, удовлетворяющие потребности и ожидания пользователей.*

***Abstract**: The article provides a description of the basic principles of color psychologies and their application in interface design. The authors of the article investigate the influence of color scheme on the emotional perception of the user and focus on choosing the right color combinations to achieve certain goals: improving usability, increasing conversion and retaining the user's attention. The article provides valuable information for designers and developers who strive to create interfaces that meet user needs and expectations.*

***Ключевые слова**: цветовые схемы, эмоции, пользовательский интерфейс, влияние на восприятие пользователя, цветовая гармония.*

***Keywords**: color schemes, emotions, user interface, user perception analysis, color harmony.*

В мире современного веб-дизайна главное не только функциональность интерфейса, но и его дизайн, способный привлечь внимание и оставить незабываемое впечатление. Психология цвета играет важную роль, влияя на восприятие пользователем эмоций, поведения и решений. Цвета могут оказывать мощное воздействие на эмоциональное состояние человека и помогать привлечь внимание к товару или услуге. Правильное использование цвета создает приятный дизайн, улучшает удобство использования, повышает узнаваемость бренда и даже увеличивает конверсию. В статье рассматриваются основные принципы психологии цвета в дизайне интерфейсов, которые помогут создать эффективный и привлекательный пользовательский интерфейс.

Проблема, которая рассматривается в статье — это принцип психологии цвета в дизайне интерфейса. Она заключается в недостаточном осознании или неправильном применении цветовых схем при создании веб-сайтов, мобильных приложений и других интерфейсов. Многие дизайнеры и разработчики сталкиваются с проблемой выбора цветовой палитры, которая не соответствует ожиданиям аудитории или не формирует нужные эмоциональные реакции. Проблема недостаточного понимания психологических аспектов цвета и его влияния на восприятие пользователей, может приводить к нежелательным результатам и уменьшению эффективности интерфейса.

Цвета обладают необычной силой — они могут вызывать чувства, эмоции и даже воспоминания. Например: чувства спокойствия, счастья или голода, воспоминания о какой-либо вещи. Если правильно подобрать цвета в дизайне у человека можно вызвать необходимые эмоции.

Давайте разберем, какие цвета на что влияют. Красный, желтый и оранжевый придают больше энергии вашему дизайну. Подобные цвета применяют для привлечения внимания. Именно поэтому их не стоит использовать в большом количестве, только при необходимости.

Красный часто используют на кнопках или на тексте с призывом к чему-либо. Он повышает аппетит, но также может символизировать гнев и страх, поэтому с ним нужно быть осторожным, чтобы не переборщить.

Двигаясь дальше по цветовой гамме, мы встречаем оранжевый цвет. Он является промежуточным между красным и желтым — вбирает в себя свойства обоих цветов. Хорошо подходит, когда необходимо что-то выделить, но при этом не получится использовать красный. Оранжевый хорошо сочетается с некоторыми холодными цветами, например синий.

Дальше по порядку идет желтый цвет. Он обладает энергией как красный, но уже меньшей, однако его не часто используют, так как он плохо читаемый — это сделает ваш дизайн плохо воспринимаемым. Желтый вызывает чувства счастья и молодости, поэтому его используют для детских товаров, однако способен и вызвать тревогу — поэтому обычно не используется в здравоохранении.

Несмотря на все это, при правильном подборе и композиции данные цвета могут стать прекрасным дополнением к дизайну и отлично выделять объекты и привлекать к ним внимание пользователей.

Переходим к холодным цветам. И первым будет зеленый цвет, он символизирует чистоту и природу. Именно поэтому его обильно используют в отрасли клининга. Зеленый цвет популярен благодаря его положительности. Его часто применяют на кнопках согласия и одобрения, в финансовой индустрии, например чтобы показать положительный рост рынка или акций.

Голубой, как и желтый, является промежуточным цветом, но для зеленого и синего. Он вбирает в себя чистоту зеленого и спокойствие синего — это делает его уникальным, так как воплощает собой оптимизм, именно поэтому его часто используют в биотехнологических стартапах.

Следующим идет синий цвет, очень популярный и распространенный, так он означает стабильность и спокойствие. Синий может быть сам по себе, его не обязательно выделять или смягчать другими цветами, он

отлично подходит для больших областей дизайна, например фон. Холодный характер делает синий и его оттенки универсальными, они могут быть использованы в любых отраслях.

Фиолетовый. Он сочетает в себе спокойствие синего, и сострадание розового. Фиолетовый обычно ассоциируется с изысканностью — именно поэтому его применяют в гостиничной и ресторанной сфере. Он излучает любовь и страсть, благодаря чему его используют в здравоохранение и молодежных брендах. Фиолетовый — насыщенный, шелковистый, сочный. Его можно использовать в больших пространствах дизайна. Он хорошо сочетается с желтым цветом, который играет роль акцента. Фиолетовый хорошо использовать в качестве градиента или наложения на фотографии, что придает им ретро-визуальность.

Розовый цвет. Он ассоциируется с женственностью, романтикой и любовью. Но использовать его в большом количестве может быть проблематично, лучше всего для этого подойдут его светлые оттенки в сочетании с другим холодным цветами, которые будут придавать успокаивающий характер.

Белый и черный — эти цвета являются основном для фона. Для создания элегантного вида дизайна интерфейса отличным выбором будет сочетание черного фона с яркими основными цветами. Белый символизирует чистоту и ясность, поэтому его можно сочетать в дизайне почти с любым другим цветом. Иногда можно оставить белые пространства для того, чтобы пользователь не терялся в объектах дизайна, белый будет являться разделителем.

Коричневый является вспомогательным цветом, как и зеленый цвет символизирует натуральное, природу. Но использовать его необходимо аккуратно, так как неправильно подобранные оттенки или место может все испортить и сделать дизайн грязным и отталкивающим. Лучше всего использовать его светлые оттенки.

Цвета не употребляются по одному оттенку, есть такое понятие как цветовой круг. У нас есть 3 первичных цвета — это красный, желтый, синий. При сочетании двух цветов у нас получается новый цвет, называемый вторичный цвет. Если сочетать первичный цвет с вторичным цветом получится третичный цвет. И при постановке всех типов цветов получается цветовой круг. В нем, возможно, найти любой из данных цветов.

Тем не менее, хотя цвета могут намного влиять на отношение и реакции пользователей, они не являются единственными факторами, которые следует учесть при дизайне интерфейса. Важно помнить о полном контексте — что за продукт или услуга представлена, какова целевая аудитория и какие цели должен достичь дизайн.

Все это необходимо учитывать, так как цветовые нюансы являются важной частью визуального маркетинга — они передают индивидуальность бренда, вызывают эмоции и чувства. Поэтому правильно подобранная цветовая гамма является залогом успеха вашего дизайна. Но чистые цвета не всегда могут дать ожидаемый результат, поэтому очень часто используют сочетания их оттенков.

Чистые цвета имеют нормальную насыщенность, но с помощью добавления к ним белого, серого и черного можно сформировать совершенно новый.

Для того чтобы правильно подобрать цвета необходимо понимать, как они работают вместе, образуя цветовую схему. Это называется цветовыми гармониями.

Во всем этом нам может помочь цветовой круг. Он делится на теплые и холодные цвета.

Теплые цвета в комнате создают ощущение уюта и комфорта. Холодные цвета создают ощущение чистоты и даже заставляют комнату казаться больше. Правильное сочетание теплых и холодных цветов сделает комнату или дизайн более ярким. А если вы используете в основном холодные цвета, добавьте искру тепла, чтобы подчеркнуть что-то важное.

Выбор цветовой схемы для дизайна — это ключевой момент, который требует тщательного подхода. Это может сильно влиять на восприятие пользователей и их взаимодействие с продуктом. Поэтому давайте разберем основные цветовые схемы, используемые в дизайне, как они работают и как расположены на цветовом круге.

Схема дополнительных цветов — это прямые противоположности друг друга на цветовом круге. Но противоположности притягиваются. Часто можно увидеть их в паре, например: желтый и фиолетовый, красный и синий. Но при использовании двух дополнительных цветов необходимо избегать пропорций 50/50. Это сделает дизайн сложным для восприятия.

Лучше сделать один цвет основным, а другой использовать для дополнения или выделения объектов.

Сплит-комплементарная схема использует один основной цвет и для контраста выбирает цвета, непосредственно прилегающие к его дополнительному цвету. Например, если основной цвет — красный, дополнительные будут сине-зеленый и желто-зеленый. Эта схема обеспечивает высококонтрастное, но более сбалансированное и менее напряженное взаимодействие цветов.

Аналоговая цветовая схема — это цвета, расположенные рядом друг с другом на цветовом круге. Аналоговые схемы создают ощущение спокойствия и гармонии. Она помогает создать визуально несложный и минималистичный дизайн. При использовании подобной схемы лучше придерживаться правила: один доминирующий, два дополнительных.

В монохроматической схеме используется один единственный цвет и его оттенки и тона. Эта позволяет создать визуальную простоту и согласованность, которая будет легко восприниматься. С помощью этой схемы также можно создать еще больший контраст с элементами других цветов, чтобы обратить на них внимание пользователя. Или, наоборот, объединить конкурирующие между собой детали. Но стоит быть аккуратным, так как необходимо очень удачно подобрать цвет и его оттенки.

Триадическая цвета — это три равноудаленных друг от друга цветов на круге, если их соединить линиями, то получится равносторонний треугольник — именно поэтому данную схему называют триадической. С помощью такой палитры удается одновременно добиться и контраста, и гармонии, так как гарантированно будет либо два теплых цвета и один холодный, либо два холодных и один теплый. Но также значит, что будет либо три первичных цвета, либо три вторичных, либо три третичных. Поэтому необходимо обратить внимание, что если использовать 3 вторичных цвета или 3 третичных цвета, изображение может выглядеть темным и беспорядочным. Это исправляют первичные цвета, которые дают больше вибрации и жизни.

Тетрадическая схема похожа на триадическую, включает в себя две пары комплементарных цветов, образуя прямоугольник на цветовом круге. Например, красный и зеленый, синий и оранжевый. Это богатая

и разнообразная цветовая схема, но требует аккуратного использования, чтобы избежать хаоса.

Разреженная цветовая схема использует разные оттенки, тона и насыщенность одного цвета, а затем добавляет чистые оттенки из другого диапазона на цветовой палитре. Это может создать очень привлекательный, но согласованный набор цветов.

Рассмотренные варианты употребления цветов в дизайне говорит о том, что, прежде чем делать пользовательский интерфейс, нужно задуматься какие цвета будут применяться. Для каких целей делается интерфейс. И уже в зависимости от задач, поставленных перед вами употреблять те или иные цвета.

Другие ключевые факторы включают типы и размеры шрифтов, расположение элементов на странице, пространственные отношения между объектами, анимации и многое другое. Все эти элементы влияют на общее восприятие интерфейса и взаимодействие с ним.

В конечном счете, эффективность интерфейса зависит от того, насколько хорошо он соответствует потребностям и ожиданиям пользователей, а также от общей работоспособности и надежности интерфейса. Успешное сочетание всех этих элементов создает впечатляющий и привлекательный интерфейс, который приятно использовать.

Список литературы

1. Иттен, И. Искусство цвета / И. Иттен. — пер. с англ. Л. Монаховой. — Москва: Аронов, 2021.— 96 с.
2. Адамс, Шон Словарь цвета для дизайнеров / Шон Адамс. — Москва: КоЛибри, 2020.— 256 с. — ISBN 978–5–389–13369–3.
3. Базыма, Б. А. Психология цвета. Теория и практика. / Б. А. Базыма. — Санкт-Петербург: Речь, 2007.— 208 с.
4. Коваленко, Т. А. Влияние интерфейса на восприятие программного продукта/ Т. А. Коваленко // Информационно-Вычислительные технологии и их приложения: сб. науч. тр. XXIII Междунар. науч.-техн. конф. Пенза, 2019. С. 104–107.

5. Нелюбова, М. В. Психология цвета / М. В. Нелюбова. — Санкт-Петербург: Санкт-Петербургский государственный университет, 2000.— 8–13 с.
6. Берлин, Б. Основные цвета: Их универсальность и видоизменения / Б. Берлин, П. Кей. — Москва: ФЛИНТА, 1969.— 520 с.
7. Эванс, Г. История цвета. Как краски изменили наш мир / г Эванс. — Москва: Эксмо, 2019.— 224 с. — ISBN 978–5–04–108306–9.

УДК 004

Информационные технологии в подборе персонала

Чиркова Татьяна Владиславовна

магистрант Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

Научный руководитель **Овчинников Иван Иванович**

профессор кафедры Государственного и муниципального управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

***Аннотация**: Наш мир развивается, все больше новых технологий появляется. В настоящее время информационные технологии используют все компании в независимости от их размеров, доходностей, положений на рынке. Эффективная работа организации напрямую взаимосвязана от самих работающих в ней сотрудников. Для того, чтобы персонал компании подходил не только для выполнения той или иной функции, но и разделял общие цели компании, необходимо производить качественный отбор кандидатов. Но как отбирать кандидатов быстро и качественно? В данной статье мы рассмотрим использование информационных технологий при подборе персонала.*

***Abstract**: The world develops with more and more new technologies appearing. Nowadays information technologies are used by all companies regardless of their size, profitability, position in the market. The effective work of the organization is directly interconnected with the very employees working in it. In order for the company's personnel to be suitable not only for a particular function, but also to share the overall goals of the company, it is necessary to make a*

qualitative selection of candidates. But how does one select candidates quickly and qualitatively? This article will discuss the use of information technology in personnel selection.

***Ключевые слова**: информационные технологии, рекрутмент, управление персоналом, информационные системы, подбор персонала.*

***Keywords**: information technology, recruitment, personnel management, information systems, personnel selection.*

Качественно подобранный персонал — это один из элементов успешной организации. Для того, чтобы работа по поставленным задачам выполнялась эффективно, необходимо иметь не только профессиональную команду, но и качественные используемые в работе информационные технологии.

Раннее при традиционном подборе персонала (без помощи информационных технологий) использовались методы, которые требуют большие временные и трудовые затраты. Например, чтобы просто понять, что данный кандидат не подходит на вакансию, на просмотр такого резюме необходимо было затратить от 2–5 минут. А ведь таких резюме может быть тысяча.

Сейчас с поиском подходящих кандидатов стало намного проще, появилось множество информационных технологий, которые помогают рекрутерам делать их работу быстрее и качественнее. Организации стали использовать порталы вакансий, социальные сети для поиска лучших кандидатов на должность. Благодаря Интернету этот процесс стал более эффективным, поскольку это охватывает большое количество человек, люди узнают о предложениях в реальном времени и из любой точки мира, тем самым повышается вероятность найма подходящих и эффективных сотрудников. Стоить отметить, что на подбор персонала повлиял высокий рост вакансий, связанных с работой в социальных сетях. Рекрутеры и в своей работе для поиска таких кандидатов стали использовать различные социальные сети. Порой по профилю потенциального кандидата в социальной сети можно получить о нем больше информации, чем из его предоставленного резюме.

В России в основном используются онлайн-платформы для подбора персонала, такие как HeadHunter, Super Job, Rabota.ru. Эти системы по-

зволяют размещать активные вакансии, проводить автоматизированный отбор резюме, выявляя соискателей, наилучшим образом соответствующих требованиям вакансии, просматривать отклики на выставленные вакансии и т.д.

Помимо онлайн-платформ есть системы, позволяющие проводить первичные онлайн собеседования, не требующие присутствия человека. Можно сказать, что это аналог телефонного интервью. Многие компании внедряют различных виртуальных собеседников, чат-ботов. Отсутствие необходимости человека для простейшего общения с соискателем также упрощает работу рекрутера. Такие программы могут задавать вопросы, принимать и обрабатывать простые текстовые ответы. Они предоставляют возможность проведения онлайн-интервью и тестирования. Это особенно полезно при найме на удаленные позиции.

Примером такой системы может служить, так называемый RobotHR. Такая технология используется для массового подбора персонала. С помощью RobotHR можно проводить предварительное интервью, используя чат-бота. Система отбирает по заданным критериям, отсеивая неподходящих кандидатов.

Исходя из вышесказанного, можно выделить целый ряд пользы использование информационных технологий в подборе персонала:

1. Автоматизация рутинных задач. Информационные технологии позволяют автоматизировать рутинные процессы в подборе персонала, такие как размещение вакансий на различных информационных ресурсах, отбор резюме по заданным критериям, проведение с кандидатами онлайн-тестирования и онлайн-интервью с последующей оценкой кандидата. Автоматизированный подбор персонала позволяет сократить время на выполнение рутинной работы, повышая скорость закрытия вакансий.
2. Широкий выбор кандидатов. Информационные технологии позволяют работодателям привлекать кандидатов не только из своего города, но и из других стран, не ограничиваясь никакими географическими рамками. Это открывает возможность подбора из большего числа потенциальных соискателей, повышая шансы на закрытие вакансий подходящим кандидатом.

3. Формирование аналитических данных. Современные системы управления кандидатами предоставляют мощные инструменты аналитики и отчетности, позволяющие анализировать эффективность различных этапов подбора персонала. Это помогает оптимизировать процесс и принимать обоснованные решения.
4. Улучшенное взаимодействие с соискателями. Рекрутеры — это те, с кем в первую очередь знакомятся потенциальные кандидаты, поэтому необходимо произвести хорошее первое впечатление о самой компании. С помощью информационных технологий соискателям предоставляют различные удобные инструменты для отправки их резюме, заполнения анкет, прохождения тестов и проведения интервью онлайн. Это помогает создавать положительный образ компании, формируя ее имидж на рынке труда.
5. Улучшение качества подбора. Информационные технологии позволяют рассмотреть потенциального соискателя с различных сторон, что позволяет произвести более детальный анализ кандидатов.

Однако стоит отметить, что информационные технологии не могут полностью заменить человеческий фактор в процессе найма. Некоторые аспекты, такие как эмоциональный интеллект, оценка культурной совместимости, могут быть сложны для автоматизации и требуют вмешательства опытного специалиста по найму. Тем не менее, использование информационных технологий в подборе персонала значительно улучшает эффективность и результативность процесса найма. В настоящее время эффективный подбор невозможен без использования информационных технологий.

Список литературы

1. Аллин, О. Н. Кадры для эффективного бизнеса. Подбор и мотивация персонала // О. Н. Аллин, Н. И. Сальникова. — М.: Генезис 2014.
2. Кудинов А.С. CRM. Практика эффективного бизнеса / А. Кудинов, М. Сорокин, Е. Голышева. — М.: Изд-во «1С-Паблишинг», 2012.
3. Павлова, И. С. Подбор и отбор кадров на основе информационных технологий / И. С. Павлова. — Текст: непосредственный // Молодой ученый.— 2020.— № 43. — С. 59–62.

4. Саак А. Е. Информационные технологии управления: учебник для вузов / А. Е. Саак, Е. В. Пахомов, В. Н. Тющняков.— 2-е изд. — СПБ.: Питер, 2012.
5. Романова Ю.Д., Винтова Т.А., Коваль П.Е., Музычкин П.Е., Информационные технологии в управлении персоналом: Учебник и практикум для прикладного бакалавриата / М.: Юрайт, 2016.

УДК 004

Виртуальные ассистенты в государственном управлении: новая эра взаимодействия с гражданами

Раджабов Гамид Теймурович

магистрант кафедры Государственного и муниципального управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

***Аннотация**: Благодаря цифровизации увеличилось количество обращений граждан за государственными(муниципальными) услугами, но в тоже время поднимается проблема оптимизации обращений и информированности населения. Зачастую граждане не знают какие услуги им доступны, как и куда подавать заявления. В настоящей статье рассмотрим инструменты искусственного интеллекта, которые помогают государству в диалоге с гражданами, а также исследуем функции и преимущества виртуальных ассистентов (чат-ботов). Поднимем проблемы конфиденциальности данных при работе с виртуальными ассистентами. Кроме того, приведем примеры внедрения виртуальных ассистентов в государственных ведомствах стран мира, которые уже показали свою эффективность. В заключении сделаем выводы о необходимости комплексных исследований и разработок в области искусственного интеллекта для нужд государственного управления с целью повышения эффективности работы государственных органов власти.*

***Abstract**: Thanks to digitization the number of citizens' requests for state (municipal) services has increased, but at the same time the problem of optimization of requests and public awareness is raised. Often citizens do not know what services are available to them, as well as they are not aware of how and where to apply for those services. In this article the authors will consider the tools of artificial intelligence that help the state in dialog with citizens, as well as explore the*

functions and advantages of virtual assistants (chatbots). Data privacy issues when working with virtual assistants are raised. In addition, The authors will give examples of the introduction of virtual assistants in government agencies in countries around the world, which have already shown their effectiveness. In conclusion, the conclusions are drawn about the need for comprehensive research and development in the field of artificial intelligence for the needs of public administration in order to improve the efficiency of public authorities.

***Ключевые слова**: цифровизация, государственное управление, информационные технологии, чат-боты, прозрачность, взаимодействие граждан с государством.*

***Keywords**: digitalization, public administration, information technology, chatbots, transparency, interaction of citizens with the state.*

Сегодня цифровизация государственного управления стала приоритетным направлением развития стран мира. Информационные технологии в государственном управлении не только упрощает процессы взаимодействия граждан с государством, но и способствует повышению эффективности и прозрачности государственных услуг. Передовыми инструментами в этой области стали чат-боты — интеллектуальные программы, способные вести диалог с пользователем в автоматическом режиме. Чат-боты в государственном управлении помогают гражданам в ряде вопросов: от ответов на стандартные запросы до заполнения форм и документов. Это не только облегчает доступ к необходимой информации, но и уменьшает нагрузку на человеческие ресурсы, позволяя сотрудникам государственных органов сосредоточиться на сложных задачах. Однако, внедрение чат-ботов также сопряжено с рядом вызовов. Например, требуют отдельного внимания вопросы защиты персональных данных, обеспечения безопасности информационных систем и поддержки доверия граждан к электронным способам взаимодействия с государством. Кроме того, необходимо учитывать аспекты интеграции чат-ботов в инфраструктуру и обеспечить их функционирование на всех этапах обслуживания.

Применение виртуальных ассистентов во взаимодействии государства с гражданами даёт ряд преимуществ, в частности:

- непрерывное функционирование ассистента, что позволяет гражданину обратиться за информацией или государственной услугой в любое время суток;

- ассистент запоминает ответы часто задаваемых вопросов и использует их с другими гражданам, что в свою очередь позволяет гражданам получать ответы сразу;
- ассистент оптимизирует работу службы поддержки и снимает с них часть нагрузки;
- ассистента настраивают на поддержку народных языков и диалекты, для тех, кто проживает в отдаленных или малонаселенных пунктах;
- ассистент практически без ошибок соблюдает регламентированные процедуры и стандарты;
- ассистента легко интегрировать в платформы и сервисы государственных услуг.

Примеры виртуальных ассистентов в государственном управлении

«Ask Jamie» — ассистент (чат-бот) государственных структур Сингапура для предоставления информации гражданам в короткие сроки. Виртуальный помощник разрабатывался с целью обработки вопросов граждан об услугах и инструкциях предоставляемыми государственными органами Сингапура.

«Jamie» используют на веб-сайтах государственных ведомств Сингапура. Чат-бот предоставляет мгновенные ответы на запросы, что помогает сократить время ожидания, которое связано с телефонными или электронными запросами. Интерфейс ассистента прост в использовании и обрабатывает запросы и отвечает на естественном языке. Ассистент «Jamie» доступен круглосуточно и позволяет обрабатывать срочные запросы вне рабочего времени.

«Ask USDA». Министерство сельского хозяйства США (далее — USDA) внедрило специального виртуального ассистента, который предоставляет информацию фермерам и гражданам. Ассистент упрощает работу сотрудникам службы поддержки, а также подробно рассказывает об услугах и инициативах USDA.

Чат-бот использует технологии искусственного интеллекта для обработки запросов и составления ответов гражданам в режиме реального

времени. «Ask USDA» распознает естественный язык и разрешает пользователям задавать вопросы без необходимости использования специфических команд.

Отличительной чертой чат-бота является информирование граждан по широкому количеству тем, от правил питания и безопасности пищевых продуктов до программ помощи фермерам и управлению земельными ресурсами.

Также как и «Jamie», «Ask USDA» доступен круглосуточно и обеспечивает поддержку пользователям в любое время суток.

«SUVE» — ассистент, разработанный и используемый в Эстонии с целью предоставления сведений гражданам о пандемии коронавируса, мерах безопасности, статистике заражений и доступных здравоохранительных услугах.

SUVE информирует граждан через социальные сети и специальные веб-сайты. Помощник использует технологии искусственного интеллекта для обработки запросов пользователей и предоставления ответов на часто задаваемые вопросы. В условиях пандемии особенно важно было предоставлять гражданам актуальную информацию о мерах противодействия коронавирусной инфекции.

SUVE также снижает нагрузку на государственные службы поддержки и медицинские учреждения, предоставляет ответы на общие вопросы. Проект показывает эффективность технологий искусственного интеллекта для информированности и поддержки населения в кризисных ситуациях.

Виртуальный ассистент «Робот Макс» на портале госуслуг — это программное решение, призванное упростить взаимодействие граждан России с государственными услугами. Робот создан для того, чтобы помогать гражданам в навигации по порталу, предоставляя информацию и отвечая на частые вопросы.

Ассистент обрабатывает запросы о государственных услугах, в том числе регистрация по месту жительства, получение паспорта или водительских прав и другие. Помощник применяет технологии искусственного интеллекта для анализа вопросов и предоставления ответов.

Ассистент способен обучаться на основе взаимодействия с гражданами. Чем больше пользователей задают вопросы, тем более точными и по-

лезными становятся ответы ассистента. Помощник «Макс» также обладает функцией прямого диалога. Граждане могут получать ответы в форме диалога. Создается ощущение беседы с живым оператором.

Конфиденциальность данных

Помимо преимуществ виртуальных ассистентов, существуют риски, связанные с конфиденциальностью данных граждан. Государственные органы обрабатывают большое количество личной информации, поэтому защита персональных данных становится приоритетным направлением и играет большую роль при выборе технологий и инструментов искусственного интеллекта. Помощники должны гарантировать защиту персональных данных от возможных утечек или злоупотреблений.

Вместе с тем, чат-боты являются целями атак хакеров и преступных группировок со всего мира. Хакеры атакую виртуального ассистента чтобы получить конфиденциальные данные граждан. Государственные органы должны использовать передовые методы шифрования и постоянно обновлять защитные механизмы для предотвращения таких атак, а также регламентировать и назначать ответственных за обработку личной информации.

Кроме того, ассистент может непреднамеренно распространить данные непосредственно в чате. В таких случаях искусственный интеллект неправильно понимает запросы граждан и выдает информацию, которая должна оставаться конфиденциальной. Во избежание подобных случаев необходимо внедрение строгих протоколов обработки запросов и проверки данных на предмет конфиденциальности перед предоставлением.

Вдобавок ко всему, процесс обучения чат-ботов требует больших объемов данных с личной информацией граждан, которые должны обезличиваться для недопустимости раскрытия перед третьими лицами

Выводы

Виртуальные ассистенты или чат-боты в государственном управлении —мощный инструмент, который трансформирует взаимодействие граждан с государственными услугами. Виртуальные помощники уско-

ряют и упрощают процессы, улучшают доступность и качество обслуживания, а также помогают оптимизировать ресурсы и сокращать расходы. Однако, чтобы успешно внедрить чат-боты, необходимо учитывать все технологические, юридические, этические и социальные аспекты.

Разработка чат-ботов должна быть ориентирована на обеспечение безопасности, конфиденциальности данных и удобства эксплуатации. Критически важно обрабатывать запросы на разных языках и диалектах, легко адаптироваться к меняющимся условиям и интегрироваться с существующими платформами.

Учитывая возможные проблемы, государственные ведомства должны разрабатывать стратегии, направленные на эффективное использование потенциала чат-ботов чтобы улучшить качество государственного управления и взаимодействия с гражданами. Такой подход гарантирует представление интересов всех членов общества, а также способствуют созданию открытого, доступного и эффективного государства.

Список литературы

1. Братко А. Г. Искусственный разум, правовая система и функции государства // НИЦ ИНФРА-М. 2024. С. 177–272.
2. Коданева С. И. Перспективы и риски внедрения искусственного интеллекта в государственном управлении // Социальные и гуманитарные науки: отечественная и зарубежная литература. Серия 4: государство и право. 2021. № 1–2. С. 131–139.
3. Талапина Э. В. Использование искусственного интеллекта в государственном управлении // Информационное общество. 2021. № 3 С. 409–414.
4. Сулимин В.В., Шведов В.В., Анализ использование искусственного интеллекта в цифровой экономике для улучшения прозрачности и эффективности государственного управления // Теория и практика общественного развития. 2023. № 6. С. 181–186.
5. Попов Я.А., Юшков Е.С., Артёмов Г. А. Правовое регулирование использования технологий искусственного интеллекта в государственном управлении // Научные дискуссии. Том 4. 2024. № 1. С. 133–137.

6. Указ Президента РФ от 10 октября 2019 года № 490 «О развитии искусственного интеллекта в Российской Федерации» (с изм. 2024 года). — Ст. 19.
7. «Спросите Джейми» Виртуальный ассистент [Электронный ресурс]. — Режим доступа: https://www.tech.gov.sg/products-and-services/ask-jamie/ (дата обращения: 30.04.2024).
8. «Ask USDA» Виртуальный ассистент [Электронный ресурс] — Режим доступа: https://ask.usda.gov/s/ (дата обращения: 30.04.2024).
9. «Suve» Автоматизированный чат-бот [Электронный ресурс] — Режим доступа: https://eebot.ee/en/ (дата обращения: 30.04.2024).
10. Робот «Макс» — Виртуальный помощник [Электронный ресурс] — Режим доступа: https://www.gosuslugi.ru/newsearch (дата обращения: 30.04.2024).

УДК 659.13/.17

Технологии динамического креатива

Назаров Филипп Олегович

студент факультета Рекламы и связей с общественностью Российского государственного гуманитарного университета

***Аннотация**: В данной статье мы поговорим о диджитал коммуникациях, а конкретно, сосредоточимся на такой технологии как "Динамическая оптимизация креативов". В кратце поговорим о том, что это такое, как это использовать и на что эта технология способна. Узнаем какие преимущества и недостатки несёт данный подход. А также, затронем наш рынок: посмотрим насколько сейчас данная техника внедрилась в отечественную рекламу и пользуется ли она популярностью и успехом.*

***Abstract**: Digital communications, and specifically, such technology as "Dynamic Optimization of Creatives" are discussed in this article. In brief the authors will talk about the essence, ways of use and capabilities if this technology. Advantages and disadvantages brought by this approach are highlighted. The domestic market will also be touched upon. The authors try to see how far this technique has now been introduced into domestic advertising and whether it is popular and successful or not.*

***Ключевые слова**: реклама, креатив, сообщение, пользователь, DCO, технология динамического креатива, искусственный интеллект, оптимизация, тестирование.*

***Keywords**: advertising, creative, message, user, DCO, dynamic creative technology, artificial intelligence, optimisation, testing.*

Введение

Реклама, направленная на конкретного пользователя — по праву считается эффективной. Ведь, как минимум, обращение к конкретному человеку, воспринимается лучше чем к группе людей. Сообщение, обращенное к массовой аудитории, не будет восприниматься так чётко как обращение к конкретной ЦА, а обращение уже к конкретному человеку будет намного влиятельней, чем даже к небольшой группе людей (как сравнение — школьный класс и репетитор). В этой релевантности есть основная задача коммуникаций. Человек, в современном мире, сформировал привычку обрабатывать различные рекламные сообщения. Он определенным образом воспринимает рекламу по телевизору, и уже по-другому, например, когда посредник компании обращается к нему лично (через почту, на улице, по телефону и т.д). Конечно, реализация рекламного сообщения через прямой контакт не говорит нам о повышении доверия клиента к предоставляемой ему услуге, но повышает его заинтересованность, причастность, фокус на данном вопросе, ведь рекламодатель тем самым обращается именно к нему, и ведёт диалог именно с ним. Данное осознание уже провоцирует хоть какое-то причастие.

- Но как добиться похожего эффекта от баннера, рекламного ролика и любой диджитал-рекламы, направленной на пользователя?
- Как же, через картинку на экране, постараться приблизить ощущение обращения именно к нему, к конкретному пользователю?

Ответ есть — это системы и технологии динамической оптимизация креативов (DCO).

DCO — (dynamic creative optimization) помогает выстраивать более тесный контакт с потенциальным клиентом. Посредством уже существующей информации о пользователе, учитывая возраст, пол, время обращения и т.д., система помогает создать более точное обращение и, благодаря этому, фор-

мирует большую заинтересованность, причастность, укрепляет контакт и создаёт у пользователя ощущение важности обращения именно к нему.

Предположим, сотрудник компании обращается к вам "вживую" по телефону и предлагает свою услугу. Он учтёт не только лишь имя и зачитает речевой модуль (пример плохого обращения), но и начнёт задавать вопросы, по которым и будет учитывать предпочтения пользователя и по которым и будет, в дальнейшем, выстраивать своё предложение.

Другими словами, динамическая оптимизация креативов — форма программатической рекламы, которая позволяет рекламодателям оптимизировать эффективность своего креатива с помощью технологий в реальном времени.

Каково будущее DCO?

Не так уж давно реклама не имела свойств меняться и подстраиваться под каждого пользователя. Она не учитывала данные, такие как местоположение клиента, девайс, день недели и время суток, погодные условия, историю поиска и предыдущие взаимодействия с веб-сайтом.

Но затем, появилась динамическая креативная оптимизация (DCO).

Легко сочетаясь с технологией программатической рекламы, она автоматически стала создавать, перебирать и оптимизировать персонализированную рекламу в режиме реального времени.

DCO использует поведенческие, демографические, психографические и другие данные о потребителях для создания десятков, сотен или тысяч вариантов рекламного креатива и коммуникации!

На протяжении всей кампании, алгоритмы машинного обучения постоянно корректируют рекламные объявления в зависимости от взаимодействия клиентов с различными версиями. Поскольку технология обслуживает и тестирует различные творческие комбинации, она собирает данные об эффективности рекламы, которые клиенты могут использовать для оптимизации будущих рекламных кампаний.

DCO существует уже давно, и по-прежнему популярен среди маркетологов, он постоянно поддаётся доработкам и улучшениям. За последние несколько лет эта технология развилась и включила в себя генеративный

искусственный интеллект. И хотя предстоящая потеря “куки” может поставить под угрозу все способы оптимизации рекламы, которые рекламодатели могут использовать, креатив остается ключевым рычагом, который бренды могут использовать для повышения эффективности.

Принцип работы DCO

Для смены нескольких креативов, в зависимости от времени суток, могут потребоваться десятки или сотни версий. DCO может сделать этот сложный, трудоемкий, долгий и подверженный ошибкам процесс более эффективным.

Чтобы использовать технологию DCO, рекламодатели создают свои рекламные объявления из взаимозаменяемых компонентов. Поскольку креативы модульные, пользователи видят постоянно меняющиеся комбинации заголовков, подзаголовков, изображений, цен, логотипов, призывов к действию и других элементов рекламы.

Что касается тестирования, DCO склонен использовать A/B/n [2] и многовариантное тестирование [2], так как количество вариантов очень велико по сравнению с тем, что может уловить A/B-тестирование [3].

Вместо простого тестирования двух разных версий, A/B/n-тестирование позволяет использовать n вариантов, каждый из которых тестирует один рекламный элемент. Например, вариант “A” может использовать синюю цветовую схему, вариант “B” — красную цветовую схему, “C” — черно-белую, а вариант “D” — любую другую. Также вариант “B” может тестировать другой оттенок, вариант “C” — другой заголовок, а вариант “D” — другое изображение. Многовариантное тестирование проверяет различные комбинации отдельных элементов в каждом варианте объявления.

Таким образом, один вариант объявления может одновременно тестировать разные призывы к действию, заголовок и фон.

Эволюция DCO

Раньше у DCO был более человеческий подход, да и некоторые компании до сих пор придерживаются старого подхода к разработке креативов

и их оптимизации вручную с помощью A/B или A/B/n-тестирования вместо использования технологии DCO. Но, со временем, цифровые креативные форматы стали более «шаблонными», что делает автоматизированный, основанный на алгоритмах подход к планированию и созданию кампаний более простым, а потому и привлекательным.

Технологии DCO обеспечивают краткосрочную производительность, поскольку машинное обучение оптимизируется исключительно для достижения результатов. Он не полагается на «интуицию» относительно того, что работает, а что нет. Инструменты искусственного интеллекта могут выявлять отношения и корреляции, которые люди не обязательно видят между клиентами и различными результатами креатива.

Вместо того, чтобы просто тестировать части рекламы, они также оптимизируют ее на основе характеристик клиентов. Затем ИИ может изолировать переменные, которые с наибольшей вероятностью помогут достичь целей рекламодателя, и соответствующим образом изменить креатив.

А благодаря появлению генеративной технологии искусственного интеллекта рекламодатели могут передавать на аутсорсинг такие задачи, как написание текста, вставку изображений или изменение фона с помощью инструментов искусственного интеллекта, что обеспечивает возможность творческого производства в больших масштабах, что, в свою очередь, создает больше возможностей для тестирования.

Иногда бренды прибегают к A/B-тестированию (всего с двумя вариантами), потому что у них нет времени придумывать множество различных фрагментов текста и вариантов изображений. И тут снова приходит генеративный искусственный интеллект, ведь он ускоряет процесс композиции, поэтому бренды могут исследовать множество идей.

Можно сгенерировать хоть 10–15 вариантов, затрачивая на это минимум ресурсов и их сил. Маркетологи по-прежнему могут просмотреть креатив перед его публикацией.

Дальнейшее развитие DCO

Чтобы оставаться жизнеспособным, технологиям DCO придется бороться с потерей сигнала. Поскольку сторонние файлы cookie устарева-

ют, а другие сигналы, такие как, IP-адреса и идентификаторы мобильных устройств перестают работать, брендам будет сложнее идентифицировать и сегментировать аудиторию и измерять результаты.

Чтобы в будущем эффективно обслуживать рекламу DCO, поставщикам необходимо будет иметь связи как со стороной покупателя, так и со стороной продавца. Таким образом, они будут извлекать выгоду лишь из обратной связи, которая и будет использовать DCO.

Лучшими компаниями, для показа рекламы DCO, после потери сигнала будут такие компании как: Google, Meta и Amazon, из-за их, уже сформированных, огромных объемов данных.

Как бренд или рекламодатель, если вы углубляетесь в DCO, вам нужно спросить себя: ради идей или ради краткосрочных результатов?

Если и то, и другое, рекламодателям следует разработать стратегию, которая сочетает в себе принятие решений человеком и оптимизацию под руководством машин. Но им необходимо глубоко разбираться в процессах, чтобы знать ответ на вопрос: «Где начинается человек и где берет верх машинное обучение?»

DCO на российском рынке

В связи с нынешними реалиями в России, некоторые крупные компании, обладающие обширными базами данных начали разработку своих технологий DCO.

Из таких, мы имеем DCO от компании “Яндекс”. Они создали свою технологию, которая позволяет оптимизировать показ динамического креатива без остановки рекламной кампании для получения наилучшего результата.

С её помощью можно проверить маркетинговые гипотезы, определить, какой CTA работает лучше, какое предложение сработало эффективнее и какая цена товара оптимальна. Она, как и предшественники, использует алгоритмы искусственного интеллекта (AI) для автоматического сопоставления разных вариантов рекламы с правильной аудиторией и выбирает наиболее эффективную комбинацию элементов креатива для конкретного пользователя.

Также, компания “Мэйл.ру” тоже начала развивать эту технологию:

Технология, разработанная Mail.ru Group, ктакже позволяет оптимизировать рекламные кампании в режиме реального времени. Она анализирует данные о поведении пользователей и автоматически подбирает наиболее эффективные варианты рекламных объявлений. Это помогает повысить конверсию и снизить стоимость привлечения клиентов.

Конечно, они только в начале пути, но уже понимают, что данная технология имеет множество преимуществ. Ведь динамические рекламные объявления помогают не только охватить новую аудиторию и сокращают время на настройку и запуск кампании, но и уменьшают необходимость ручной настройки и отслеживания актуальности рекламы.

Список литературы

1. Hana Yoo AdExchanger — What Is The Future Of Dynamic Creative Optimization (DCO)? [Электронный ресурс]. — URL: https://www.adexchanger.com/adexplainer/what-is-the-future-of-dynamic-creative-optimization-dco.
2. A/B/n и MVT-тестирование: польза для бизнеса, сходства и различия [Электронный ресурс]. — URL: https://vc.ru/marketing/316401-a-b-n-i-mvt-testirovanie-polza-dlya-biznesa-shodstva-i-razlichiya.
3. Карпов М. А/Б тесты — что это такое и как проводить? [Электронный ресурс]. — URL: https://vc.ru/productstar/425821-a-b-testy-chto-eto-takoe-i-kak-provodit.
4. Динамические рекламные объявления от Mail.ru Group [Электронный ресурс]. — URL: https://target.my.com/pro/education/online-course/ads-tools/dro.

УДК 004

Применение нейросетей в повседневной жизни человека

Черменёв Никита Михайлович

студент факультета Рекламы и связей с общественностью Российского государственного гуманитарного университета

***Аннотация**: Статья исследует влияние нейронных сетей на современное общество и поведение отдельного человека. В статье рассматривается роль нейросетей в различных сферах повседневной жизни, включая медицину, образование, развлечения, транспорт и работу. Основное внимание уделяется преимуществам и недостаткам использования нейросетей в повседневных ситуациях, таких как улучшение качества жизни, обеспечение безопасности и конфиденциальности данных, а также влияние на человеческие отношения. Статья также рассматривает перспективы развития нейросетевых технологий в будущем и их возможное влияние на общество.*

***Abstract**: The article explores the impact of neural networks on modern society and individual behavior. The article discusses the role of neural networks in various areas of daily life, including medicine, education, entertainment, transportation, and work. The focus is on the advantages and disadvantages of using neural networks in everyday situations, such as improving quality of life, ensuring data security and privacy, and the impact on human relationships. The article also looks at the prospects of neural network technology and its possible impact on society.*

***Ключевые слова**: нейросети, искусственный интеллект, повседневная жизнь, медицина, образование, развлечения, транспорт, работа, безопасность данных, эффективное использование, вызовы, риски.*

***Keywords**: neural networks, artificial intelligence, daily life, medicine, education, entertainment, transport, work, data security, effective use, challenges, risks.*

В области науки нейросети применяются для анализа обширных данных, что открывает новые возможности для исследователей. Благодаря этому они могут проводить анализ данных быстрее и точнее, чем когда-либо прежде, что ускоряет научный прогресс. Это позволяет ученым совершать более сложные исследования и делать более точные выводы, что способствует развитию в различных областях науки.

Использование нейросетей в медицине — это новейшее достижение, которое сделало возможным быстрое и точное диагностирование заболеваний. Благодаря этим технологиям врачи могут предсказать развитие болезней и начать лечение на ранней стадии, что повышает шансы пациентов на выздоровление.

В области искусственного интеллекта нейросети играют ключевую роль, способствуя созданию систем машинного обучения, которые могут обучаться и адаптироваться самостоятельно. Это привело к появлению инновационных технологий, таких как автономные автомобили, способные принимать решения на дороге, а также персональные ассистенты, оснащенные умением понимать человеческий язык и выполнять сложные задачи.

В современной повседневной действительности мы нередко встречаем и вступаем в контакт с нейросетями, которые, не сознавая этого, используются в системах рекомендаций. Они анализируют наши предпочтения и прошлые выборы, предлагая нам товары и услуги, что значительно улучшает наш пользовательский опыт. Также нейросети активно задействуются в системах распознавания речи, таких как Siri и Google Assistant, что позволяет голосовым командам управлять нашими устройствами. Необъятные возможности нейросетей также применяются в области безопасности, где они помогают обеспечивать нашу защиту, распознавая наши лица.

Медицина

В сфере медицины нейросети стали неотъемлемой частью, применяясь во многих областях, начиная от разработки новых препаратов до диагностики заболеваний. Одним из ключевых применений нейросетей в медицине являются диагностические исследования, где они способны быстро и точно анализировать большие объемы медицинских данных. Особенно ценны они при обработке медицинских изображений, таких как МРТ и КТ. Нейросети могут выявлять патологии, которые могли бы остаться незамеченными для человеческого глаза, что улучшает точность диагностики и сокращает время, затраченное на анализ каждого изображения.

Нейросети активно применяются в медицине не только для диагностики, но и для предсказания развития болезней. Они способны анали-

зировать данные пациентов, включая их медицинскую историю, и прогнозировать дальнейшее состояние. Это помогает врачам принимать обоснованные решения о терапии, подбирая оптимальное лечение для каждого индивидуума.

Важную роль нейросети также играют в разработке новых препаратов. Они могут изучать разнообразные молекулы и прогнозировать их потенциальную эффективность в борьбе с различными заболеваниями. Это способствует ускорению процесса создания новых лекарств, сокращая время и ресурсы, необходимые для проведения традиционных клинических испытаний.

Творчество

Сегодня нейросети активно внедряются в области творчества, такие как кино, искусство и живопись, принося свежие идеи и раскрывая новые перспективы. В кинематографе нейросети открывают возможности для создания уникальных фильмов и спецэффектов, давая новое видение творческому процессу. В искусстве нейросети могут вдохновлять на создание оригинальных произведений, воссоздавая стиль известных мастеров и придавая им новый смысл. В живописи нейросети способны порождать удивительные шедевры, перенося нас в мир фантазии и экспериментов.

Благодаря процессу «стилевого переноса», нейросеть способна принимать стиль одной картинки, изучать его и применять к другой, тем самым порождая уникальные произведения искусства. Это открывает новые горизонты для творчества и вдохновляет на создание оригинальных и уникальных работ.

В кинематографии нейросети нашли свое применение в создании визуальных эффектов, анимаций, а также в генерации сюжетов. Они способны изучать опыт предыдущих фильмов и делать прогнозы относительно потенциального успеха будущих кинолент. Это помогает кинематографистам создавать новые сюжеты и эффекты, повышая качество и интригу кинопроизведений.

Художники теперь могут воспользоваться помощью нейросетей в области искусства, чтобы обрести новые идеи и вдохновение. Генерация новых форм и паттернов стала возможной благодаря этому инструменту, что

открывает художникам новые возможности для экспериментов с различными стилями и формами. Нейросети стали мощным инструментом, который позволяет творческим личностям расширить свой творческий потенциал, создавая уникальные и оригинальные произведения искусства.

Мир звуковых произведений открывает перед нами новые возможности благодаря нейросетям, которые активно применяются в создании музыки. Алгоритмы машинного обучения позволяют им анализировать огромное количество музыкальных произведений различных жанров, эпох и стилей, изучая разнообразные элементы, такие как ритмика, мелодика и структура.

Постепенно обучаясь, нейросети начинают выявлять уникальные шаблоны и закономерности, присущие музыке, от простых аккордовых последовательностей до сложных музыкальных структур. Благодаря методам машинного обучения, нейросети смогли сделать шаг вперед, начав «понимать» эти шаблоны и применять их для создания оригинальных композиций.

IT

С использованием IT технологий открываются перед композиторами и музыкантами совершенно новые перспективы. Нейросети позволяют им творить уникальные музыкальные произведения, которые ранее были бы недоступны для человеческого творчества. Создание новых мелодий и песен становится возможным благодаря использованию искусственного интеллекта. Таким образом, данные технологии не только содействуют развитию музыкального искусства, но и способствуют его трансформации, формируя совершенно новые звуковые и музыкальные образы.

Современные IT-технологии претерпевают значительные изменения благодаря нейросетям, которые играют важную роль. Обработка данных и их прогнозирование являются ключевыми функциями нейросетей, особенно в области больших данных. Выявление скрытых паттернов и трендов, а также анализ огромного объема информации позволяют компаниям принимать обоснованные решения на основе этих данных.

В мире, где интерфейсы становятся все более естественными и интуитивно понятными, нейросети активно применяются для распознавания

изображений и речи. Их способность обучаться на примерах и повышать точность со временем делает их неотъемлемой частью систем, таких как автоматическое управление транспортными средствами.

Системы искусственного интеллекта, основанные на нейросетях, обладают уникальными возможностями, позволяющими им самостоятельно обучаться и адаптироваться, минуя необходимость явного программирования. Эти системы находят применение в различных областях, включая борьбу с киберугрозами. Используя свою способность учиться на прошлых инцидентах, они успешно обнаруживают и пресекают новые атаки.

В медицинской сфере нейросети с успехом применяются для диагностики заболеваний, анализируя данные и изображения пациентов, что позволяет выявлять признаки болезней на ранних этапах. Кроме того, эти системы играют важную роль в создании персонализированных систем рекомендаций. Анализируя предпочтения и поведение пользователей, они предлагают наиболее подходящие товары и услуги.

Промышленность внедряет нейросети для прогнозирования отказов оборудования и повышения его надежности. Это позволяет избежать дорогостоящих простоев и ремонта. Нейросети обучаются на данных о работе оборудования, что помогает проводить своевременное техническое обслуживание и предотвращать неожиданные проблемы.

Автоматический контроль качества продукции. Нейросети способны быстро и точно обнаруживать дефекты на изделиях, что повышает эффективность процесса проверки качества. Это приводит к сокращению потерь от брака, увеличению удовлетворенности заказчиков и обеспечивает высокий уровень качества продукции. Оптимизация рабочих процессов. Нейросети анализируют огромные объемы данных о производственных процессах, что помогает находить наилучшие способы их выполнения. Это способствует сокращению времени выполнения процессов, уменьшению расходов на материалы и энергию, а также увеличивает общую продуктивность труда.

В промышленности широко применяются нейросети для распознавания образов на фотографиях и видео. Это позволяет автоматизировать контроль качества и сортировку изделий, а также обнаруживать и классифицировать объекты в условиях производства. Управление роботами

становится все более популярным, поскольку нейросети обучаются управлять роботами, автоматизируя сложные и опасные для человека задачи. Это приводит к улучшению безопасности рабочего места, снижению рисков и возможности перераспределения ресурсов на более сложные задачи.

Современная промышленность нашла в нейросетях мощный инструмент, который позволяет улучшить качество продукции, снизить затраты и повысить эффективность работ. Нейросети способны обрабатывать информацию на высоком уровне и с несравненной скоростью, что делает их ценным активом в производстве.

Вывод

Нейросети играют неоценимую роль в многих аспектах нашей повседневной жизни, хотя мы можем и не всегда осознавать этого. Их применение встречается практически повсеместно и затрагивает широкий спектр различных приложений.

Одним из наиболее заметных примеров применения нейросетей являются системы рекомендаций в интернет-магазинах. Они анализируют наши предыдущие покупки и интересы, чтобы предложить нам товары, которые могут нас заинтересовать.

Распознавание речи в наших смартфонах и других устройствах также обеспечивается с помощью нейросетей. Когда вы используете голосового помощника, такого как Siri или Google Assistant, их способность понимать ваши запросы обусловлена применением нейросетей.

В автономных автомобилях нейросети используются для обработки и интерпретации данных с датчиков и камер. Они помогают автомобилям «видеть» окружающий мир и принимать решения на основе этой информации. В области здравоохранения нейросети играют важную роль в диагностике заболеваний. Они способны анализировать медицинские изображения, помогая врачам определить наличие или отсутствие заболеваний. Наконец, социальные сети используют нейросети для анализа наших интересов и предпочтений. Это помогает им предлагать нам наиболее интересный и релевантный контент, улучшая тем самым наш опыт использования этих платформ.

В целом, можно сказать, что нейросети играют центральную роль в многих аспектах нашей повседневной жизни, значительно улучшая качество и удобство многих сервисов и технологий, которыми мы пользуемся каждый день.

Список литературы

1. Горбань А.Н. (1990) Обучение нейронных сетей. 156 с.
2. Вакуленко С.А. (2018) Практический курс по нейронным сетям. 22 с.
3. Горожанина Е.И. (2017) Нейронные сети. 118 с.
4. Барский А.Б. (2016) Введение в нейронные сети. 68 с.

УДК 004

Технические аспекты практического применения системы рейтинга в Китае

Салина Анна Сергеевна

студент Российского университета транспорта

Гринчар Николай Николаевич

доцент Российского университета транспорта

***Аннотация**: В данной статье были рассмотрены технологии, применяемые в системе рейтинга в Китае. Работа отражает специфику технической реализации и внедрения системы, проблемы и некоторые прогнозы на ее дальнейшее развитие.*

***Abstract**: This paper examined the technology used in the rating system in China. The paper reflects the specifics of the technical realization and implementation of the system, the problems and some predictions for its future development*

***Ключевые слова**: Китай, технологии, анализ данных, система, рейтинг, развитие, цифровизация, проблема, влияние, цифровое общество.*

***Keywords**: China, technology, data analysis, system, ranking, development, digitalisation, problem, impact, digital society.*

В связи с развитием общества и цифровых технологий, в частности, нельзя не отметить повсеместное внедрение технологий в обычную жизнь. Существующая в КНР Система социального рейтинга граждан является ярчайшим примером синергии государства с новейшими технологиями. Однако, в данной ситуации цифровая трансформация государства еще не окончена — это длительный, и с каждым разом совершенствующийся, процесс[1]. Но даже в этом случае можно делать выводы не только об уже существующих технологиях, но и прогнозировать их дальнейшее развитие.

Усиление внимания к проблематике системы рейтинга связано в первую очередь с разработкой новейших компьютерных технологий и способов обработки данных. На основе данных, опубликованных в официальных документах[3] и законодательных актах, а так же публикаций в официальных СМИ Китая, можно сделать выводы о применяемых технологиях.

Можно выделить основные, наиболее востребованные и современные технологии, которые уже применяются, либо которые будут применяться в ближайшее время:

1. Искусственный интеллект (ИИ): в системе социального кредита в Китае данные технологии применяются для анализа и обработки больших объемов данных, выявления шаблонов поведения и принятия решений о рейтинге граждан и организаций.
2. Большие данные (Big Data): для сбора, хранения и анализа данных о поведении граждан и организаций используются технологии больших данных, которые позволяют эффективно обрабатывать информацию из различных источников.
3. Облачные технологии: для хранения и обработки данных применяются облачные хранилища, обеспечивающие высокую доступность, масштабируемость и безопасность информации.
4. Биометрическая идентификация: для уникальной идентификации граждан в рамках системы социального кредита могут использоваться биометрические технологии, такие как сканирование отпечатков пальцев, распознавание лиц и другие методы. (Данная технология реализована в качестве очков дополненной реальности с функцией распознавания лиц для служащих транспортных объектов.)

5. Кибербезопасность: с учетом значительного объема данных, собираемых в рамках системы социального кредита, важным элементом является применение технологий кибербезопасности и контроля доступа для защиты информации от несанкционированного доступа и утечек.
6. Блокчейн-технологии: некоторые регионы в Китае экспериментируют с использованием блокчейна для обеспечения прозрачности, надежности и целостности данных в системе социального кредита.
7. Машинное обучение: технологии машинного обучения применяются для создания алгоритмов анализа данных, выявления закономерностей и прогнозирования поведения граждан и организаций.
8. Геолокация: технологии геолокации могут быть использованы для отслеживания местоположения граждан и организаций, что может быть важным для определения их активности и соответствия правилам и нормам.
9. Аналитика данных: для обработки и анализа данных, собранных в рамках системы, применяются современные методы аналитики данных, такие как машинное обучение, статистические методы и другие.
10. Распределенные реестры: в некоторых случаях могут быть использованы технологии распределенных реестров для хранения информации о рейтингах граждан и организаций, обеспечивая прозрачность и надежность данных.
11. Цифровые идентификаторы: для уникальной идентификации граждан и организаций в системе социального кредита могут применяться цифровые идентификаторы, которые облегчают процесс сбора и анализа данных.
12. Мобильные приложения: для удобства пользователей системы социального кредита разрабатываются мобильные приложения, позволяющие отслеживать свой рейтинг, получать уведомления и управлять своими данными.
13. Цифровая подпись: для обеспечения подлинности и целостности данных используются цифровые подписи, которые позволяют проверить авторство информации и защитить ее от подделок. Данная технология особенно востребована в государственных структурах.

    И многие другие.

Однако, не все имеющиеся технологии используются на данный момент, или используются не в полной мере. Так, на территории Китая существуют как развитые в технологическом плане регионы, так и менее развитые, где данная система рейтинга до сих пор не была введена[2]. К тому же, внедрение и поддержание системы рейтинга требует значительных технических ресурсов, а также специализированных адаптированных алгоритмов и инфраструктуры для сбора и обработки данных. Эти сложности затрудняют эффективное функционирование системы в Китае. В целом, с технической точки зрения, внедрение и стабильное функционирование системы рейтинга требуют разработки сложных технологических решений, высокой степени автоматизации и обработки данных, а также строгого контроля качества информации для обеспечения эффективности и надежности системы.

В итоге рассмотрения данного вопроса можно сделать вывод о том, что в процессе совершенствования технологий будут происходить как улучшение системы рейтинга, так и развитие цифровой структуры в контексте государства. Происходит это неравномерно, однако, развитие, так или иначе, неизбежно ввиду огромного влияния технологий на современную жизнь.

Список литературы

1. Рувинский Р. З. Правовые аспекты внедрения системы социального кредита в современное публичное управление: монография / Р. З. Рувинский. — Н. Новгород: НИУ РАНХиГС, 2022.— 264 с. ISBN 978–5–00036–290–7.
2. Dander, Valentin [Hrsg.]; Bettinger, Patrick [Hrsg.]; Ferraro, Estella [Hrsg.]; Leineweber, Christian [Hrsg.]; Rummler, Klaus [Hrsg.] Digitalisierung — Subjekt — Bildung. Kritische Betrachtungen der digitalen Transformation Opladen; Berlin; Toronto: Verlag Barbara Budrich 2020, 276 S. (Критические аспекты цифровой трансформации) ISBN 978–3–8474–2350–8, DOI 10.3224/84742350.
3. 国务院关于印发社会信用体系建设规划纲要 (2014–2020 年)/"Planning Outline for the Construction of a Social Credit System (2014–2020)" (Уведомление Государственного Совета КНР об издании Плана построения системы социального кредита на 2014–2020 гг.) GF No. (2014)21.

УДК 004

Разработка проектного решения по автоматизации обработки нарядов на тестирование и установку на полигонах эксплуатации ИТ-проектов

Зудов Федор Евгеньевич

студент кафедры Информационных систем цифровой экономики Института экономики и финансов Российского университета транспорта

***Аннотация**: Данная статья представляет собой исследование организационной структуры и бизнес-процессов в контексте управления процессами передачи и установки программного обеспечения (ПО) в организации. Анализируются основные проблемы, возникающие при передаче и установке ПО, и предлагаются решения на основе автоматизации с использованием современных информационных технологий. Проектирование и разработка системы управления нарядами на тестирование и установку ПО также являются ключевыми аспектами данного исследования.*

***Abstract**: This paper is a study of organizational structure and business processes in the context of managing software transfer and installation processes in an organization. The main problems arising in software transfer and installation processes are analyzed and solutions based on automation using modern information technologies are proposed. The design and development of a system for managing software testing and installation work orders are also key aspects of this study.*

***Ключевые слова**: управление процессами передачи ПО, проектирование системы управления, качество обслуживания клиентов, процессы передачи и установки ПО.*

***Keywords**: software transfer process management, management system design, customer service quality, software transfer and installation processes.*

Организации, занимающиеся разработкой и эксплуатацией программного обеспечения, сталкиваются с рядом сложностей при передаче и установке ПО на объектах эксплуатации. Эффективное управление этими процессами играет важную роль в обеспечении качественного обслуживания клиентов и повышении эффективности работы организации в целом.

Рассмотрение структуры организации, включая подразделения, их функции и взаимосвязи, позволяет понять организационную динамику

и определить ответственность за процессы передачи и установки ПО. Изучение бизнес-процессов в данной области выявляет ключевые этапы и задачи, необходимые для успешной реализации проектов.

Анализ типичных проблем и вызывающих их факторов при передаче и установке ПО позволяет оценить текущие методы управления и контроля процессов нарядов. Оценка влияния этих проблем на эффективность работы организации и качество обслуживания клиентов является важным этапом в разработке решений.

Исследование существующих подходов и методов решения проблем передачи и установки ПО включает анализ современных технологий и инструментов автоматизации процессов. Определение требований к автоматизированному рабочему месту (АРМ) для разработчиков, группы сопровождения и группы эксплуатации является важным шагом в создании эффективной системы управления процессами.

Проектирование архитектуры веб-приложения для управления процессом нарядов на тестирование и установку ПО представляет собой ключевой этап в разработке решений. Автоматизация обработки нарядов, контроль исполнения задач и генерация отчетности позволяют оптимизировать процессы и повысить эффективность работы организации.

Автоматизация управления процессами передачи и установки ПО в организации является важным направлением развития для повышения эффективности работы и качества обслуживания клиентов. Проектирование и внедрение системы управления нарядами на тестирование и установку ПО с использованием современных информационных технологий позволяет эффективно решать типичные проблемы и повышать уровень сервиса организации.

Одним из важных шагов в автоматизации процессов управления нарядами на тестирование и установку ПО является интеграция с уже существующими системами в организации, такими как системы управления проектами, системы учета задач, а также системы мониторинга и аналитики. Интеграция позволит создать единую информационную среду, обеспечивающую целостную и оперативную обработку данных.

При внедрении новой системы управления процессами важно обеспечить обучение персонала и изменить культуру организации в отношении

важности и эффективности автоматизированных процессов. Это может включать в себя проведение тренингов, разработку руководств по использованию новой системы и проведение мероприятий по вовлечению сотрудников.

После внедрения системы управления нарядами на тестирование и установку ПО необходимо провести регулярный анализ процессов с целью выявления узких мест и возможностей для оптимизации. Это поможет постоянно совершенствовать систему и обеспечивать ее соответствие изменяющимся потребностям организации.

При разработке и внедрении системы управления нарядами необходимо уделить особое внимание вопросам безопасности и конфиденциальности данных. Это включает в себя защиту от несанкционированного доступа к информации о нарядах, шифрование данных и соблюдение соответствующих нормативных требований и стандартов.

При проектировании системы управления нарядами необходимо учитывать ее масштабируемость и гибкость, чтобы она могла эффективно функционировать как для небольших проектов, так и для крупных корпоративных систем. Гибкость системы позволит легко адаптировать ее под изменяющиеся потребности и условия работы организации.

Разработка системы управления нарядами на тестирование и установку ПО должна рассматриваться как непрерывный процесс совершенствования. Постоянное внимание к обратной связи от пользователей, анализу результатов и внесению коррективов поможет обеспечить высокую эффективность и качество работы системы в долгосрочной перспективе.

Список литературы

1. Лутц М Изучаем Python Том 1 / М Лутц. — СПб: Вильямс, 2019.— 832 с. — ISBN 978–5–907144–52–1
2. Хеллман Д Стандартная библиотека Python 3. Справочник с примерами / Д Хеллман. — Москва; СПб: Вильямс, 2018.— 1376 с. — ISBN 978–5–6040043–8–8
3. Бриггс, Дж., Python для детей. Самоучитель по программированию / Дж., Бриггс,. — Москва: Манн, Иванов и Фербер, 2017.— 320 с.

4. Куликов С.С Тестирование программного обеспечения. Базовый курс / С.С Куликов. — Минск: Четыре четверти, 2020.— 310 с.
5. Плаксин М. А. Тестирование и отладка программ для профессионалов будущих и настоящих / М. А. Плаксин. — Москва: БИНОМ. Лаборатория знаний, 2013.— 167 с.
6. Канер Сэм и др. Канер Сэм и др. Тестирование программного обеспечения. Фундаментальные концепции менеджмента бизнес-приложений / Канер Сэм и др. Канер Сэм и др.. — Москва: «ДиаСофт», 2001.— 544 с.
7. Игнатьев А. В. Тестирование программного обеспечения / А. В. Игнатьев. — Москва: Лань, 2022.— 56 с.

УДК 004

Обзор уязвимостей и методов защиты контейнеров

Гальцев Павел Николаевич

студент кафедры Информационных систем цифровой экономики Российского университета транспорта

Научный руководитель **Морозова Вера Ивановна**

кандидат экономических наук, доцент кафедры Информационных систем цифровой экономики Российского университета транспорта

***Аннотация**: Современные информационные технологии все чаще используют контейнеризацию для упаковки и развертывания приложений. Однако, уязвимости контейнеров становятся серьезной угрозой для безопасности IT-систем. В данной статье рассматривается проблема уязвимостей контейнеров, их возможные последствия и методы защиты от них.*

***Abstract**: Modern information technology is increasingly using containerization to package and deploy applications. However, container vulnerabilities are becoming a serious threat to the security of IT systems. This paper discusses the problem of container vulnerabilities, their possible consequences, and methods to protect against them.*

***Ключевые слова**: контейнеры, уязвимости, безопасность, сканеры контейнеров, информационная безопасность.*

***Keywords**: containers, vulnerabilities, security, container scanners, information security.*

С развитием информационных технологий и широким распространением облачных вычислений контейнеризация стала неотъемлемой частью современной разработки программного обеспечения. Контейнеризация представляет собой технологию, которая позволяет упаковать приложение со всеми необходимыми зависимостями и конфигурациями в единый контейнер. Это обеспечивает лёгкость развёртывания, управления и масштабирования приложений, а также повышает их переносимость между различными средами.

Однако, несмотря на все преимущества контейнеризации, она также создаёт новые вызовы в области безопасности. Контейнеры могут стать уязвимыми для различных видов атак, таких как вредоносный код, уязвимости в программном обеспечении и несанкционированный доступ.

Для обеспечения безопасности контейнеров необходимо использовать специальные инструменты и технологии. В данной статье мы рассмотрим основные уязвимости контейнеров и методы защиты.

Вот некоторые из главных уязвимостей контейнеров:

1. Уязвимости образов: Образы контейнеров могут содержать уязвимости в программном обеспечении, операционных системах и библиотеках. Эти уязвимости могут быть использованы для получения доступа к контейнеру после его развертывания.
2. Неправильная конфигурация: Контейнеры могут быть неправильно сконфигурированы, что делает их уязвимыми для атак. Например, контейнер может быть настроен с открытыми портами, которые не используются, или с разрешениями, которые слишком широки.
3. Уязвимости цепочки поставок: Злоумышленники могут внедрять вредоносный код в образы контейнеров на ранних этапах цепочки поставок. Когда эти образы развертываются, вредоносный код может получить доступ к производственным системам.

4. Уязвимости хоста: Контейнеры работают на хост-системах, которые также могут быть уязвимыми. Злоумышленники могут использовать уязвимости хоста для получения доступа к контейнерам.
5. Утечки данных: Контейнеры могут содержать конфиденциальные данные, такие как пароли или ключи API. Эти данные могут быть украдены злоумышленниками, если контейнеры не должным образом защищены.

К сожалению, нет волшебного средства, которое могло бы решить все уязвимости контейнеров, но есть базовые рекомендации, следуя которым, можно значительно обезопасить себя. На каждый конкретный случай, есть решение. В общем виде существует несколько рекомендаций для защиты контейнеров от этих уязвимостей:

1. Использование надежных образов: Необходимо использовать образы контейнеров из надежных источников.
2. Регулярное обновление программного обеспечения: Все программное обеспечение в контейнерах должно быть обновлено до последних версий.
3. Правильная настройка контейнеров: Контейнеры необходимо настроить таким образом, чтобы они были наиболее безопасными. Например, использовать принцип наименьших привилегий и закрывать ненужные порты.
4. Сканирование контейнеров: Необходимо производить регулярное сканирование контейнеров на наличие уязвимостей.
5. Изолирование контейнеров: Необходимо использовать сети контейнеров и другие методы изоляции, чтобы отделить контейнеры друг от друга и от хост-системы.
6. Шифрование данных: Необходимо шифровать конфиденциальные данные, которые хранятся в контейнерах.

Использование этих мер безопасности поможет защитить контейнеры от уязвимостей и повысить уровень безопасности приложений.

Список литературы

1. Годзурас, Э. Docker compose для разработчика / Э. Годзурас. — Москва: DMK press, 2023.— 220 с. — ISBN 978–5–93700–203–7.

2. Кочер П. С. Микросервисы и контейнеры Docker / П. С. Кочер. — Москва: ДМК Пресс, 2019.— 240 с.
3. Моуэт, Э. Использование Docker / Э. Моуэт. — Москва: ДМК Пресс, 2022.— 354 с.
4. Сейерс Э. Х. Docker на практике / Э. Х. Сейерс, А. Милл. — Москва: ДМК Пресс, 2020.— 516 с.

УДК 004

Основные принципы работы современного языка программирования 1С

Филин Дмитрий Олегович

студент кафедры Информационных систем цифровой экономики Российского университета транспорта

Научный руководитель **Медникова Оксана Васильевна**

кандидат технических наук, доцент кафедры Информационных систем цифровой экономики Российского университета транспорта

***Аннотация**: В последние годы в Российской Федерации активно развивается импортозамещение в области информационных технологий. Одним из ключевых направлений является замена импортного программного обеспечения отечественным. В данной статье будет рассмотрен современный язык программирования 1С. Данный язык является ведущим инструментом для разработки прикладных решений в области автоматизации учета и управления предприятий. В статье будут подробно рассмотрены основные принципы работы языка 1С. Данная статья предназначена как для опытных, так и для начинающих разработчиков на платформе 1С, которые хотят углубить свои знания и повысить эффективность создаваемых ими решений.*

***Abstract**: In recent years, the Russian Federation has been actively developing import substitution in the field of information technologies. One of the key directions is the replacement of imported software with domestic software. This article will consider the modern programming language 1C. This language is the leading tool for the development of applied solutions in the field of automation of accounting and management of enterprises. The article will discuss the basic principles of the 1C language in detail. This article is intended for both experienced and*

novice 1C platform developers, who want to deepen their knowledge and increase the effectiveness of the solutions they create.

***Ключевые слова**: 1С, язык программирования, объектно-ориентированное программирование, событийно-ориентированный механизм, система управления базами данных, язык запросов, расширения и дополнения, управление данными.*

***Keywords**: 1C, programming language, object-oriented programming, event-oriented mechanism, database management system, query language, extensions and additions, data management.*

В современном цифровом мире ключевую роль в автоматизации бизнес-процессов, управлении данными и повышении эффективности организаций играет программное обеспечение. Язык программирования 1С занимает лидирующие позиции в разработке прикладных решений для автоматизации учета и управления, который достаточно широко используемых в российских компаниях и государственных учреждениях.

Язык 1С — это мощная и гибкая платформа, сочетающая в себе современные принципы и подходы к программированию. Понимание основных принципов работы этого языка необходимо разработчикам, стремящимся создавать эффективные, масштабируемые и надежные приложения.

В представленной статье будут рассмотрены ключевые концепции и механизмы, лежащие в основе современного языка программирования 1С. Понимание этих принципов поможет разработчикам более эффективно использовать возможности языка 1С, создавать качественный код и решать сложные задачи по автоматизации бизнес-процессов. Кроме того, знание основ языка 1С поможет лучше оценить его преимущества, ограничения и перспективы развития в контексте современных тенденций в разработке программного обеспечения.

Первым будет рассмотрена такая концепция, как «Объектно-ориентированный подход».

Поскольку в основе языка 1С лежит парадигма объектно-ориентированного программирования, это означает, что программный код организован в виде объектов, обладающих определенными свойствами и методами (функциями). Объекты могут взаимодействовать и наследовать свойства

друг от друга, что обеспечивает гибкость и расширяемость программного кода. Объектно-ориентированный подход позволяет разработчикам структурировать код и создавать модульные, легко поддерживаемые и расширяемые приложения. Это также способствует повторному использованию кода и облегчает сотрудничество между разработчиками в рамках крупных проектов.

Следующим будет рассмотрен «событийно-ориентированный механизм».

В 1С реализован событийно-ориентированный механизм, который позволяет программному коду реагировать на различные события, происходящие в системе, такие как открытие формы, нажатие кнопки, изменение данных и так далее. Разработчик может определить обработчики событий — процедуры, которые будут выполняться при возникновении соответствующего события. Событийно-ориентированный подход обеспечивает гибкость и адаптивность приложений, позволяя им динамически реагировать на действия пользователя и изменения в системе. Это упрощает разработку интерактивных пользовательских интерфейсов и предоставляет возможность создавать сложную бизнес-логику.

Ещё одной из основных концепций является «Визуальная среда разработки».

1С предоставляет визуальную среду разработки, значительно упрощающую процесс создания программных приложений. Разработчик может создавать формы, отчеты, разного типа обработки и другие объекты с помощью встроенных визуальных конструкторов без необходимости писать большой объем кода вручную. Визуальная среда разработки повышает производительность разработчиков, позволяя быстро создавать прототипы и визуализировать элементы пользовательского интерфейса. Она также облегчает совместную работу над проектами, предоставляя единую среду для создания, отладки и тестирования приложений.

Так же заслуживает внимания «Интегрированная система управления базами данных».

В 1С встроена собственная система управления базами данных (СУБД), обеспечивающая хранение и обработку данных. Язык 1С предоставляет инструменты для работы с данными, такие как запросы, транзакции и блокировки. Это позволяет создавать надежные и эффективные приложения для

управления информацией. Интегрированная СУБД упрощает разработку, устраняя необходимость использования сторонних систем управления базами данных. Он также обеспечивает высокую производительность и оптимизацию для задач, связанных с обработкой больших объемов данных.

«Клиент-серверная архитектура» как один из основных механизмов работы языка 1С.

Приложения 1С могут работать в режиме клиент-сервер, где сервер выполняет основную часть обработки данных, а клиенты взаимодействуют с сервером для выполнения операций и отображения данных. Такой подход обеспечивает масштабируемость и возможность одновременной работы сразу нескольких пользователей. Клиент-серверная архитектура позволяет распределять нагрузку между большим количеством узлов, что в свою очередь повышает производительность и отказоустойчивость системы. Также благодаря этому упрощается администрирование и обновление приложений, так как изменения необходимо вносить только на сервере.

Самым важным для понимания является «Встроенный язык запросов».

В 1С реализован собственный язык запросов, позволяющий выполнять сложные операции выборки, обработки и агрегирования данных. Язык запросов основан на синтаксисе SQL, однако имеет ряд расширений, возможностей и особенностей, специфичных для 1С. Встроенный язык запросов обеспечивает гибкость при работе с данными, позволяя разработчикам создавать сложные отчеты и выполнять аналитические задачи, что также упрощает интеграцию с другими системами и источниками данных.

Последним в этой статье будет описан «Механизм расширений и дополнений».

Платформа 1С имеет в себе механизм расширений и дополнений, позволяющий разработчикам создавать дополнительные компоненты и расширять функциональные возможности системы. Это обеспечивает гибкость и возможность адаптировать приложения к конкретным бизнес-требованиям. Механизм расширений и дополнений способствует развитию экосистемы 1С, позволяя другим разработчикам создавать и распространять дополнительные модули и библиотеки. Это способствует расширению возможностей платформы и обеспечению более быстрой адаптации к стремительно меняющимся потребностям пользователей.

Заключение

Описанные выше основные принципы языка программирования 1С позволяют разработчикам создавать высококачественные, эффективные и масштабируемые приложения для автоматизации бизнес-процессов и управления данными, кроме того, они обеспечивают высокую производительность и надежность создаваемых решений.

Понимание основных принципов языка 1С важно для разработчиков, стремящихся повысить свою квалификацию и создавать эффективные, масштабируемые, надежные приложения. Знание этих принципов позволяет лучше использовать возможности платформы, создавать качественный код и решать сложные задачи автоматизации. Кроме того, это помогает оценить преимущества, ограничения и перспективы развития языка 1С в контексте современных тенденций разработки программного обеспечения.

Список литературы

1. Радченко М.Г., Хрусталева Е.Ю. 1С: Предприятие 8.3. Практическое пособие разработчика. — М.: ООО «1С-Паблишинг», 2020.— 965 с.
2. Рязанцева Н.А., Рязанцев Д.Н. 1С: Предприятие 8.3. Архитектура системы. — М.: ООО «1С-Паблишинг», 2018.— 344 с.
3. Гончаров Д.И., Козлова Е. В. Объектно-ориентированное программирование в 1С: Предприятие 8.3. — М.: ООО «1С-Паблишинг», 2021.— 576 с.
4. Бартеньев О.В. 1С: Предприятие 8.3. Язык запросов. — М.: ООО «1С-Паблишинг», 2019.— 224 с.
5. Филиппов Ю. А. Разработка в системе 1С: Предприятие 8.3. — СПб.: Питер, 2020.— 640 с.
6. Ажеронок В.А. 1С: Предприятие 8.3. Управление базами данных. — М.: ООО «1С-Паблишинг», 2017.— 416 с.
7. Мастицкий С. Э. Программирование в системе 1С: Предприятие 8.3. — М.: Национальный Открытый Университет «ИНТУИТ», 2019.— 352 с.
8. Чупин А. С. Расширения и дополнения в 1С: Предприятие 8.3. — М.: ООО «1С-Паблишинг», 2020.— 288 с.

9. Ажеронок В.А., Смирнова Т. Ю. Клиент-серверная архитектура в 1С: Предприятие 8.3. — М.: ООО «1С-Паблишинг», 2018.— 320 с.

УДК 004.92:371.3

Интеграция 3Д-моделирования в школьное обучение

Карпенко Михаил Андреевич

студент Самарского государственного технического университета

Научный руководитель **Забержинский Борислав Эдуардович**

кандидат технических наук, доцент кафедры Информационных технологий Самарского государственного технического университета

***Аннотация**: В статье рассматривается роль трехмерного моделирования в образовательных программах, обсуждаются преимущества использования 3D-моделей в обучении и вызовы, стоящие перед школами и учениками.*

***Abstract**: This article examines the role of 3D modeling in educational programs, discussing the benefits of using 3D models in learning and the challenges facing schools and students.*

***Ключевые слова**: трехмерное моделирование, образование, 3D-технологии, школьный курс, обучение, будущие специалисты.*

***Keywords**: three-dimensional modeling, education, 3D technologies, school course, teaching, future specialists.*

В наши дни трудно представить сферу производства, где не используется трехмерная объемная графика. Практически для каждого продукта изначально разрабатывается его чертеж. Еще 10–20 лет назад проектировщики использовали обыкновенный холст бумаги и карандаш, но развитие современных технологий привело нас к появлению программ, использующих специальные инструменты для создания и редактирования 3D-объектов. В производственных целях на основе таких объектов инженер может точно представить модель детали или продукта до его реального изготовле-

ния. Это позволяет ускорить процесс разработки, сократить издержки на создание прототипов и улучшить качество конечного продукта.

Технологии трехмерного моделирования активно применяются в различных отраслях промышленности, начиная от автомобильного и авиационного производства (рис. 1), где требуется точное моделирование каждой детали, до медицинских и архитектурных сфер, где трехмерные модели используются для графического представления и анализа сложных структур и объектов.

С развитием компьютерных технологий и программного обеспечения процесс создания и редактирования 3D-объектов становится все более доступным и удобным. Это открывает новые возможности для будущих дизайнеров и инженеров, которые уже начинают интересоваться данной тематикой еще на стадии школьного обучения.

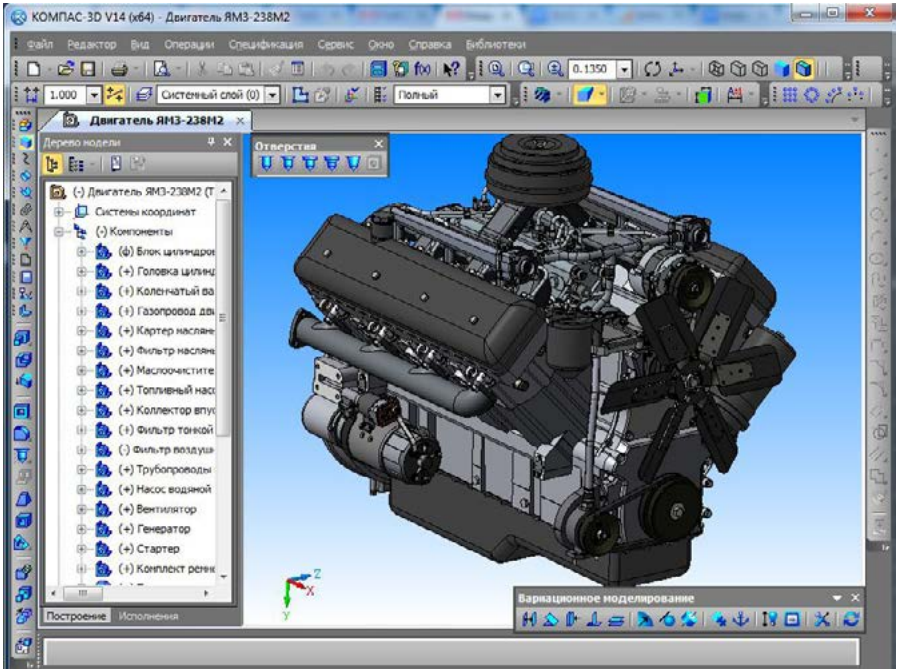

Рисунок 1. **Трехмерная модель двигателя в Компас 3D. [1]**

Однако, если ознакомиться со школьной программой по информатике, а также учебниками, утвержденными приказом Министерства просвещения Российской Федерации № 858 от 21 сентября 2022 года[2], то можно заметить, что полноценный отдельный курс по 3D-моделированию в рамках основного общего образования отсутствует. Соответствующий раздел затрагивается лишь поверхностно, не вдаваясь в подробности.

В таблице 1 приведено сравнение содержания учебников Л. Л. Босовой и А. Ю. Босовой для 7–11 классов, иллюстрирующее области, где встречаются темы, связанные с 3D-моделированием.

Внимательно ознакомившись с таблицей, можно убедиться, что раздел 3D-моделирования подается ученикам только в общих чертах и не рассматривается как самостоятельный раздел. Кроме того, таким темам как «3D-Моделирование» и «Компьютерная графика» вовсе отведено небольшое количество часов, что не позволяет школьникам углубиться и развить свои навыки в данной области.

Но в целом, применение 3D-объектов, как инструмент к пониманию различных учебных материалов, может быть выгодным и эффективным дополнением к обучению. Например, в биологии можно использовать 3D-модели для визуализации внутренней структуры клеток, органов или молекул ДНК, что поможет ученикам лучше понять и запомнить анатомические и биологические процессы. В математике же 3D-моделирование можно использовать для визуализации геометрических фигур и решения задач по стереометрии.

Следует признать, что уже сейчас спектр школьных предметов, включающих в себя элементы 3D-графики довольно широк. В чем же смысл и какова цель ее использования в рамках образования? В первую очередь, это возможность раскрыть и визуализировать учебный материал, делая его более простым и понятным для учащихся, особенно в случае абстрактных или сложных тем. Во-вторых, работа с трехмерными моделями способствует развитию пространственного мышления у учеников, что полезно не только в научных и технических дисциплинах, но и в повседневной жизни. Немаловажным является и то, что использование современных 3D-технологий повышает мотивацию и заинтересованность школьников за счет создания более увлекательного и интерактивного обучающего процесса.

Таблица 1. **Разделы 3D-моделирования в школьном курсе Информатики**

Учебник	**Раздел курса и поурочное планирование**	**Темы уроков, в которых может быть затронут курс «3D-моделирования»**
«Информатика. 7–9 классы» Л. Л. Босова, А. Ю. Босова.	**7 класс:** «Обработка графической информации» Теория: 2 часа; **Практика**: 2 часа.	**7 класс:** «Компьютерная графика»; «Создание графических изображений»; «Обобщение и систематизация знаний по теме Обработка графической информации».
	8 класс: –	**8 класс**: –
	9 класс: «Моделирование и формализация» **Теория**: 6 часов **Практика**: 3 часа	**9 класс:** «Моделирование как метод познания»; «Графические информационные модели»; «Обобщение и систематизация основных понятий темы Моделирование и формализация»
«Информатика. 10 класс» Л. Л. Босова, А. Ю. Босова.	Глава 5. «Современные технологии создания и обработки информационных объектов» Теория: 1 час	«Объекты компьютерной графики»: «Компьютерная графика и её виды»
«Информатика. 11 класс» Л. Л. Босова, А. Ю. Босова.	–	–

Для организации учебного процесса по 3D-моделированию в общеобразовательных учреждениях необходимо наличие следующих элементов:

- Программное обеспечение (Blender, Компас-3D, SketchUP, Cinema4D и т.д.)
- Аппаратное обеспечение (Компьютер)

Среди программ, служащих для создания и редактирования 3Д-моделей можно выделить особо распространенные и полюбившиеся новым пользователям или специалистам, уже давно работающих в своей области[3]. В таблице 2 представлена сравнительная характеристика программ, которые могли бы использоваться в школьной программе, по их цене, функциям и среде применения.

Таблица 2. **Сравнительная характеристика программ по 3Д-моделированию**

Уровень сложности	**Программа**	**Примерная стоимость подписки в год (руб)**	**Среда применения**
Для новичков и любителей	3D Slash	2 200	–
	SculptGL	–	–
	SketchUP	12 000	Строительство, архитектура, ландшафтный дизайн
	FreeCAD	–	Машиностроение, архитектурное проектирование

Уровень сложности	Программа	Примерная стоимость подписки в год (руб)	Среда применения
Для любителей и профессионалов	DesignSpark Mechanical	–	Проектирование изделий и деталей, прототипирование
	Blender	–	Анимация, кино, видеоигры, архитектурное проектирование
	ArchiCAD	20 000	Проектирование зданий и сооружений, планировка квартир
	Autodesk Fusion 360	66 000	Машиностроение, промышленность, проектирование изделий
	Cinema 4D	72 000	Моушн-дизайн, кино, видеоигры, реклама

Опираясь на представленную таблицу, нетрудно заметить, что использование программ, не требующих платной подписки, может быть намного выгоднее для государства. Например, SkulptGL — отличный вариант, чтобы познакомиться с основами 3D-моделирования. Благодаря простому интерфейсу и немалому функционалу можно добиться впечатляющих результатов. Программа является онлайн-браузером и не требует отдельной установки, что облегчит работу сотрудникам школы. SkulptGL может отлично подойти для школьников 7–8 классов и послужить своеобразным стартом в обучении.

Blender — ПО с открытым исходным кодом и бесплатным доступом, чем привлекает новых пользователей. Программа идеально подходит

для освоения трехмерного дизайна — от самых азов до всех его возможностей. Функции Blender позволяет с нуля сформировать 3D-модель при помощи доступных примитивов, полигонов и различных модификаторов. Затем заняться скульптингом, текстурированием, композитингом, рисованием с помощью Grease Pencil, анимацией и рендерингом. Нетребовательность к компьютерному железу может оказаться влияющим фактором выбора программного продукта у большинства школ, не имеющих возможности позволить себе мощное аппаратное обеспечение. Blender не уступает ни одному из своих конкурентов, а в качестве быстроты реагирования на команды и удобного, оптимизированного интерфейса даже превосходит их. Согласно опросу, проведенному среди респондентов 63.45% (335 из 528 проголосовавших) считают, что Blender — программное обеспечение, которое необходимо преподавать в школах для изучения 3D-моделирования[4].

Актуальность использования средств 3D-моделирования в различных школьных дисциплинах растет с каждым годом, в связи с чем возникает ряд сложно решаемых проблем[5]. Например:

1. Финансовые затраты: Приобретение необходимого оборудования и программ может быть дорогостоящим. Не все школы и учреждения дополнительного образования могут позволить себе такие затраты без дополнительного финансирования.
2. Недостаток квалифицированных кадров: На сегодняшний день, учителей и педагогов, обладающих достаточным количеством знаний и опыта в данной области, не так много.
3. Актуализация учебных программ: Быстрое развитие технологий в области 3D моделирования требует постоянного обновления учебных программ и материалов. Необходимо постоянно адаптировать учебные планы к новым тенденциям и технологиям.

Таким образом, можно сказать, что 3D-моделирование, несмотря на сложности, связанные с материальными затратами, несомненно, является тем направлением, обучение которому государству необходимо развивать в общеобразовательных организациях. Поскольку подготовка специалистов в этой области укрепит научно-технический потенциал страны и повысит конкурентоспособность на мировом рынке.

Трехмерное моделирование — новый язык цифровой среды и отличная отправная точка для поиска работы в области компьютерной графики, без которой не обходится ни один современный проект, что, в свою очередь, способствует постоянному поиску новых специалистов. Школьные годы — идеальное время для подростка, чтобы попробовать себя и узнать стоит ли в ближайшем будущем делать упор в столь инновационной сфере.

Список литературы

1. Новостной портал полоцка | новополоцка [Электронный ресурс] // Трехмерное проектирование с помощью Компас 3D системы [сайт]. [2016]. URL: https://polotsk-portal.ru/poleznoe/10422-trehmernoe-proektirovanie-s-pomoschyu-kompas-3d-sistemy.html (дата обращения: 05.03.2024).
2. Приказ Минпросвещения России от 21.09.2022 N 858 «Об утверждении федерального перечня учебников, допущенных к использованию при реализации имеющих государственную аккредитацию образовательных программ начального общего, основного общего, среднего общего образования организациями, осуществляющими образовательную деятельность и установления предельного срока использования исключенных учебников» (Зарегистрировано в Минюсте России 01.11.2022 N 70799). URL: https://co3tular71.gosuslugi.ru/netcat_files/30/69/prikaz_minprosveshch_rossii_ot_21.09.2022_n_858_fpu.pdf. (дата обращения: 13.03.2024).
3. Лайфхакер [Электронный ресурс] // 21 лучшая программа для 3D-моделирования [сайт]. [2021]. URL: https://lifehacker.ru/programmy-dlya-3d-modelirovaniya/ (дата обращения: 18.03.2024).
4. Хабр [Электронный ресурс] // 3D в школе: кто, чему и как должен учить? [сайт]. [2016]. URL: https://habr.com/ru/articles/275495/ (дата обращения: 21.03.2024).
5. Московский Государственный Университет МГПУ [Электронный ресурс] // Реализация технологии 3D-печати в общеобразовательных школах в дополнительном образовании. Развитие и проблемы [сайт]. [2023]. URL: https://mgpu-media.ru/issues/issue-46/informatsionnye-tekhnologii/realizatsiya-tekhnologii-3d-pechati-v-obshcheobrazo-

vatelnykh-shkolakh-v-dopolnitelnom-obrazovanii-razvitie-i-problemy.html (дата обращения: 15.03.2024).

УДК 004.832.28

Использование искусственного интеллекта в современных системах информационной безопасности

Гаджиев Гаджибек Казбекович

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В статье рассматривается использование искусственного интеллекта (ИИ) в современных системах информационной безопасности. В условиях растущего объема цифровой информации и соответствующего увеличения уровня угроз безопасности данных актуальность применения ИИ для борьбы с этими угрозами становится неоспоримой. Статья выделяет основные преимущества ИИ в области информационной безопасности, включая автоматизацию процессов обнаружения угроз, способность к обучению на основе опыта, улучшение скорости реакции и сокращение риска человеческого фактора. Также анализируются вызовы и ограничения, с которыми сталкиваются системы на основе ИИ, такие как необходимость в обучении моделей на больших объемах данных, угрозы безопасности данных, требования к инфраструктуре и проблемы интерпретируемости принимаемых решений.*

***Abstract**: The article deals with the use of artificial intelligence (AI) in modern information security systems. With the growing volume of digital information and the corresponding increase in the level of data security threats, the relevance of AI application to combat these threats becomes undeniable. The article highlights the main benefits of AI in the field of information security, including the automation of threat detection processes, the ability to learn from experience, improved responsiveness, and reduced human error risk. It also analyzes the challenges and limitations faced by AI-based systems, such as the need to train models on large amounts of data, data security threats, infrastructure requirements, and decision interpretability issues.*

***Ключевые слова**: информационная безопасность, искусственный интеллект, системы безопасности, угрозы безопасности данных, автоматизация процессов, обнаружение угроз, обучение на основе опыта, скорость реакции.*

***Keywords**: information security, artificial intelligence, security systems, data security threats, process automation, threat detection, learning from experience, responsiveness.*

Введение

Информационная безопасность становится все более важной в современном мире, где данные играют ключевую роль во всех аспектах деятельности. С ростом объема цифровой информации увеличивается и уровень угроз, связанных с ее безопасностью. Для борьбы с этими угрозами становится необходимым развитие и применение новых технологий, в том числе искусственного интеллекта (ИИ). В данной статье рассматривается использование ИИ в современных системах информационной безопасности, его преимущества и вызовы.

Преимущества использования искусственного интеллекта в системах информационной безопасности

Автоматизация процессов обнаружения угроз

Одним из главных преимуществ использования ИИ в информационной безопасности является возможность автоматизировать процессы обнаружения и анализа угроз. Системы на основе ИИ могут анализировать большие объемы данных и выявлять аномалии, указывающие на потенциальные угрозы безопасности.

Способность к обучению на основе опыта

Искусственный интеллект обладает способностью к обучению на основе накопленного опыта. Это позволяет системам информационной безопасности адаптироваться к новым угрозам и сценариям атак, улучшая свою эффективность с течением времени.

Улучшение скорости реакции

Системы на основе ИИ способны обрабатывать информацию и принимать решения в режиме реального времени, что позволяет оперативно реагировать на угрозы безопасности и предотвращать потенциальные атаки.

Сокращение риска человеческого фактора

Автоматизация процессов безопасности с использованием ИИ позволяет сократить роль человеческого фактора, который часто является слабым звеном в системах безопасности из-за возможности допущения ошибок или игнорирования предупреждений.

Вызовы и ограничения

Недостаточная обученность моделей

Одним из вызовов при использовании ИИ в системах информационной безопасности является необходимость обучения моделей на больших объемах данных. Недостаточное количество данных или их некачественность может привести к недостаточной эффективности системы.

Угрозы безопасности данных

Системы, основанные на ИИ, могут стать объектом атак со стороны злоумышленников, которые попытаются вмешаться в их работу или подать ложную информацию для искажения результатов анализа.

Необходимость внедрения инфраструктуры

Внедрение систем на основе ИИ требует значительных инвестиций в инфраструктуру и персонал, способный работать с этими системами.

Проблема интерпретируемости

Еще одним вызовом является сложность интерпретации решений, принимаемых системами на основе искусственного интеллекта. Некоторые модели могут давать точные результаты, но их принципы работы могут быть непонятными для людей, что затрудняет проверку и анализ действий системы.

Этические вопросы

Использование искусственного интеллекта в системах информационной безопасности также вызывает вопросы этики и конфиденциальности данных. Например, возникают опасения относительно возможного нарушения приватности при сборе и анализе данных пользователей.

Примеры применения искусственного интеллекта в сфере информационной безопасности

Обнаружение аномалий в сетевом трафике

Системы на основе искусственного интеллекта могут анализировать сетевой трафик и выявлять аномалии, указывающие на возможные атаки или взломы.

Анализ угроз безопасности

Искусственный интеллект может использоваться для анализа данных и выявления потенциальных угроз безопасности, а также предсказания вероятности их возникновения.

Автоматизация реакции на инциденты безопасности

Системы на основе ИИ могут автоматически реагировать на обнаруженные угрозы безопасности, например, блокируя доступ к зараженным ресурсам или запуская процессы восстановления после атак.

Адаптивная защита

Искусственный интеллект позволяет создавать системы, способные адаптироваться к изменяющимся угрозам и сценариям атак, что повышает эффективность защиты информации.

Кроме того, стоит отметить, что использование искусственного интеллекта в системах информационной безопасности также предполагает значительное снижение времени реакции на угрозы. Традиционные методы обнаружения и реагирования на атаки могут требовать значительного времени для анализа данных и выявления угроз. Однако системы на основе искусственного интеллекта способны анализировать и обрабатывать информацию в реальном времени, что позволяет оперативно реагировать на инциденты безопасности и минимизировать ущерб.

Следует также отметить, что использование искусственного интеллекта в сфере информационной безопасности может снизить нагрузку на человеческие ресурсы. Автоматизация процессов обнаружения угроз, анализа данных и принятия мер по защите информации позволяет сократить необходимость в постоянном мониторинге и управлении системами безопасности со стороны человека.

Однако следует учитывать, что использование искусственного интеллекта также сопряжено с определенными рисками и ограничениями. Например, некорректная настройка или обучение моделей машинного обучения может привести к ложным срабатываниям и ошибочным действиям системы. Кроме того, возможность злоупотребления искусственным интеллектом для целей кибератак также является серьезным вызовом для безопасности информации.

Таким образом, несмотря на свои преимущества, использование искусственного интеллекта в современных системах информационной безопасности требует внимательного подхода к разработке, настройке и мониторингу системы, а также постоянного обновления и адаптации к изменяющимся угрозам и сценариям атак.

Заключение

Использование искусственного интеллекта в современных системах информационной безопасности представляет собой мощный инструмент в борьбе с угрозами безопасности. Несмотря на вызовы и ограничения, связанные с этой технологией, ее преимущества в виде автоматизации, скорости реакции и адаптивности делают ее неотъемлемой частью стра-

тегии обеспечения безопасности информации в современном цифровом мире. Дальнейшее развитие искусственного интеллекта в этой области может привести к созданию более эффективных и интеллектуальных систем безопасности, способных адаптироваться к постоянно меняющимся угрозам.

Список литературы

1. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020.— [С. 563–568].
2. Кирилова К. С. и др. Проблема обезвреживания руткитов уровня ядрав системах специального назначения //I-methods.— 2020. — Т. 12.— № 3.— [С. 2].
3. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2020.— № . 4.— [С. 72–76].
4. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных unix подобных операционных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018).— 2018.— [С. 570–573].
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015.— [63 с]. — EDN CMMEML.

УДК 004.056.5

Киберугрозы в банковской сфере: как защитить финансовые данные

Винокуров Иван Антонович

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В современном мире, где цифровые технологии проникают во все сферы жизни, банковская сфера не является исключением. Однако вместе с возможностями, которые предоставляет цифровизация, приходят и угрозы кибербезопасности, способные серьезно подорвать доверие к финансовым учреждениям. Защита финансовых данных становится приоритетом для банков, поскольку утечки или кражи таких данных могут привести к серьезным финансовым потерям и утрате репутации.*

***Abstract**: In today's world where digital technologies are penetrating every aspect of life, the banking industry is no exception. However, along with the opportunities presented by digitalization come cybersecurity threats that can seriously undermine trust in financial institutions. Protecting financial data is becoming a priority for banks, as leaks or theft of such data can lead to serious financial and reputational losses.*

***Ключевые слова**: банковские услуги, киберугрозы, цифровые каналы, мобильные приложения, интернет-банкинг, фишинг, вредоносное программное обеспечение, DDoS-атаки, риск, компания, данные, услуга.*

***Keywords**: banking services, cyber threats, digital channels, mobile applications, Internet banking, phishing, malware, DDoS attacks.*

Финансовые институты в том виде, в котором мы их знаем, существуют уже несколько веков. Банковская практика претерпела значительные изменения, но основные принципы остались прежними. Банки всегда хранили большие объемы личной и финансовой информации о своих клиентах. Сегодня все эти данные легко доступны и требуют надежных мер кибербезопасности для их защиты.

Развитие финансовых технологий за последние несколько десятилетий привело к появлению множества инноваций и изменений, включая электронные переводы средств, кредитные/дебетовые карты, онлайн-банкинг

и мобильные платежи. Банкам пришлось не только модернизировать свои системы, чтобы приспособить их к этим изменениям, но и трансформировать свои процессы, чтобы обеспечить постоянную безопасность по мере внедрения новых технологий. Меры безопасности, направленные на защиту конфиденциальной информации и предотвращение атак киберпреступников, таких как фишинг и попытки распространения вредоносных программ, также важны сегодня.

Банковское законодательство постоянно меняется в соответствии с требованиями современныхб анковских систем. Банки несут юридическую ответственность за защиту данных клиентов и предохранение их от кибератак и несанкционированного доступа. В этой статье мы рассмотрим, как современные банки и компании, предоставляющие финансовые услуги, выполняют эту обязанность.

Несмотря на растущую зависимость мировой финансовой системы от цифровой инфраструктуры, до сих пор неясно, кто несет ответственность за защиту систем от кибератак. Отчасти это объясняется быстро меняющейся обстановкой. Поскольку инновации, конкуренция и пандемии еще больше ускоряют цифровую революцию, глобальная финансовая система станет еще более уязвимой, если не будут приняты активные меры. Хотя многие участники угроз преследуют цель получения прибыли, растет число атак чисто разрушительного и деструктивного характера. Более того, те, кто научился воровать, также узнали о сетях и операциях финансовой системы, что позволит им в будущем совершать (или продавать такие знания и возможности другим) более разрушительные и деструктивные атаки. Этот быстро меняющийся ландшафт рисков приводит к тому, что зрелые и хорошо регулируемые системы не успевают реагировать на него.

Повышение уровня защиты мировой финансовой системы — это в первую очередь организационная задача. Усилия по укреплению защиты и усилению регулирования важны, но недостаточны для того, чтобы опередить растущие риски. В отличие от многих отраслей, большинство представителей индустрии финансовых услуг не испытывают недостатка в ресурсах или возможностях для внедрения технических решений. Основная проблема заключается в коллективных действиях: как наилучшим образом организовать системную защиту с участием правительства, финансо-

вых органов и промышленности, а также как эффективно и рационально использовать эти ресурсы.

Нынешняя разрозненность заинтересованных сторон и инициатив отчасти объясняется уникальными аспектами и развивающейся природой киберрисков. Различные сообщества действуют изолированно и решают проблему в рамках своих мандатов.Финансовые регуляторы сосредоточены на устойчивости, дипломаты — на национальных кодексах поведения, агентства национальной безопасности — на сдерживании вредоносной активности, а руководители компаний — на рисках, характерных для конкретной компании, а не для отрасли.Поскольку границы между финансовыми и технологическими компаниями становятся все более размытыми, границы ответственности за безопасность также становятся все более размытыми.

Особенно ярко выражен разрыв между финансовым, национальным и дипломатическим сообществами. Финансовые организации сталкиваются с уникальными рисками, связанными с киберугрозами, однако их отношения с национальными службами безопасности, которые необходимы для эффективного противодействия этим угрозам, остаются напряженными.

Такой разрыв ответственности и сохраняющаяся неопределенность в отношении ролей и мандатов по защите глобальной финансовой системы подпитывают риски. Отчасти эта неопределенность обусловлена нынешним геополитическим климатом и высоким уровнем недоверия, которые препятствуют сотрудничеству между представителями международного сообщества. Сотрудничество в области кибербезопасности было затруднено, фрагментировано и часто ограничивалось самым узким кругом доверия, поскольку затрагивало чувствительные вопросы национальной безопасности. Международное сотрудничество с участием многих заинтересованных сторон — это не «приятное событие», а «необходимое событие».

Сфера банковских услуг становится все более уязвимой перед различными киберугрозами из-за роста числа цифровых каналов обслуживания клиентов, таких как мобильные приложения и интернет-банкинг. Киберпреступники используют разнообразные методы атак, чтобы получить несанкционированный доступ к финансовым данным и средствам клиентов. Среди наиболее распространенных угроз можно выделить фишинг,

вредоносное, программное обеспечение, DDoS-атаки, а также атаки на системы обработки платежей и точки продаж.

Как защитить финансовые данные:

1. Многоуровневая защита сети: реализация комплексной защиты сети, включающую брандмауэры, системы обнаружения вторжений и шифрование трафика.
2. Шифрование данных: шифрование всех финансовых данных в покое и в движении для предотвращения их перехвата и несанкционированного чтения.
3. Многофакторная аутентификация: внедрение многофакторной аутентификации для всех видов доступа к финансовым данным для обеспечения дополнительного уровня защиты.
4. Обучение персонала: проведение регулярных тренингов по кибербезопасности для сотрудников банка, чтобы они могли распознавать и предотвращать киберугрозы.
5. Регулярные аудиты безопасности: систематическое проведение аудита безопасности для выявления и устранения уязвимостей в инфраструктуре и приложениях.
6. Мониторинг и реагирование на угрозы: развертывание систем мониторинга безопасности, позволяющих выявлять необычную активность и своевременно реагировать на потенциальные угрозы.
7. Соблюдение регулирований: соблюдение всех требований и стандартов безопасности, установленных регулирующими органами.
8. Резервное копирование и восстановление данных: разработка стратегии резервного копирования данных и плана восстановления после инцидента для минимизации потерь в случае успешной атаки.

Заключение

Банки должны придавать кибербезопасности высший приоритет, уделяя особое внимание защите финансовых данных своих клиентов. Применение современных методов защиты и строгий контроль за кибербезопасностью помогут снизить риск киберугроз и сохранить доверие клиентов к финансовым учреждениям.

Финансовые услуги охватывают широкий спектр предприятий, управляющих денежными средствами, включая кредитные союзы, банки, компании по выпуску кредитных карт, страховые компании, компании потребительского кредитования, фондовые брокеры, инвестиционные фонды и некоторые государственные предприятия. Эти учреждения играют важнейшую роль в мировой экономике, способствуя осуществлению сделок, предоставляя кредиты и позволяя физическим и юридическим лицам инвестировать и приумножать богатство.

С развитием технологий появились цифровые банковские услуги, онлайновые инвестиционные платформы, электронные платежные системы и другие финансовые услуги, предоставляемые через Интернет. Эта цифровая трансформация сделала финансовые услуги более доступными и удобными. Кибербезопасность в сфере финансовых услуг играет важную роль в предотвращении потерь. Благодаря сетевой безопасности, системам обнаружения вторжений, защите от вредоносных программ и другим мерам кибербезопасности финансовые учреждения могут предотвратить кибератаки и смягчить их последствия. Защищая финансовые операции и данные клиентов, кибербезопасность в сфере финансовых услуг помогает поддерживать доверие потребителей. Она дает клиентам уверенность в том, что их данные и деньги в безопасности, что способствует доверию к услугам финансового учреждения.

Список литературы

1. Ариба В. Управление данными в финансовых услугах: как обеспечить целостность данных для управления рисками и отчетности // Astera[Электронный ресурс]. — URL: https://www.astera.com/ru/type/blog/data-governance-in-financial-services.
2. Информационная безопасность в банках [Электронный ресурс]. — https://www.tadviser.ru/index.php/Статья: Информационная_безопасность_в_банках.
3. Дистанционное банковское обслуживание и цифровая трансформация бизнес-процессов // Компания BSS [Электронный ресурс]. — https://bssys.com/blog/distantsionnoe-bankovskoe-obsluzhivanie-i-tsifrovaya-transformatsiya-biznes-protsessov/.

УДК 004.056

Меры защиты информации в автоматизированных системах управления ODT

Губарев Владимир Дмитриевич

студент факультета Инфокоммуникационных систем связи
Санкт-Петербургского государственного университета телекоммуникаций
имени профессора М. А. Бонч-Бруевича

***Аннотация**: Данная статья освещает вопросы безопасности информации в автоматизированных системах управления, использующих формат ODT (Open Document Text). Подробно рассмотрены ключевые меры защиты, включая шифрование данных, аутентификацию и управление доступом, регулярные обновления, использование антивирусной защиты, резервное копирование данных, а также обучение персонала по вопросам безопасности. Статья подчеркивает важность этих мер для обеспечения надежной защиты конфиденциальности и целостности информации в ODT-системах, призывая к системному подходу к безопасности в контексте автоматизированных систем управления.*

***Abstract**: This article highlights the issues of information security in automated management systems using the ODT (Open Document Text) format. Key security measures including data encryption, authentication and access control, regular updates, use of anti-virus protection, data backup, and security training are discussed in detail. The article emphasizes the importance of these measures to ensure that the confidentiality and integrity of information in ODT systems is well protected, calling for a systematic approach to security in the context of automated control systems.*

***Ключевые слова**: ODT, Автоматизированные системы управления, Безопасность информации, Шифрование данных, Аутентификация, Управление доступом, Регулярные обновления, Антивирусная защита, Резервное копирование данных, Обучение персонала по безопасности, Конфиденциальность, Целостность данных, Информационная безопасность.*

***Keywords**: ODT, Automated management systems, Information security, Data encryption, Authentication, Access control, Regular updates, Anti-virus protection, Data backup, Security personnel training, Confidentiality, Data integrity, Information security.*

Файлы ODT (OpenDocument Text Document) — это текстовые документы в формате OpenDocument.

Стандарт Open Document Format (ODF) — это формат файлов с открытым исходным кодом для сохранения и обмена текстом, электронными таблицами, диаграммами, графиками и презентациями, сжатый в zip-архив и основанный на расширяемом языке разметки (XML).

Данный формат поддерживается как международный стандарт и имеет открытый исходный код, что с одной стороны позволяет свободно и бесплатно использовать его любому разработчику ПО, обеспечивает совместимость для различных программ, придерживающихся этого формата. С другой же стороны может хранить в себе массу уязвимостей, которые может реализовать потенциальный нарушитель.

Текстовые документы этого формата могут создаваться с помощью таких программ, как Open Office или LibreOffice, и будут отличаться от других текстовых файлов расширением.odt. Эти документы широко используются в различных офисных программах.

С развитием технологий и внедрением автоматизированных систем управления (ODT) в различные отрасли, вопрос безопасности и защиты информации становится критическим. Автоматизированные системы, использующие формат ODT (Open Document Text), требуют специальных мер по защите от угроз виртуального мира. В данной статье рассмотрим ключевые меры защиты информации в ODT-системах.

1. Шифрование данных

Одним из основных методов защиты информации в ODT-системах является шифрование данных. Шифрование позволяет перевести конфиденциальную информацию в нечитаемый вид для посторонних лиц, не обладающих ключом. Для ODT-файлов рекомендуется использовать сильные алгоритмы шифрования, такие как AES (Advanced Encryption Standard), обеспечивающие высокий уровень безопасности.

2. Аутентификация и управление доступом

Важным аспектом безопасности ODT-систем является правильная аутентификация пользователей и строгий контроль доступа. Использова-

ние сильных паролей, двухфакторной аутентификации и регулирование прав доступа к файлам помогут предотвратить несанкционированный доступ к информации.

3. Регулярные обновления и патчи

Разработчики ODT-систем постоянно улучшают свои продукты, выявляя и устраняя уязвимости. Регулярные обновления и патчи помогают поддерживать систему в актуальном и безопасном состоянии. Отсутствие обновлений может стать причиной уязвимостей, которые могут быть использованы злоумышленниками.

4. Антивирусная защита

Использование антивирусного программного обеспечения является неотъемлемой частью безопасности ODT-систем. Оно помогает выявлять и блокировать вредоносные программы, которые могут угрожать сохранности информации в системе.

5. Резервное копирование данных

Регулярное создание резервных копий данных позволяет восстановить информацию в случае ее утраты или повреждения. Этот шаг не только обеспечивает защиту от потери данных, но и является важным элементом восстановления после атаки или сбоя системы.

6. Обучение персонала по вопросам безопасности

Создание безопасной среды в ODT-системах также зависит от обучения персонала. Сотрудники должны быть осведомлены о базовых принципах безопасности, уметь распознавать подозрительную активность и следовать правилам безопасности при работе с системой.

В заключение следует сказать, что меры защиты информации в автоматизированных системах управления, использующих формат ODT, играют

ключевую роль в предотвращении угроз и обеспечении стабильной работы системы. Шифрование данных, аутентификация пользователей, регулярные обновления и другие описанные меры совместно формируют надежный барьер для защиты конфиденциальности и целостности информации в ODT-системах.

Список литературы

1. Афанасьев, Алексей Алексеевич Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. Гриф УМО МО РФ: моногр. / Афанасьев Алексей Алексеевич. — М.: Горячая линия — Телеком, 2012.— 798 с.
2. Еременко, А. В. Двухфакторная аутентификация пользователей компьютерных систем на удаленном сервере по клавиатурному почерку / А. В. Еременко. — М.: Синергия, 2015.— 978 с.
3. Зубов, А. Н. Математика кодов аутентификации / А. Н. Зубов. — М.: Гелиос АРВ, 2007.— 568 с.
4. Зубов, А. Ю. Коды аутентификации / А. Ю. Зубов. — М.: Гелиос АРВ, 2017.— 965 с.
5. Рассел, Джесси Аутентификация / Джесси Рассел. — М.: VSD, 2012.— 441 с.
6. Рассел, Джесси Единая система идентификации и аутентификации / Джесси Рассел. — М.: VSD, 2013.— 184 с.
7. Стюгин, М. А. Метод аутентификации с использованием динамических ключей / М. А. Стюгин. — М.: Синергия, 2016.— 801 с.
8. Кушнир Д. В., Шемякин С. Н. Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: естественные и технические науки Учредители: Санкт-Петербургский государственный университет промышленных технологий и дизайна.— № . 4. — С. 63–6.
9. Алехин Р. В. и др. Исследование критической уязвимости сервиса аутентификации и последствий для медицинских учреждений, относящихся к субъектам критической информационной инфраструктуры // Офтальмохирургия.— 2022.— № . 4s. — С. 115–122.

10. Голубов Н. А., Косов Н. А. Внутренние угрозы: Разнообразие и профилактика инсайдеров в организациях.— 2023.
11. Зимин А. Е., Косов Н. А. Обеспечение информационной безопасности в процессе создания и использования программ для ЭВМ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017).— 2017. — С. 343–348.
12. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 563–568.

УДК 004.056.5

Анализ средств защиты информации в гипервизорах на базе KVM

Пепп Михаил Андреевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бронч-Бруевича

***Аннотация**: В статье описываются требования к обеспечению безопасности средств виртуализации на базе гипервизора KVM (Kernel-based Virtual Machine). Примеры функциональной поддержки выделенных требований рассматриваются на основании трех программных продуктов: SELinux, AppArmor и Аккорд-KVM. Автор приводит некоторые решения, позволяющие продуктам соответствовать мерам защиты виртуальной инфраструктуры, их достоинства и возможные уязвимости.*

***Abstract**: The article describes the security requirements for KVM (Kernel-based Virtual Machine) hypervisor-based virtualization tools. Examples of functional support of the highlighted requirements are considered on the basis of three software products: SELinux, AppArmor and Accord-KVM. The author provides some solutions that allow the products to meet the virtual infrastructure protection measures, their merits and possible vulnerabilities.*

***Ключевые слова**: виртуализация, информационная инфраструктура, KVM, Linux, кибератака, информационная безопасность, программное обеспечение.*

***Keywords**: virtualization, information infrastructure, KVM, Linux, cyberattack, information security, software.*

Виртуализация — это использование программного обеспечения для создания абстрактного уровня над физическим компьютерным оборудованием. Это позволяет разделить ресурсы одного компьютера, такие как процессоры, память и хранилище, на несколько виртуальных машин. Каждая виртуальная машина функционирует под управлением собственной операционной системы и ведет себя как отдельный компьютер, хотя фактически использует лишь часть ресурсов базового компьютерного оборудования. Использование виртуализации значительно сокращает время обработки и доступа к постоянно растущему объему информации без необходимости значительных изменений в информационной инфраструктуре компании. Это также позволяет штату IT-специалистов работать более эффективно и дает возможность сотрудникам отдела администрирования более результативно использовать мощности информационной инфраструктуры компании.

Гипервизор действует как интерфейс между виртуализированной операционной системой гостя и физическим оборудованием. Гипервизоры первого типа работают непосредственно на аппаратном обеспечении системы. Гипервизоры второго типа функционируют под управлением операционной системы устройства, предоставляя ей в дополнение виртуализационные возможности, такие как поддержка устройств ввода-вывода и управление памятью. [1].

Система с открытым исходным кодом Kernel-based Virtual Machine (KVM) принадлежит к категории «аппаратных гипервизоров» (первого типа). Она работает в среде Linux на платформе x86, которая поддерживает аппаратную виртуализацию на базе Intel VT либо AMD SVM (Secure VM) [2]. На сегодняшний день многие компании придерживаются тренда на импортозамещение, в некоторых отраслях это является острой необходимостью. Особенно полезными сейчас являются информационные продукты с открытым исходным кодом, яркими представителями которых являются операционные системы семейства Linux. Одним из популярных выборов для виртуализации инфраструктуры компании, построенных на ОС Linux, является гипервизор KVM (Kernel-based Virtual Machine). Он позволяет создавать виртуальные машины с поддержкой как операционных систем Windows, так и Linux, а также эффективно распределять ресур-

сы между ними, что обеспечивает возможность одновременного запуска нескольких виртуальных машин.

KVM — относительно новая разработка, но глубина и простота его реализации, а также постоянная поддержка со стороны разработчиков на Linux делают его достойным серьезного рассмотрения. Добавляя возможности виртуализации в стандартное ядро операционной системы, виртуализированная среда может воспользоваться всеми преимуществами текущей работы над ядром, ведь согласно этой модели, каждая виртуальная машина — это обычный процесс Linux со стандартным планировщиком.

Поскольку виртуальная машина KVM разработана на основе Linux, она следует стандартам модели безопасности операционной системы. Однако для обеспечения безопасности информации, использующейся мощностями виртуальной машины, и контроля целостности ее конфигурации необходимы дополнительные меры. Согласно приказам № 17, 21 и 31 ФСТЭК России набора функций средств виртуализации для настройки виртуальной инфраструктуры с учетом требований безопасности методического документа ФСТЭК России от 11.02.2014 недостаточно, поэтому для их защиты от несанкционированных изменений необходимо использовать дополнительные (внешние) средства защиты информации (СЗИ) [3].

Базовой операционной системой (ОС) для развертывания KVM является Debian. Данная ОС поддерживает две системы принудительного контроля доступа — Security-Enhanced Linux (SELinux) и AppArmor. В дополнение к ним в статье будет рассмотрено специальное программное обеспечение (СПО) «Аккорд-KVM».

Требования к рассматриваемым программным средствам указаны в упомянутых ранее приказах ФСТЭК России, поэтому в статье к анализу будут представлены характеристики, отвечающие соответствующим требованиям.

Для начала рассмотрим базовый набор мер, включающий следующие аспекты: регистрация событий безопасности, контроль защиты персональных данных, обеспечение целостности системы, защита виртуализированной среды, сетей и передачи данных, а также идентификация и аутентификация пользователей и ресурсов с управлением их взаимодействия. Все три системы безопасности способны охватить данные требования с помощью своих функциональных возможностей.

Примером является политика безопасности, предустановленная в RedHat, основном разработчике SELinux, которая обеспечивает защиту хостовой операционной системы от компрометации виртуальной машины. По умолчанию все запускаемые виртуальные машины получают домен qemu_t, а образы дисков виртуальных машин имеют тип virt_image_t. Все чаще производитель запрещает загрузку виртуальных машин с образами, хранящимися не в /var/lib/libvirt/images. Это означает, что в случае взлома виртуальной машины доступ к директориям типа /etc, /usr, / на хостовой ОС становится невозможным, если на них не установлен домен qemu_t, что является нарушением принципа наименьших привилегий [4].

Существует дополнительная модель безопасности — проект sVirt, который позволяет обеспечить защиту гостевых операционных систем друг от друга. Если система была скомпилирована с поддержкой sVirt, то она будет всегда включена, когда включен SELinux.

У СПО «Аккорд-KVM» также часть базовых требований выполняется средствами интеграции со сторонними надстройками «Аккорд-Х» и «Аккорд-Х К». Например, обеспечение контроля и управления ролями субъектов и объектов доступа, а также поддержание безопасности внутренних данных самой СПО полностью функционирует за счет этих надсистем.

Базовые настройки AppArmor позволяют защитить хостовую ОС от скомпрометированной гостевой ОС. Расширение sVirt позволяет защитить гостевые ОС друг от друга. Однако существует две серьезные проблемы, которые пока не решены. Первой уязвимостью является возможность выхода системы из-под контроля, при использовании жесткой символической ссылки, т.к. контроль осуществляется с использованием в профиле полного пути до файла, а не его функционала или возможностей. Причиной второй проблемы также являются пути к файлам. Общеизвестно, что злоумышленники очень часто используют папку с временными файлами для начала атаки, а также генерируют случайные имена для своего вредоносного программного обеспечения. Таким образом, если программе нужен доступ в каталог /tmp для создания временного файла со случайным именем, то администратору придется расширить права программы, что может привести к увеличению площади возможной атаки [5].

При детальном рассмотрении дополнительных мер безопасности можно увидеть, что они являются расширением некоторых базовых. В основном они направлены на обеспечение возможности просмотра и анализа функционирования самой системы безопасности, мониторинга выполняемых политик и обеспечение целостности обрабатываемых системой данных.

Все три системы осуществляют достаточно подробное журналирование событий, что позволяет эффективно контролировать полный цикл обеспечения безопасности и избежать смешения информации различного уровня доступа.

В разделе с примерами для AppArmor были приведены две проблемы, влияющие на ее устойчивость к кибератакам. Однако, разумеется, у других программных продуктов также существуют слабые места. Злоумышленники постоянно развивают свои навыки и методы поиска путей обхода любых запретов ограничений и ловушек. Даже самые банальные из них до сих пор остаются опасными. Фишинговые атаки, недостаток качественной документации к функциям и ошибкам программного обеспечения, компрометация административных прав, сложности в установке правильной конфигурации систем безопасности. Всё это относится к давно известным и проверенным средствам подрыва купола устойчивости любой системы, и все же полностью защититься от них крайне сложная задача. Поэтому разработчики SELinux, AppArmor и Аккорд-KVM постоянно работают над усовершенствованием своих систем, обучением эффективной работе с ними и поиском новых решений для догоняющих это развитие угроз.

Список литературы

1. Дэви Я.Н., Сиван А., Дэви С.Д., Прийя Н. Безопасность при живой миграции виртуальных машин для KVM // Сборник статей Международной конференции по автоматизации процессов, управлению и вычислениям. 2011
2. Пестов, И. Е. Анализ архитектуры виртуальной машины / И. Е. Пестов, З. А. Федорова // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022): XI Международная научно-

техническая и научно-методическая конференция, Санкт-Петербург, 15–16 февраля 2022 года. Том 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2022. — С. 747–751. — EDN TNLHNK.

3. Цветков, А. Ю. Исследование существующих механизмов защиты операционных систем семейства linux / А. Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля — 01 2018 года / Под редакцией С. В. Бачевского. Том 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2018. — С. 657–662. — EDN XSUGRV.
4. Мониторинг информации инстансов облачной инфраструктуры / И. Е. Пестов, И. А. Смуров, П. О. Федоров, Е. С. Федорова // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2022): Сборник лучших докладов Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей, Санкт-Петербург, 06–08 декабря 2022 года / Сост. Н. Н. Иванов. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2023. — С. 216–220. — EDN PIDCEX.
5. Зубарев И. В., Радин П. К. Основные угрозы безопасности информации в виртуальных средах и облачных платформах // Вопросы кибербезопасности. 2014. № 2 (3). С. 40–45.

УДК 004

Тестирование на проникновения с использованием крупномасштабных языковых моделей

Трофимов Евгений Александрович

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной научной статье рассматривается возможность использования крупномасштабных языковых моделей (LLM) в области тестирования на проникновение. Основное внимание уделено анализу того, как LLM могут способствовать автоматизации создания и выполнения тестов на проникновение, обеспечивая тем самым повышение эффективности и скорости выявления уязвимостей. В статье подробно излагаются методики обучения моделей, а также приводятся результаты экспериментальной проверки их способности предсказывать потенциальные точки проникновения в систему. Кроме того, обсуждаются этические аспекты применения LLM в кибербезопасности, включая риски злоупотребления такими технологиями.*

***Abstract**: This research paper examines the feasibility of using large-scale language models (LLMs) in the field of penetration testing. The focus is on analyzing how LLMs can help automate the creation and execution of penetration tests, thereby providing increased efficiency and speed of vulnerability detection. The paper details the methodologies used to train the models and presents results of experimental validation of their ability to predict potential penetration points into a system. In addition, the ethical aspects of LLMs applications in cybersecurity are discussed, including the risks of misuse of such techniques.*

***Ключевые слова**: Крупномасштабные языковые модели (LLM), тестирование на проникновение, автоматизация кибербезопасности, обнаружение уязвимостей, интеграция LLM в кибербезопасность, процессы кибербезопасности, риски использования ИИ.*

***Keywords**: Large Language Models (LLM), penetration testing, cybersecurity automation, vulnerability detection, integration of LLMs into cybersecurity, cybersecurity processes, risks of AI usage.*

Современный мир информационных технологий характеризуется стремительным ростом сложности и объема данных, что, в свою очередь, повышает риски в области кибербезопасности. Противостоять угрозам

безопасности информационных систем становится всё более трудоемким и сложным заданием. В этом контексте, автоматизация процессов кибербезопасности, особенно тестирования на проникновение, представляется крайне перспективной областью для применения инновационных технологий, таких как крупномасштабные языковые модели (LLM).

Тестирование на проникновение является критически важным элементом защиты информационных систем, направленным на выявление уязвимостей, которые могут быть использованы злоумышленниками для нанесения ущерба. Традиционно данный процесс требует значительного количества ручной работы специалистами в области кибербезопасности, что делает его не только затратным, но и подверженным ошибкам из-за человеческого фактора.

Применение LLM в тестировании на проникновение открывает новые возможности для повышения эффективности и точности этих процедур. LLM могут анализировать большие объемы кода и данных, предсказывая потенциальные уязвимости и автоматизируя создание тестовых сценариев. Кроме того, эти модели могут помочь в обучении и подготовке специалистов по кибербезопасности, предоставляя им детализированные аналитические отчеты и рекомендации.

Использование LLM для автоматизации и улучшения процессов в различных областях

Крупномасштабные языковые модели (LLM), такие как GPT и BERT, представляют собой мощный инструмент для автоматизации и улучшения процессов в различных областях, включая кибербезопасность. В контексте тестирования на проникновение LLM могут значительно повысить эффективность и скорость выявления уязвимостей благодаря следующим способностям, представленным в Таблице 1.

Применение LLM в тестировании на проникновение обещает значительные преимущества, но требует тщательного учета этических и технических аспектов, включая обеспечение конфиденциальности, защиту данных и предотвращение неправомерного использования таких технологий.

Таблица 1. **Характерные черты LLM для автоматизации и улучшения процессов в различных областях**

Способность LLM	Описание
Автоматическое создание тестовых сценариев	LLM могут анализировать код, системные конфигурации и сетевые протоколы для идентификации уязвимостей и генерации тестовых сценариев.
Улучшение покрытия тестирования	Понимание больших объемов информации позволяет LLM расширять покрытие тестирования и включать редко используемые аспекты и векторы атак.
Повышение скорости тестирования	Благодаря быстрому анализу данных и генерации отчетов, LLM сокращают время, необходимое для тестирования на проникновение.
Обучение и поддержка аналитиков	LLM предоставляют обучающие материалы и рекомендации для улучшения стратегий тестирования, помогая обучать специалистов по безопасности.
Адаптация к изменяющимся угрозам	LLM могут обновлять тестовые сценарии и методы обнаружения в соответствии с последними тенденциями и техниками атак.

Методики обучения моделей и результаты экспериментальной проверки их способности предсказывать потенциальные точки проникновения в систему.

Методики обучения крупномасштабных языковых моделей (LLM) для тестирования на проникновение включают несколько ключевых подходов, которые обеспечивают эффективность их применения в области кибербезопасности. Эти подходы включают обучение с учителем, обучение без учителя, обучение с подкреплением и трансферное обучение.

В обучении с учителем модели LLM тренируются на размеченных данных, которые включают примеры уязвимостей в коде, описания безопасностных инцидентов и атак. Эти данные могут содержать как код, так и естественный язык, описывающий уязвимости и контексты, в которых они были обнаружены. Модель учится идентифицировать шаблоны и индикаторы, которые обычно связаны с уязвимостями, что позволяет ей впоследствии предсказывать потенциальные точки проникновения в новом или неизвестном коде.

В случаях, когда размеченные данные ограничены или отсутствуют, LLM могут использовать обучение без учителя для изучения структур и закономерностей в больших наборах данных, таких как логи серверов или большие кодовые базы. Методы кластеризации и аномального обнаружения позволяют модели выявлять необычные или отклоняющиеся паттерны, которые могут указывать на потенциальные уязвимости.

Этот подход позволяет модели оптимизировать свои стратегии поиска уязвимостей через систему вознаграждений и штрафов. Например, модель может получать положительное вознаграждение за успешное обнаружение уязвимости и отрицательное — за пропуск уязвимости или ложное срабатывание. Это стимулирует модель к более точному и целенаправленному поиску потенциальных угроз.

Трансферное обучение включает предварительное обучение модели на одном большом наборе данных, а затем дополнительное обучение или «тонкая настройка» на специфическом, часто более мелком и фокусированном наборе данных. Это позволяет модели адаптироваться к конкретной доменной специфике или задаче, такой как поиск уязвимостей в определенных типах приложений или систем.

В контексте использования языковых моделей на основе трансформеров (LLM) для обнаружения точек проникновения в системы безопасности, результаты экспериментальной проверки показывают, что такие модели могут достигать высокой эффективности при правильной настройке и обучении. Однако, есть ряд нюансов, влияющих на итоговые результаты.

Эксперименты выявили, что модели, обученные на детально аннотированных и разнообразных данных, лучше всего справляются с задачей определения потенциальных угроз. Точность таких моделей часто зависит от качества и объема тренировочных данных. При использовании обширных наборов данных, включающих различные типы атак, модели показали способность эффективно распознавать как известные, так и новые угрозы.

С другой стороны, эксперименты также выявили сложности, связанные с применением обучения без учителя. Хотя такие подходы предлагают возможность обнаружения неизвестных атак, они могут страдать от высокого уровня ложноположительных срабатываний, что создает дополнительные трудности при мониторинге систем на предмет безопасности.

Дополнительно, результаты показали, что модели на основе подкрепляющего обучения могут адаптироваться к меняющимся атакам и стратегиям проникновения, что делает их особенно ценными в динамических условиях современной кибербезопасности. Однако, такие модели требуют значительных вычислительных ресурсов и времени для обучения, что может быть барьером для их широкого применения.

Этические аспекты применения LLM в кибербезопасности

Применение языковых моделей на основе трансформеров (LLM) в кибербезопасности открывает перед сектором новые возможности, однако также сопряжено с серьезными этическими вызовами и рисками. Одним из основных этических вопросов является возможность злоупотребления этими технологиями. Как и любой мощный инструмент, LLM могут быть использованы как для укрепления безопасности, так и для её подрыва. Модели, способные анализировать и предсказывать уязвимости систем, могут служить не только защите, но и направлять атакующих к слабым точкам системы.

Другой важный аспект — вопрос конфиденциальности данных. При работе с LLM, особенно при обучении на реальных данных, важно удостовериться, что используемая информация не раскрывает чувствительные данные, что может привести к нарушениям приватности и доверия. Это требует разработки строгих протоколов в отношении того, какие данные могут быть использованы для обучения моделей, и как эти данные защищаются.

Применение LLM в кибербезопасности также поднимает вопросы ответственности. В случае, если система на основе LLM допускает ошибку, что приводит к ущербу или нарушению безопасности, определение степени ответственности может быть затруднено. Это касается и вопросов о том, кто несет ответственность за действия системы: разработчики, пользователи или же сама система. Необходимо подходить к применению LLM в кибербезопасности с осторожностью, обеспечивая соответствие высоким этическим стандартам, чтобы максимизировать пользу от их использования и минимизировать риски. Важно создать соответствующий регулятивный и нормативный фреймворк, который будет регулировать использование таких технологий, защищая права и конфиденциальность всех сторон.

В завершение, интеграция LLM в области кибербезопасности открывает перспективные направления для укрепления защиты информационных систем. Несмотря на значительные преимущества, которые предлагают эти технологии, важно стремиться к их этичному и ответственному применению. Продолжение работы над усовершенствованием методов обучения, повышением точности моделей и разработкой международных стандартов будет способствовать оптимальному использованию LLM для обеспечения кибербезопасности при одновременном снижении потенциальных рисков.

Список литературы

1. Нейронные сети в кибербезопасности: угрозы и методы защиты Новосельцев А.А., Сафронов А.Е. В сборнике: Международный форум KAZAN DIGITAL WEEK — 2023. Сборник материалов. Сост. Р. Ш. Ахмадиева, Р. Н. Минниханов. Под общей редакцией Р. Н. Минниханова. Казань, 2023. С. 477–482.
2. Системы llm-агентов для решения задач ретроспективного анализа Смольников А.Б., Черномуров С.А., Евстратова О.Д., Заботкина Е. М. Наукосфера. 2024. № 2–2. С. 215–219.
3. Применение машинного обучения с подкреплением в задаче тестирования на проникновение Мясников А. В. Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2020. № 11. С. 104–107.
4. Нейросети в цифровых системах связи Сгибнев А.К. В сборнике: Трансформация науки и образования в современном обществе: теория и практика междисциплинарных исследований. Материалы I Всероссийской научно-практической конференции. Ростов-на-Дону, 2024. С. 111–113.
5. Цифровые технологии: надежды и риски бит. Бизнес & Информационные технологии. 2024. № 1 (134). С. 8–25.

УДК 004

Анализ методов машинного обучения для обнаружения фишинговых атак

Горбунов Святослав Леонидович

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной научной статье рассматриваются различные методы машинного обучения, применяемые для обнаружения фишинговых атак. Статья начинается с обзора основных типов фишинговых атак и их характеристик, что помогает определить ключевые параметры для анализа эффективности машинных алгоритмов. Затем представлены наиболее популярные подходы к машинному обучению, включая обучение с учителем и без учителя, а также их способность адаптироваться к постоянно изменяющимся методам атак. Подвергаются сравнительному анализу модели, таких как случайные леса, нейронные сети и методы опорных векторов, и оценке их точности в реальных условиях. В заключение обсуждаются возможные пути улучшения существующих моделей машинного обучения для более эффективного предотвращения фишинговых атак в будущем, включая интеграцию адаптивных и динамических обучающих систем.*

***Abstract**: This research paper discusses various machine learning techniques used to detect phishing attacks. The paper begins with an overview of the main types of phishing attacks and their characteristics, which helps to identify the key parameters for analyzing the effectiveness of machine learning algorithms. Then, the most popular machine learning approaches, including learning with and without a teacher, and their ability to adapt to ever-changing attack methods are presented. Models such as random forests, neural networks and support vector methods are subjected to comparative analysis and their accuracy under real-world conditions is evaluated. Finally, possible ways to improve existing machine learning models to better prevent phishing attacks in the future, including the integration of adaptive and dynamic learning systems, are discussed.*

***Ключевые слова**: Фишинг, машинное обучение, обнаружение атак, кибербезопасность, нейронные сети, случайные леса, метод опорных векторов, анализ данных, информационная безопасность, адаптивные системы обучения.*

***Keywords**: phishing, machine learning, attack detection, cybersecurity, neural networks, random forests, support vector method, data analysis, information security, adaptive learning systems.*

Введение

В современном мире, где цифровые технологии проникают в каждый аспект нашей жизни, фишинг остаётся одной из самых распространённых

и вредоносных угроз кибербезопасности. Фишинговые атаки, нацеленные на получение конфиденциальной информации пользователей через обман, причиняют значительный ущерб как отдельным лицам, так и организациям. Эффективное обнаружение и предотвращение фишинговых атак становится критически важным для защиты персональных данных и обеспечения безопасности информационных систем.

Машинное обучение представляет собой перспективный инструмент в этой борьбе, благодаря своей способности анализировать большие объемы данных и выявлять сложные паттерны, которые могут указывать на фишинг. В данной статье представлен анализ различных методов машинного обучения, включая нейронные сети, случайные леса и методы опорных векторов, с целью оценить их эффективность в задачах обнаружения фишинговых атак. Основное внимание уделяется сравнению их производительности, адаптивности к новым угрозам и возможностям интеграции в существующие системы кибербезопасности.

Типы фишинговых атак

Существуют различные типы фишинговых атак — от классического фишинга через электронную почту до более изобретательных способов, например, направленного фишинга и смишинга. Все они преследуют одну цель — кража ценных сведений о пользователе.

В случае направленного фишинга злоумышленники ориентируются на определенную аудиторию, например, системных администраторов конкретной компании. Они адаптируют свои атаки и методы маскировки под интересы и характеристики данной группы, чтобы увеличить вероятность успешного проникновения. В таких атаках могут быть использованы персонализированные электронные сообщения, веб-сайты или другие коммуникационные каналы, специально созданные для обмана и получения доверия от целевой аудитории. Целью злоумышленников при направленном фишинге может быть получение доступа к конфиденциальной информации компании, взлом системы или выполнение других вредоносных действий, специально направленных на эту группу пользователей.

В случае направленного фишинга, злоумышленники направляют свои атаки на четко определенную группу лиц, таких как системные администраторы внутри определенной организации. Этот вид атаки предполагает тщательную проработку и адаптацию стратегии к специфическим особенностям и характеристикам целевой аудитории. Используя тактику индивидуального подхода и персонализации, злоумышленники создают иллюзию достоверности своих запросов или сообщений, внушая жертвам доверие и увеличивая вероятность успешного выполнения атаки.

В контексте уэйлинг-атаки, часто целевыми объектами становятся высокопоставленные члены организации, директора или руководители. Этот вид кибератак основан на стратегии, направленной на манипуляцию социальными и профессиональными отношениями, а также восприятием роли внутри организации. Злоумышленники стремятся использовать обман и манипуляцию с целью получения доступа к конфиденциальной информации или финансовым ресурсам через целенаправленное воздействие на ключевые фигуры в организации.

Фишинговые атаки с использованием СМС называются смишингом. Человеку присылается сообщение, в котором содержится ссылка или номер, на который он должен перезвонить.

Вишинг, как форма социального инжиниринга, направлен на обман и манипуляцию пользователем с целью получения доступа к личной или корпоративной информации. Этот вид атаки включает в себя создание и распространение обманчивых коммуникаций, которые маскируются под легитимные запросы от организаций или учреждений. Злоумышленники, осуществляющие вишинг, стремятся убедить свою жертву предоставить конфиденциальные данные, такие как пароли, номера банковских карт или личные идентификационные сведения.

Сравнительный анализ методов машинного обучения

В рамках анализа методов машинного обучения для обнаружения фишинговых атак, принято различать три основные категории: обучение с учителем, обучение без учителя и глубокое обучение. Обучение с учителем включает алгоритмы, где модели обучаются на предварительно

размеченных данных, что позволяет им различать легитимные и мошеннические запросы. Примеры таких методов включают деревья решений, случайные леса и методы опорных векторов. Эти техники анализируют обучающие данные и формируют модель, способную классифицировать новые данные как фишинговые или нефишинговые на основе изученных признаков.

Обучение без учителя, в свою очередь, не требует предварительно размеченных данных и работает по принципу обнаружения аномалий в данных. Алгоритмы, такие как кластеризация и анализ главных компонентов, ищут необычные шаблоны, которые могут указывать на мошенничество, анализируя структурные особенности данных и выделяя аномалии, которые отклоняются от нормы.

Глубокое обучение, использующее сложные структуры вроде сверточных нейронных сетей и рекуррентных нейронных сетей, позволяет моделировать и обрабатывать большие объемы данных с высокой точностью. Эти методы автоматически выявляют и извлекают важные признаки из данных, что делает их особенно подходящими для обнаружения сложных и изощренных фишинговых атак, где требуется анализировать множество параметров и их взаимосвязи.

Заключение

Подводя итог, стоит отметить, что предотвращение фишинговых атак требует постоянного совершенствования моделей машинного обучения. Одним из потенциальных путей улучшения эффективности защиты является интеграция адаптивных и динамических обучающих систем. Эти системы способны быстро реагировать на новые виды атак и изменения тактики злоумышленников, обеспечивая более гибкую и эффективную защиту.

Интеграция адаптивных алгоритмов машинного обучения позволит моделям автоматически адаптироваться к изменяющейся угрозе, обучаясь на новых данных и выявляя новые образцы фишинга. Динамические обучающие системы, в свою очередь, будут способствовать непрерывному улучшению моделей на основе обратной связи и анализа результатов

защитных мер, что повысит их эффективность и точность в выявлении фишинговых атак.

Таким образом, интеграция адаптивных и динамических обучающих систем представляет собой перспективный путь к улучшению моделей машинного обучения в области кибербезопасности, что позволит эффективнее защищать пользователей и организации от фишинговых угроз в будущем.

Список литературы

1. Социальная инженерия: её методы и способы защиты Бударный Г.С., Дюсметова А.А., Казанцев А.А., Красов А.В. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т.. Санкт-Петербург, 2023. С. 200–204.
2. Анализ безопасности доменных систем Штеренберг С.И., Бударный Г.С., Чумаков И.В. В книге: Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022. С. 587–588.
3. Определение признаков фишинговых сообщений в электронной почте Борисов С.В., Севостьянов В.А., Цветков А.Ю. В сборнике: Студенческая весна — 2023. Материалы 77-й региональной научно-технической конференции студентов, аспирантов и молодых ученых. Санкт-Петербург, 2023. С. 88–92.
4. Разновидности нарушений безопасности и типовые атаки на операционную систему Бударный Г.С., Казанцев А.А., Красов А.В., Полянычева А.В. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). Сборник научных статей XI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией А. В. Шестакова, сост. В. С. Елагин, Е. А. Аникевич. Санкт-Петербург, 2022. С. 406–411.
5. Анализ существующих механизмов защиты и атак в операционных системах Цветков А.Ю. В сборнике: Актуальные проблемы инфотеле-

коммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т.. Санкт-Петербург, 2023. С. 927–931.

УДК 004.8

Разработка и оценка эффективности системы обнаружения аномальной активности в вендинговых автоматах на основе методов искусственного интеллекта

Горбунов Святослав Леонидович

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной научной статье рассматривается проблема обеспечения информационной безопасности вендинговых автоматов, особенно в контексте угрозы кибератак, направленных на хищение финансовой информации и средств. Статья представляет разработку инновационной системы обнаружения аномальной активности, основанной на технологиях машинного обучения и глубокого обучения. Обсуждается концепция и техническая реализация системы, включая алгоритмы анализа данных и модели идентификации подозрительного поведения. В работе подробно описываются методы сбора и обработки данных, обучения моделей и их валидации, что позволяет системе эффективно прогнозировать и предупреждать потенциальные угрозы. Результаты тестирования системы на реальных устройствах показывают высокую эффективность в распознавании и предотвращении взлома, подчеркивая важность внедрения таких технологий для повышения безопасности вендинговых автоматов. Статья завершается обсуждением влияния системы на улучшение устойчивости торговых автоматов к внешним угрозам и на защиту конфиденциальности пользовательских данных.*

***Abstract**: This research article addresses the problem of information security of vending machines, especially in the context of the threat of cyber attacks aimed at stealing financial information and funds. The paper presents the development of an innovative anomalous activity detection system based on machine learning and deep learning technologies. The concept and technical implementation of the system, including data analysis algorithms and suspicious behavior identification models, are discussed. The paper details the methods of data collection and processing, model training and validation, which enables the system to effectively predict and prevent potential threats. The results of testing the system on real devices show high effec-*

tiveness in recognizing and preventing tampering, highlighting the importance of implementing such technologies to improve the security of vending machines. The paper concludes with a discussion of the impact of the system on improving the resilience of vending machines to external threats and on protecting the privacy of user data

***Ключевые слова**: Вендинговые автоматы, обнаружение аномалий, искусственный интеллект, машинное обучение, кибербезопасность, анализ данных, нейронные сети, алгоритмы кластеризации.*

***Keywords**: vending machines, anomaly detection, artificial intelligence, machine learning, cybersecurity, data analytics, neural networks, clustering algorithms.*

Введение

В последние годы технологии вендинговых автоматов, которые предлагают потребителям товары от закусок до билетов, стали частью нашей повседневной жизни. В то время как технологический прогресс расширяет возможности и удобство использования таких устройств, он также увеличивает их уязвимость перед лицом кибератак. Вендинговые автоматы, оснащенные функциями безналичного расчета и подключенные к Интернету, могут стать целью для мошенников, стремящихся украсть банковские данные или нарушить их работу.

В данной статье представлен новый подход к обеспечению безопасности вендинговых автоматов с использованием методов искусственного интеллекта. Эта система предназначена не только для обнаружения уже известных видов атак, но и для прогнозирования и предотвращения потенциально новых угроз, что делает ее особенно актуальной в условиях постоянно развивающихся технологий взлома.

Система обнаружения аномалий использует сложные алгоритмы машинного обучения для анализа поведения пользователей и работы оборудования в реальном времени. Основываясь на анализе больших объемов данных, система способна выявлять необычные паттерны, которые могут указывать на попытку взлома или другие формы мошенничества. Эти алгоритмы включают в себя как нейронные сети, так и методы кластеризации, которые обучаются на основе исторических данных и могут адаптироваться к новым угрозам.

Разработка такой системы представляет собой значительный шаг вперед в области защиты коммерческих автоматов от киберпреступности.

Методология

Была разработана комплексная методология для создания системы обнаружения аномальной активности в вендинговых автоматах с использованием алгоритмов искусственного интеллекта. Исследование началось с этапа сбора данных, который включал аккумуляцию обширного массива операционных и транзакционных данных от вендинговых автоматов. Эти данные были предметом тщательной предобработки, включающей нормализацию, очистку и структурирование для последующего использования в обучающих моделях.

Далее последовало обучение машинных моделей, основанное на принципах глубокого обучения и нейронных сетей, а также использование методов кластеризации для выявления аномальных паттернов поведения. Процесс обучения включал настройку параметров алгоритмов для максимизации точности и минимизации ошибок, а также использование кросс-валидации для проверки обобщающей способности моделей на независимых данных.

Завершающий этап методологии заключался в валидации моделей, где были использованы различные метрики эффективности, такие как точность, полнота и F-мера, для оценки качества моделей в задачах обнаружения аномалий. В процессе валидации также проводился мониторинг за реакцией системы на потенциальные атаки в режиме реального времени, что позволило оценить оперативность и надежность системы перед её интеграцией в эксплуатационную среду вендинговых автоматов.

Реализация системы

Реализация предложенной системы обнаружения аномальной активности в вендинговых автоматах была выполнена с использованием передовых технологий искусственного интеллекта, обеспечивающих высокую точность и оперативность в детекции потенциальных угроз. В основе системы лежит модульная архитектура, включающая в себя компоненты для сбора

данных, их анализа, обнаружения аномалий и реагирования на инциденты. Каждый из этих модулей был интегрирован в управляющую программу вендинговых автоматов, что позволило обеспечить непрерывный мониторинг активности устройства и мгновенное реагирование на аномалии.

Техническая реализация включала развертывание серверов обработки данных, которые осуществляли прием и анализ информации от вендинговых автоматов в реальном времени. Для обработки данных применялись алгоритмы машинного обучения, способные адаптироваться к изменяющимся условиям эксплуатации устройств и эффективно идентифицировать не только известные виды атак, но и новые, ранее не встречавшиеся аномалии. Особое внимание было уделено защите персональных и платежных данных пользователей, для чего в системе были реализованы механизмы шифрования и безопасной передачи данных.

Дополнительно, система оснащена интерфейсом взаимодействия с операторами вендинговых сетей, что позволяет персоналу оперативно получать уведомления о подозрительных действиях и управлять параметрами системы безопасности. Это включает в себя возможности настройки чувствительности детекторов аномалий и выбора стратегий ответа на угрозы, что делает систему гибко адаптируемой к специфическим требованиям конкретной коммерческой сети.

Реализация данной системы обнаружения аномальной активности представляет собой комплексное решение, ориентированное на обеспечение высокого уровня безопасности вендинговых автоматов и защиты от атак с использованием самых современных достижений в области искусственного интеллекта и кибербезопасности.

Анализ результатов

Анализ включал оценку эффективности системы по нескольким ключевым показателям, таким как точность, полнота, и F-мера, что позволило обеспечить объективное измерение производительности в различных операционных условиях. Эти метрики были выбраны для того, чтобы оценить, насколько успешно система идентифицирует действительные случаи аномальной активности, минимизируя при этом количество ложных срабатываний.

Для анализа данных использовалась статистическая обработка результатов тестирования, проведенного на реальных устройствах в коммерческих условиях. В процессе анализа были рассмотрены различные сценарии взаимодействия пользователей с вендинговыми автоматами, включая стандартные транзакции и искусственно созданные условия для симуляции атак. Сравнение результатов работы системы до и после её внедрения позволило выявить значительное снижение уровня незаконных вмешательств и мошеннических операций.

Заключение

Подводя итог, стоит отметить, что разработанная система обнаружения аномальной активности в вендинговых автоматах демонстрирует значительные преимущества в обеспечении безопасности и защите от кибератак по сравнению с традиционными подходами. Благодаря применению современных алгоритмов машинного обучения и глубокого обучения, система способна эффективно идентифицировать и реагировать на аномалии в поведении пользователей и операционных данных, что существенно повышает уровень защиты пользовательских и платёжных данных.

Анализ результатов экспериментальных тестов подтвердил высокую эффективность системы в реальных условиях эксплуатации вендинговых автоматов. Особенно значимым является уменьшение количества незаконных вмешательств и мошеннических операций, что не только защищает финансовые интересы владельцев автоматов, но и укрепляет доверие конечных пользователей к этому виду сервиса.

На основе проведенного исследования можно сделать вывод о необходимости дальнейшего развития и адаптации предложенной системы для широкого спектра применений, включая другие типы автоматизированных устройств и систем. Исследование также подчеркивает важность продолжения работы в направлении улучшения алгоритмов обработки данных и машинного обучения, чтобы повысить точность, скорость реагирования и универсальность системы обнаружения аномалий в условиях растущего количества киберугроз.

Список литературы

1. Социальная инженерия: её методы и способы защиты Бударный Г.С., Дюсметова А.А., Казанцев А.А., Красов А.В. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т.. Санкт-Петербург, 2023. С. 200–204.
2. Анализ безопасности доменных систем Штеренберг С.И., Бударный Г.С., Чумаков И.В. В книге: Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022. С. 587–588.
3. Архитектура системы обнаружения и прогнозирования уязвимостей информационных систем на основе методов искусственного интеллекта Левшун Д. С. Информатизация и связь. 2024. № 3. С. 91–98.
4. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры Красов А.В., Гельфанд А.М., Фадеев И.И., Казанцев А. А. Свидетельство о регистрации программы для ЭВМ RU 2020617705, 10.07.2020. Заявка № 2020616731 от 29.06.2020.

УДК 004

Адаптивные системы защиты от DDoS-атак на базе технологий глубокого обучения

Даниленко Виктор Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной научной статье рассматриваются методы адаптивной защиты от DDoS-атак с применением технологий глубокого обучения. Описывается принцип построения нейросетевых моделей, способных в реальном времени анализировать сетевой трафик и адаптироваться к меняющимся векторам атак. Описаны системы, которые с помощью обучения распознают легитимный и вредоносный трафик, что позволяет минимизировать ложноположительные срабатывания и улучшить реакцию*

на инциденты. Подходы, основанные на глубоком обучении, демонстрируют высокую точность и масштабируемость, делая их эффективными в борьбе с DDoS-атаками различной сложности. Результаты показывают, что использование адаптивных систем способно существенно повысить устойчивость информационных систем к распределенным сетевым атакам.

***Abstract**: This research paper discusses methods of adaptive defense against DDoS attacks using deep learning techniques. The principle of building neural network models capable of analyzing network traffic in real time and adapting to changing attack vectors is described. Systems are described that use learning to recognize legitimate and malicious traffic to minimize false positives and improve incident response. Deep learning approaches demonstrate high accuracy and scalability, making them effective in combating DDoS attacks of varying complexity. The results show that the use of adaptive systems can significantly improve the resilience of information systems to distributed network attacks.*

***Ключевые слова**: Адаптивные системы защиты, DDoS-атаки, глубокое обучение, нейросетевые модели, сетевой трафик, анализ данных, обнаружение аномалий, информационная безопасность, машинное обучение.*

***Keywords**: Adaptive defence systems, DDoS attacks, deep learning, neural network models, network traffic, data analysis, anomaly detection, information security, machine learning.*

Введение

Современный цифровой мир сталкивается с усиленной угрозой распределенных отказоустойчивых сервисных атак (DDoS), что ставит повышенные требования к системам кибербезопасности. Традиционные методы защиты часто оказываются неэффективными перед лицом адаптивных и сложных векторов атак, что делает критически важным поиск новых решений в данной области. Одним из перспективных направлений является применение технологий глубокого обучения, способных обучаться на основе данных и динамически адаптироваться к меняющейся тактике злоумышленников.

Системы, основанные на глубоком обучении, предлагают революционный подход к обнаружению и противодействию DDoS-атакам благодаря своей способности к самообучению и выявлению скрытых в данных закономерностей, что традиционным системам недоступно. В статье исследуется потенциал использования таких моделей, как сверточные

и рекуррентные нейронные сети, для создания адаптивных систем защиты, способных распознавать и отражать DDoS-атаки в режиме реального времени.

Принцип построения нейросетевых моделей

Принцип построения нейросетевых моделей, способных в реальном времени анализировать сетевой трафик и адаптироваться к меняющимся векторам атак, основывается на нескольких ключевых этапах:

Сбор и предобработка данных

Для обучения нейронной сети требуется большое количество данных о сетевом трафике. Данные собираются из различных точек сети и могут включать пакеты данных, метаданные, логи и другую информацию, отражающую нормальное поведение и атаки. Затем эти данные подвергаются предобработке, которая включает нормализацию, устранение шума, заполнение пропусков и кодирование категориальных признаков.

Формирование обучающего набора

После предобработки данные разделяются на обучающие и тестовые наборы. Обучающий набор используется для «обучения» нейросети, а тестовый — для проверки её способности правильно классифицировать трафик.

Выбор архитектуры нейросети

Используются различные архитектуры глубоких нейронных сетей, такие как сверточные нейронные сети (CNN) для анализа данных в виде временных рядов или рекуррентные нейронные сети (RNN), в частности сети с долговременной краткосрочной памятью (LSTM), для обработки последовательностей данных.

Обучение нейросети

В процессе обучения нейросеть настраивает свои веса таким образом, чтобы минимизировать ошибку между её предсказаниями и реальными метками классов в обучающем наборе. Обучение продолжается до тех пор, пока не будет достигнута достаточная точность или другие критерии остановки.

Валидация и тестирование

После обучения модель тестируется на независимом тестовом наборе данных для оценки её способности к обобщению и правильной классификации новых данных.

Оценка модели и настройка параметров

Анализируются результаты и метрики эффективности модели, такие как точность, полнота, F1-мера и ROC AUC. На основе этих данных могут быть скорректированы параметры модели для улучшения её производительности.

Реализация и мониторинг

Готовая модель внедряется в сетевую инфраструктуру, где она анализирует трафик в реальном времени. Система должна быть способна быстро реагировать на изменения в данных, обновляя модель при появлении новых типов атак.

Непрерывное обучение

Для адаптации к новым угрозам модель должна постоянно обновляться, что может быть достигнуто путем непрерывного обучения на новых данных. Это может включать техники онлайн-обучения, где модель регулярно обновляется по мере поступления новых данных о сетевом трафике.

Автоматизация отклика

При обнаружении атаки система должна автоматически внедрять соответствующие меры защиты, такие как блокирование вредоносного трафика или изменение правил маршрутизации.

Такая модель является динамичной и адаптивной, что позволяет эффективно реагировать на постоянно эволюционирующие киберугрозы в динамичной сетевой среде.

Адаптивные системы защиты от DDoS-атак

Системы, оснащенные возможностями машинного и глубокого обучения для идентификации легитимного и вредоносного трафика, играют ключевую роль в современной кибербезопасности. Эти системы используют различные алгоритмы обучения для анализа сетевого трафика в реальном времени, что позволяет им эффективно распознавать и отличать нормальные запросы от потенциально опасных.

Основной задачей таких систем является уменьшение ложноположительных и ложноотрицательных срабатываний. Ложноположительное срабатывание происходит, когда система неверно определяет легитимный трафик как вредоносный, что может привести к ненужным блокировкам и прерыванию работы сервиса. Ложноотрицательное срабатывание — это когда вредоносный трафик не распознается и пропускается системой, что может привести к успешной кибератаке.

Чтобы справиться с этими вызовами, системы используют сложные алгоритмы и большие объемы обучающих данных для тренировки. Эти данные включают как исторические, так и текущие данные о трафике, которые помогают системе учиться и адаптироваться к новым угрозам. Процесс обучения включает не только различение типов трафика, но и оценку контекста операций, что значительно повышает точность идентификации угроз.

С постоянным обновлением и адаптацией к новым тенденциям и атакам, системы обучения становятся более устойчивыми к ошибкам и способными предоставлять более точные и оперативные реакции на инци-

денты. Это, в свою очередь, ведет к повышению общей безопасности сетей и информационных систем.

Заключение

В завершение, можно сделать вывод о том, что интеграция глубокого обучения в системы защиты от DDoS-атак представляет собой многообещающее направление, которое может существенно повысить уровень безопасности информационных систем в условиях постоянно растущей киберугрозы.

Список литературы

1. Кибирев М.П., Миняев А.А., Скорых М. А. Сравнительный анализ утилит для проведения атаки PTH // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023).— 2023. — С. 710–715.
2. Ковалев И. А., Косов Н. А. Состязательные атаки в нейронных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 490–492.
3. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 406–411.
4. Ковцур М. М. и др. Исследование способов удаленного перехвата трафика в корпоративных сетях //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия.— 2021. — Т. 1. — С. 68–75.
5. Исследование влияния атак на беспроводные сети WI-FI 6E Ковцур М.М., Винников С.А., Трезоров В.И., Киструга А.Ю.Экономика и качество систем связи. 2023. № 2 (28). С. 87–92.

УДК 004

Оценка точности и скорости детектирования DDoS-атак с использованием глубокого обучения

Даниленко Виктор Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной научной статье рассматривается применение методов глубокого обучения для детектирования DDoS-атак, с особым акцентом на анализе точности и скорости этих методов. Используя различные архитектуры нейронных сетей, включая сверточные и рекуррентные сети, проведено сравнение их эффективности в задачах обнаружения атак в реальном времени. Особое внимание уделяется способности моделей минимизировать ложные срабатывания при сохранении высокой скорости реагирования, что критически важно для систем кибербезопасности в условиях больших объемов данных.*

***Abstract**: This research paper discusses the application of deep learning techniques to detect DDoS attacks, with a particular focus on analyzing the accuracy and speed of these techniques. Using different neural network architectures, including convolutional and recurrent networks, a comparison of their performance in real-time attack detection tasks is made. Particular attention is paid to the models' ability to minimize false positives while maintaining high response rates, which is critical for cybersecurity systems in data-intensive environments.*

***Ключевые слова**: Глубокое обучение, детектирование DDoS-атак, нейронные сети, сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN), точность обнаружения, скорость обработки, кибербезопасность, минимизация ложных срабатываний.*

***Keywords**: Deep learning, DDoS attack detection, neural networks, convolutional neural networks (CNNs), recurrent neural networks (RNNs), detection accuracy, processing speed, cybersecurity, false alarm minimisation.*

Введение

С ростом зависимости современного общества от информационных технологий, кибербезопасность становится все более важной сферой исследований. Одной из значительных угроз для онлайн-сервисов являются распределенные отказоустойчивые сервисные (DDoS) атаки, способные нарушить

работу целых систем и организаций. Традиционные методы обнаружения часто не способны справляться с растущей сложностью и масштабом таких атак, что требует разработки новых, более эффективных решений.

Глубокое обучение, благодаря своей способности к анализу больших объемов данных и выявлению сложных закономерностей, представляет собой обещающий подход в борьбе с DDoS-атаками. Применение моделей глубокого обучения, таких как сверточные нейронные сети (CNN) и рекуррентные нейронные сети (RNN), позволяет не только улучшить точность обнаружения атак, но и сократить время реакции систем безопасности.

Анализ методов глубокого обучения для детектирования DDoS-атак

Анализ методов глубокого обучения для детектирования DDoS-атак с фокусом на точность и скорость выявляет ряд ключевых аспектов, важных для выбора подходящей модели. Методы глубокого обучения, такие как сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN) и автоэнкодеры, каждый по-своему подходят для обработки и анализа сетевого трафика.

Сверточные нейронные сети, благодаря своей способности к эффективной обработке больших объемов данных и выделению важных признаков из этих данных, обладают высокой точностью. Они идеально подходят для задач, где важно быстро и точно идентифицировать сложные паттерны, что критически важно для минимизации времени реакции на атаки. Однако, требования к вычислительным ресурсам и время, необходимое для обучения таких моделей, могут быть значительными, что потенциально замедляет их применение в режиме реального времени при ограниченных ресурсах.

Рекуррентные нейронные сети и их разновидности, такие как LSTM, предоставляют преимущества при работе с последовательностями данных, такими как сетевой трафик. Они могут эффективно улавливать временные зависимости и изменения в паттернах трафика, что делает их особенно полезными для детектирования аномалий в длительных потоках данных. Эти модели могут демонстрировать высокую точность, но их скорость обработки и потребность в данных для обучения могут ограничивать их использование в сценариях с требованиями к немедленному ответу.

Автоэнкодеры предлагают уникальный подход к обнаружению аномалий, обучаясь на «нормальных» данных и выявляя отклонения как аномалии. Это позволяет им эффективно обнаруживать DDoS-атаки как значительные отклонения от обычного трафика. После начального обучения они могут работать быстро, однако точность может снижаться при наличии шума или непредвиденных легитимных изменений в трафике, что увеличивает риск ложных срабатываний.

Оценка точности и скорости детектирования DDoS-атак

В таблице «таб.1», представлена информация о различных методах глубокого обучения для детектирования DDoS-атак, описывающая их преимущества, недостатки и скорость обработки:

Таблица1. Сравнение **различных методов глубокого обучения для детектирования DDoS-атак.**

Метод	Преимущества	Недостатки	Скорость обработки
Сверточные нейронные сети (CNN)	Высокая точность в распознавании визуальных и временных паттернов; подходит для данных с пространственными зависимостями.	Требует значительных вычислительных ресурсов для обучения; менее эффективен для сложных временных зависимостей.	Быстрая после обучения; подходит для реального времени.
Рекуррентные нейронные сети (RNN) и LSTM	Эффективны в анализе временных последовательностей; учитывают предыдущие данные.	Сложны в реализации; могут страдать от проблем с затуханием градиента.	Могут быть медленнее на этапе вывода, особенно в сложных моделях.
Автоэнкодеры	Отлично подходят для обнаружения аномалий; могут обучаться на немаркированных данных.	Чувствительны к шуму; могут выдавать ложные срабатывания при необычных легитимных паттернах.	Обычно быстрые после обучения, особенно при использовании упрощенных моделей.

Выбор метода глубокого обучения для системы обнаружения DDoS-атак зависит от конкретных требований к задаче. Если задача требует высокой точности в обнаружении пространственных паттернов в данных, CNN может быть предпочтительнее. Для задач, где критично важно учитывать временные зависимости в данных, RNN или LSTM предложат лучшие результаты. Автоэнкодеры идеально подходят для сценариев, где необходимо обнаруживать аномалии без четких предварительных меток.

Следовательно, комплексный подход, возможно, комбинирующий несколько методов в одной системе, может обеспечить наилучшее сочетание точности и скорости, адаптируясь к разнообразным и динамически меняющимся угрозам в сфере кибербезопасности.

Заключение

В завершение, можно сделать вывод о том, что сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN), включая LSTM, и автоэнкодеры могут значительно улучшить способность систем кибербезопасности распознавать и реагировать на DDoS-атаки в сравнении с традиционными подходами. Эти технологии предоставляют возможности для более точного и быстрого обнаружения атак за счет своей способности анализировать большие объемы данных и выявлять сложные паттерны поведения.

Список литературы

1. Исследование влияния атак на беспроводные сети WI-FI 6E Ковцур М.М., Винников С.А., Трезоров В.И., Киструга А.Ю.Экономика и качество систем связи. 2023. № 2 (28). С. 87–92.
2. Кибирев М. П., Миняев А. А., Скорых М. А. Сравнительный анализ утилит для проведения атаки PTH // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023).— 2023. — С. 710–715.
3. Ковалев И. А., Косов Н. А. Состязательные атаки в нейронных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 490–492.

4. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 406–411.
5. Ковцур М. М. и др. Исследование способов удаленного перехвата трафика в корпоративных сетях //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия.— 2021. — Т. 1. — С. 68–75.

УДК 004

Обзор алгоритмов глубокого обучения в задачах идентификации и митигации DDoS-атак

Даниленко Виктор Сергеевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В данной научной статье представлен обзор алгоритмов глубокого обучения, применяемых в задачах идентификации и митигации DDoS-атак. Статья описывает ключевые методы, включая сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN), и автоэнкодеры, а также их способность анализировать и обрабатывать сетевой трафик для эффективного обнаружения вредоносных активностей. Освещаются преимущества и ограничения каждого подхода, а также обсуждаются перспективы их развития в контексте улучшения защитных механизмов в кибербезопасности.*

***Abstract**: This research paper presents an overview of deep learning algorithms applied to the task of identifying and mitigating DDoS attacks. The paper describes key methods, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and autoencoders, and their ability to analyze and process network traffic to effectively detect malicious activity. The advantages and limitations of each approach are highlighted, and their prospects are discussed in the context of improving cybersecurity defense mechanisms.*

***Ключевые слова**: Глубокое обучение, детектирование DDoS-атак, сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN), автоэнкодеры, идентификация угроз, митигация атак, кибербезопасность, анализ сетевого трафика, машинное обучение.*

***Keywords**: deep learning, DDoS attack detection, convolutional neural networks (CNNs), recurrent neural networks (RNNs), autoencoders, threat identification, attack mitigation, cybersecurity, network traffic analysis, machine learning.*

Введение

В эпоху цифровизации и всеобщей интернетизации, кибербезопасность становится критически важной областью, требующей непрерывного развития и адаптации к новым угрозам. Одной из наиболее распространенных и разрушительных угроз являются распределенные отказоустойчивые сервисные (DDoS) атаки. Эти атаки могут дестабилизировать операции предприятий, затормозить трафик важнейших онлайн-сервисов и даже повлиять на национальную безопасность. В связи с этим разработка эффективных средств для идентификации и митигации DDoS-атак становится приоритетной задачей. Современные методы искусственного интеллекта, особенно глубокое обучение, представляют собой мощный инструмент в арсенале специалистов по кибербезопасности. Глубокое обучение позволяет создавать модели, которые могут автоматически обнаруживать сложные паттерны и аномалии в данных сетевого трафика, что является ключом к успешному распознаванию и предотвращению DDoS-атак.

Алгоритмы глубокого обучения, применяемые в задачах идентификации и митигации DDoS-атак

Алгоритмы глубокого обучения стали ключевыми инструментами в задачах идентификации и митигации DDoS-атак благодаря их способности эффективно обрабатывать и анализировать большие объемы данных, выявляя сложные паттерны и аномалии, которые трудно распознать традиционными методами. Основные алгоритмы глубокого обучения, используемые в этих задачах, включают сверточные нейронные сети (CNN), рекуррентные нейронные сети (RNN), автоэнкодеры, и сети прямого распространения (feedforward networks). Вот как каждый из этих методов применяется в борьбе с DDoS-атаками:

Сверточные нейронные сети (CNN)

CNN применяются для анализа и обработки данных трафика, так как они способны эффективно извлекать важные признаки из многомерных данных. В контексте DDoS-атак, CNN могут анализировать паттерны тра-

фика и выявлять аномальные изменения, которые часто указывают на атаки. Они особенно эффективны в задачах, где важно распознавание визуальных образов в данных, например, во временных рядах сетевого трафика.

Рекуррентные нейронные сети (RNN) и LSTM

RNN и их развитие LSTM особенно подходят для обработки последовательностей данных, таких как логи сетевого трафика. Эти модели могут учитывать предыдущие состояния системы, что позволяет им обнаруживать сложные временные зависимости в данных трафика, характерные для DDoS-атак. RNN и LSTM могут предсказывать будущие состояния системы на основе предыдущих данных, что делает их мощным инструментом для предупреждения о потенциальных атаках.

Автоэнкодеры

Автоэнкодеры часто используются для обнаружения аномалий, включая аномалии в сетевом трафике, что делает их полезными для идентификации DDoS-атак. Эти сети обучаются восстанавливать свои входные данные, минимизируя ошибку между входом и выходом. В случае аномального трафика, ошибка реконструкции возрастает, что может служить сигналом о DDoS-атаке.

Сети прямого распространения (Feedforward Networks)

Эти нейронные сети могут быстро обрабатывать данные и классифицировать их, что делает их подходящими для реализации в системах реального времени. Они могут использоваться для определения, является ли сетевой трафик нормальным или аномальным, основываясь на изученных признаках трафика.

Общий подход

Эти модели часто комбинируются в сложные системы для улучшения точности детектирования и уменьшения ложных срабатываний. Методы

машинного обучения могут дополняться традиционными методами мониторинга и управления трафиком, создавая многоуровневую оборонительную структуру.

Использование этих алгоритмов глубокого обучения позволяет создавать более надежные и адаптивные системы кибербезопасности, способные противостоять сложным и постоянно эволюционирующим DDoS-атакам.

Перспективы развития в контексте улучшения защитных механизмов в кибербезопасности

Алгоритмы глубокого обучения становятся все более важным инструментом в области кибербезопасности, предлагая новые способы защиты от сложных угроз, таких как DDoS-атаки. С развитием этих технологий, возможности для их применения в кибербезопасности продолжают расширяться, обещая значительные улучшения в эффективности обнаружения угроз и реакции на них.

Одним из наиболее значимых аспектов является способность алгоритмов глубокого обучения адаптироваться к новым и изменяющимся паттернам атак, что позволяет им предвосхищать и нейтрализовывать угрозы, еще до того, как они смогут нанести вред. Это достигается благодаря способности моделей непрерывно обучаться на актуальных данных, что делает системы защиты более гибкими и прогностически эффективными.

Также важно отметить, что с увеличением объемов данных и улучшением алгоритмов, системы на базе глубокого обучения становятся способными быстрее и точнее идентифицировать потенциально вредоносные действия в сети. Это приводит к уменьшению ложных срабатываний и ускорению реакции на реальные угрозы, что крайне важно для поддержания непрерывности бизнес-процессов и защиты данных.

Интеграция алгоритмов глубокого обучения в кибербезопасности также открывает двери для разработки более умных, автономных систем, которые могут самостоятельно адаптироваться и реагировать на киберугрозы без необходимости постоянного вмешательства человека. Это создает

основу для более устойчивых и надежных кибербезопасных сред, способных выдерживать даже самые сложные атаки в будущем.

Заключение

В завершение, можно сделать вывод о том, что алгоритмы глубокого обучения предоставляют значительные возможности для улучшения идентификации и митигации DDoS-атак. Сверточные нейронные сети, рекуррентные нейронные сети, автоэнкодеры и другие подходы глубокого обучения демонстрируют высокую эффективность в обнаружении и предотвращении таких атак за счёт своей способности анализировать большие объёмы данных и выявлять сложные паттерны поведения. Данные технологии способствуют не только улучшению точности обнаружения атак, но и снижению количества ложных срабатываний, что критически важно для поддержания операционной стабильности и безопасности в современных сетевых средах.

Список литературы

1. Бударный Г.С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 406–411.
2. Ковцур М.М. и др. Исследование способов удаленного перехвата трафика в корпоративных сетях //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия.— 2021. — Т. 1. — С. 68–75.
3. Исследование влияния атак на беспроводные сети WI-FI 6E Ковцур М.М., Винников С.А., Трезоров В.И., Киструга А.Ю.Экономика и качество систем связи. 2023. № 2 (28). С. 87–92.
4. Кибирев М.П., Миняев А.А., Скорых М. А. Сравнительный анализ утилит для проведения атаки PTH // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023).— 2023. — С. 710–715.

5. Ковалев И. А., Косов Н. А. Состязательные атаки в нейронных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 490–492.

УДК 004.056

Методы и средства обеспечения информационной безопасности

Губарев Владимир Дмитриевич

студент факультета Инфокоммуникационных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

Бирих Эрнест Владимирович

старший преподаватель кафедры Защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: В статье рассматриваются средства и методы защиты информации в информационных системах, которые могут быть использованы при разработке политики безопасности предприятия, выборе систем защиты. Приведены их задачи, а также актуальность их совместного использования.*

***Abstract**: The article considers means and methods of information protection in information systems, which can be used in the development of enterprise security policy, selection of protection systems. Their tasks as well as the relevance of their joint use are given.*

***Ключевые слова**: информационная безопасность, программное обеспечение, идентификация, аутентификация, криптография, информация, доступность информации, целостность информации, конфиденциальность.*

***Keywords**: information security, software, identification, authentication, cryptography, information, information availability, information integrity, confidentiality.*

В нашем мире информация является важным и наиболее ценным ресурсом практически во всех областях экономической, социальной, политической

и даже духовной сферах жизни общества. Поэтому важно не только наличие различной информации, но и её защита, хранение и передача. Каждое предприятие заинтересовано в защите своих ресурсов. По этой причине информационная безопасность является актуальным и важным аспектом жизни современного человека.

Информационной безопасностью называют меры по предотвращению несанкционированного доступа, деформации, преобразования, задержки доступа и раскрытия конфиденциальной информации, иными словами — сохранения составляющих информационной безопасности: конфиденциальности, целостности и доступности.

Для обеспечения информационной безопасности используются разнообразные механизмы защиты, при создании которых используются следующие средства:

- Физические — препятствуют физическому проникновению к местам хранения информации, ими могут быть механические, электро- или электронно-механические устройства.
- Аппаратные — электронные, электромеханические устройства, установленные или подключённые к месту хранения данных. Их задачей является защита средств и систем вычислительной техники, таких как: процессор, терминал и периферийное оборудование.
- Программные — обеспечивают логические и интеллектуальные функции защиты. Они включаются в программное обеспечение или в состав систем аппаратуры контроля.
- Аппаратно-программные (Технические) — электронные устройства и специальные программы, входящие в состав системы предприятия.
- Криптографические — модифицирование информации с целью её сокрытия от посторонних лиц, и организации безопасной передачи от отправителя к получателю без её раскрытия и повреждения.
- Административные (организационные) — методы организационного характера, устанавливающие процессы функционирования системы обработки данных, применение ресурсов системы, деятельность персонала и порядок взаимодействия с системой.
- Правовые — законы, указы, нормативные акты, регламентирующие правила использования информации и взаимодействия с ней. Соблю-

дение таких норм не всегда является обязательным и в большинстве случаев несёт ознакомительный и профилактический характер.

- Морально-этические — правила обращения с информацией, сложившиеся по мере распространения ЭВМ в обществе.

Средства информационной безопасности разделяются на несколько основных категорий — формальные и неформальные.

К формальным средствам защиты относятся технические, криптографические и программные средства обеспечения информационной безопасности.

Формальным средствам защиты соответствуют такие методы обеспечения информационной безопасности как:

- Препятствие — представляет собой преграду на пути злоумышленника, будь то невозможность физически добраться до объекта хранения информации, или программное ограничение доступа к информации.
- Управление доступом — ограничение доступа не аутентифицированного пользователя. Идентификация и аутентификация используются для исключения неправомерного доступа к информации или информационного ресурса.
- Маскировка — ограничение доступа к информации путём её сокрытия или шифрования, что не позволяет незнающему пользователю получить доступ к информации.

К неформальным средствам защиты относятся организационные, законодательные и морально-этические средства обеспечения информационной безопасности.

Неформальным средствам защиты соответствуют такие методы обеспечения информационной безопасности как:

- Регламентация — установление правил, определяющих порядок доступа к информации.
- Принуждение — применяется через законы, указы или нормативные акции для выполнения указанных в них требованиях.
- Побуждение — направление для выполнения определённых профилактических действий, направленных на обеспечение безопасности.

Также в задачи организационных средств обеспечения информационной безопасности входят:

1. Разработка внутренней документации, которая устанавливает правила работы с вычислительной техникой и порядок обработки информации.
2. Проведение инструктажа и периодические проверки рабочего персонала, также инициируют подписание дополнительных соглашений к трудовым договорам, в которых установлена ответственность за разглашение или неправомерное использование конфиденциальных сведений, доступных доверенному лицу.
3. Разграничение зон ответственности, используется для избегания ситуаций, при которых информация передаётся в распоряжение одного из сотрудников, организация работы в программах документооборота и наблюдение, чтобы критические данные хранились в безопасных хранилищах.
4. Составление планов восстановления утраченных данных на случай выхода системы из строя.
5. Внедрение программного обеспечения, которое защищает данные от копирования, уничтожения, модификации или другого неправомерного использования конфиденциальных и данных.

Для организации обеспечения информационной безопасности необходимо реализовать основные составляющие:

- Создание режима охраны информации — определить какими методами и в каком порядке будет защищена информация.
- Разработка правил взаимоотношений между сотрудниками — регулирование сообщения между сотрудниками, передачи информации друг-другу и область заинтересованности каждого сотрудника.
- Регламентация работы с документами — определение порядка доступа к информации и правила обращения с конфиденциальными данными.
- Правила использования технических средств в рамках существующего правового поля Российской Федерации.
- Аналитическая работа по оценке угроз информационной безопасности — оценка риска, проведение аудитов.

Основной рекомендацией по разработке систем безопасности — это комплексный подход к проблеме. В целях обеспечения информационной безопасности необходимо использовать сразу несколько методов защиты, иначе система защиты может оказаться недостаточно крепкой. Комплекс

мер направленных на предотвращение атак называется политикой безопасности предприятия.

Своевременное проведение аудитов, повышение защищённости информационных систем и комплексное использование методов защиты информации обеспечивает безопасность информации и осуществлении сохранения целостности информации, её конфиденциальности и высокой доступности.

Список литературы

1. Беляев А. В. Курс лекций «Методы и средства защиты информации» [Электронный ресурс]. URL: http://citforum.ru/internet/infsecure/index.shtml (Дата обращения 17.04.2024)
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011.— 416 с.
3. Способы защиты информации: сайт searchinform.ru [Электронный ресурс]. URL: https://searchinform.ru/analitika-v-oblasti-ib/Issledovaniya-v-oblasti-ib/metody-obespecheniya-informatsionnoj-bezopasnosti/ (Дата обращения 17.04.2024)
4. С. К. Варлатая, М. В. Шаханова. Программно-аппаратная защита информации: учеб. пособие — Владивосток: Изд-во ДВГТУ, 2007.
5. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 266–270.
6. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 563–568.
7. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности //Актуальные проблемы инфотелекоммуникаций в науке и образовании.— 2015. — С. 193–197.
8. Бирих Э. В., Ферапонтова С. С. К вопросу об аудите персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018).— 2018. — С. 111–114.

9. Бирих Э. В. и др. Исследование вопросов повышения уровня защищенности органов исполнительной власти //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018).— 2018. — С. 107–110.

УДК 004.7

Разработка и анализ методов мониторинга и обнаружения утечек данных через технические каналы в реальном времени

Фазлыева Эмилия Маратовна

студентка Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Эта статья посвящена исследованию методов обнаружения и мониторинга утечек данных через технические каналы в режиме реального времени, оценивая их эффективность и пригодность для использования в современных системах безопасности информации.*

***Abstract**: This paper investigates methods for real-time detecting and monitoring data leaks through technical channels, evaluating their effectiveness and suitability for use in modern information security systems.*

***Ключевые слова**: мониторинг, утечка, технические каналы, разработка, методы.*

***Keywords**: needs, motivation, development, frustration, behavior, anxiety, family, consequences.*

Введение

В современном информационном обществе безопасность данных играет ключевую роль в деятельности организаций и частных лиц. Утечки конфиденциальной информации через технические каналы представляют серьезную угрозу для бизнеса, частной жизни и национальной безопасности. Поэтому разработка эффективных методов мониторинга и обнару-

жения утечек данных в режиме реального времени становится все более актуальной задачей.

В настоящей статье будут рассмотрены современные подходы и технологии в области безопасности данных, сосредоточившись на обнаружении утечек через технические каналы, такие как сетевые передачи данных и устройства хранения информации. Будет проведен анализ различных методов, основанных на машинном обучении, анализе поведения пользователей, сетевых алгоритмах и других средствах, направленных на выявление и предотвращение потенциальных утечек данных.

Целью данной работы является оценка эффективности различных методов мониторинга и обнаружения утечек данных, а также их применимость в реальных условиях работы с информацией.

Анализ существующих методов мониторинга и обнаружения утечек данных:

- Обзор современных систем безопасности данных: Этот этап включает оценку текущего положения дел в области безопасности данных, включая рассмотрение популярных коммерческих и открытых решений. Будет проведен анализ их функциональности, стойкости к различным типам атак, применимости к разным типам организаций и сетевой инфраструктуре.
- Недостатки в обнаружении утечек через технические каналы: Здесь мы выявим слабые места существующих методов обнаружения утечек. Это может быть неэффективное распознавание шаблонов атак, недостаточная скорость реакции на угрозы или сложности в интеграции с другими системами безопасности.
- Рассмотрение традиционных подходов к безопасности данных: Это включает анализ технологий шифрования, аутентификации и авторизации. Будет изучена их эффективность в предотвращении утечек данных и выявление возможных пробелов, например, связанных с утечками ключей шифрования или слабыми механизмами аутентификации.
- Изучение сценариев утечек данных: Здесь мы проанализируем различные сценарии, в которых возможны утечки данных через технические каналы. Это могут быть атаки через сетевые протоколы, утечки данных на уровне хранения, угрозы, связанные с мобильными устройствами

и др. Цель — выявить типичные пути атак и слабые места существующих систем безопасности.

Разработка новых методов мониторинга и обнаружения утечек данных:

- Предложение новых подходов к обнаружению утечек данных: Здесь мы предложим инновационные методы, такие как алгоритмы машинного обучения, анализ поведения пользователей, анализ сетевого трафика и другие техники. Эти методы должны быть способными эффективно выявлять аномальное поведение, связанное с утечками данных.
- Создание системы мониторинга: Мы разработаем систему, способную оперативно реагировать на потенциальные утечки через различные технические каналы. Это включает в себя создание централизованной платформы, интегрирующей различные методы обнаружения утечек и обеспечивающей мгновенное информирование и реагирование.
- Тестирование разработанных методов: Проведем тестирование новых методов на реальных сценариях утечек данных. Это поможет оценить их эффективность, стойкость к атакам и способность к адаптации к новым угрозам.

Сравнительный анализ различных методов мониторинга и обнаружения утечек данных:

- Сравнение производительности методов: Здесь мы проведем анализ скорости реакции различных методов мониторинга и обнаружения утечек данных. Это включает время, необходимое для обнаружения утечек, а также скорость предпринятых мер по предотвращению утечек и восстановлению информационной безопасности. Такой анализ позволит определить, насколько оперативно и эффективно каждый метод реагирует на угрозы.
- Оценка затрат и сложности внедрения: Этот аспект анализа включает в себя оценку финансовых затрат на внедрение и поддержку каждого метода мониторинга и обнаружения утечек данных. Будут учтены расходы на приобретение необходимого оборудования или программного обеспечения, обучение персонала, а также затраты на обслуживание и обновление системы. Кроме того, будет оценена сложность внедрения каждого метода, включая необходимость изменения существующей инфраструктуры, интеграции с другими системами безопасности и обучения персонала.

Практическое применение разработанных методов:

- Сравнение производительности методов: Здесь мы проведем анализ скорости реакции различных методов мониторинга и обнаружения утечек данных. Это включает время, необходимое для обнаружения утечек, а также скорость предпринятых мер по предотвращению утечек и восстановлению информационной безопасности. Такой анализ позволит определить, насколько оперативно и эффективно каждый метод реагирует на угрозы.
- Оценка затрат и сложности внедрения: Этот аспект анализа включает в себя оценку финансовых затрат на внедрение и поддержку каждого метода мониторинга и обнаружения утечек данных. Будут учтены расходы на приобретение необходимого оборудования или программного обеспечения, обучение персонала, а также затраты на обслуживание и обновление системы. Кроме того, будет оценена сложность внедрения каждого метода, включая необходимость изменения существующей инфраструктуры, интеграции с другими системами безопасности и обучения персонала.

Заключение

В заключении исследования о методах мониторинга и обнаружения утечек данных через технические каналы в реальном времени были получены следующие ключевые выводы:

1. Новые методы, основанные на машинном обучении и анализе поведения пользователей, эффективнее обнаруживают утечки данных по сравнению с традиционными подходами.
2. Новые методы обладают более высокой производительностью и оперативностью реакции на угрозы, что позволяет минимизировать риски и быстрее предотвращать утечки.
3. Экономический анализ показывает, что вложения в внедрение новых методов оправданы благодаря повышенной эффективности и снижению возможных убытков от утечек данных.
4. Рекомендации по выбору и практическому применению новых методов могут быть сделаны на основе проведенного анализа кейсов использования.

Список литературы

1. Манжула, К. А. Радиоперехват IoT трафика / К. А. Манжула, Г. С. Бударный // Научный аспект.— 2024. — Т. 33, № 2. — С. 4222–4226. — EDN PSNZRF.
2. Технические аспекты управления с использованием сети Интернет: Монография / А. А. Алейников, К. З. Билятдинов, А. В. Красов [и др.]. — Санкт-Петербург: Центр научно-информационных технологий «Астерион», 2016.— 305 с. — ISBN 978–5–00045–408–4. — EDN XGTJLL.
3. Разработка блока обнаружения и коррекции ошибок для устройства диагностирования каналов передачи цифровой информации / А. К. Сагдеев, И. Г. Штеренберг, С. И. Штеренберг, О. М. Виноградова // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2020.— № 1. — С. 15–24. — DOI 10.46418/2079–8199_2020_1_3. — EDN PYQLFU.
4. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения / А. В. Красов, С. И. Штеренберг, Р. М. Фахрутдинов [и др.] // T-Comm: Телекоммуникации и транспорт.— 2018. — Т. 12, № 10. — С. 36–40. — DOI 10.24411/2072–8735–2018–10154. — EDN YMWVOX.
5. Штеренберг, С. И. Методика управления системами обработки и сбора Больших данных с поддержкой мониторинга встроенными программными агентами / С. И. Штеренберг // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2020.— № 4. — С. 26–35. — DOI 10.46418/2079–8199_2020_4_4. — EDN DZATII.

УДК 004

Выявление и противодействие новым угрозам информационной безопасности

Юрченко Олег Дмитриевич

студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича

***Аннотация**: Научная статья посвящена анализу современных вызовов в сфере кибербезопасности и разработке эффективных методов и инструментов для их преодоления. В статье рассматриваются последние тенденции в развитии киберугроз, включая фишинг, вредоносные программы, атаки на критически важную инфраструктуру и утечки данных. Представляются результаты исследований, направленных на выявление новых векторов атак и разработку комплексных стратегий защиты, включая международное сотрудничество, развитие технологий шифрования и обучение пользователей основам кибергигиены. Особое внимание уделяется адаптации методов машинного обучения и искусственного интеллекта для предотвращения киберинцидентов и минимизации их последствий. Статья предлагает комплексный подход к укреплению информационной безопасности, который может быть применен на различных уровнях — от индивидуального пользователя до государственных структур.*

***Abstract**: The scientific article is devoted to the analysis of modern cybersecurity challenges and the development of effective methods and tools to overcome them. The article discusses the latest trends in the development of cyber threats, including phishing, malware, critical infrastructure attacks and data breaches. It presents the results of research aimed at identifying new attack vectors and developing comprehensive defense strategies, including international cooperation, development of encryption technologies, and cyber hygiene education for users. Special attention is paid to the adaptation of machine learning and artificial intelligence techniques to prevent cyber incidents and minimize their consequences. The article proposes a comprehensive approach to strengthening information security that can be applied at various levels, from the individual user to government agencies.*

***Ключевые слова**: Информационная безопасность, киберугрозы, фишинг, вредоносное ПО, критическая инфраструктура, утечка данных, методы защиты, машинное обучение, искусственный интеллект, шифрование.*

***Keywords**: Information security, cyber threats, phishing, malware, critical infrastructure, data leakage, defense methods, machine learning, artificial intelligence, encryption.*

Введение

В эпоху цифровизации и всемирной информатизации проблема обеспечения информационной безопасности приобретает особую актуальность. Развитие информационных технологий приводит к постоянному возникновению новых угроз, которые могут нанести значительный вред как отдельным пользователям, так и целым государствам. Поэтому задача своевременного выявления и эффективного противодействия новым угрозам становится приоритетной для специалистов в области информационной безопасности.

Новые угрозы информационной безопасности

Новые угрозы информационной безопасности постоянно развиваются по мере того, как технологии продвигаются вперёд и как изменяется глобальная киберпреступность. Вот несколько примеров новых угроз, с которыми сталкиваются организации и индивидуальные пользователи:

Расширенные устойчивые угрозы (APT): Эти сложные кибератаки обычно организуются государственными или крупными преступными группами и направлены на длительное незаметное проникновение в сети целевых организаций для кражи данных или шпионажа.

Фишинговые атаки с использованием искусственного интеллекта: Атаки фишинга становятся всё более изощрёнными с использованием AI для создания более убедительных поддельных сообщений и веб-сайтов, что увеличивает вероятность обмана пользователей.

Ransomware-as-a-Service (RaaS): это модель предоставления программ-вымогателей как услуги, что позволяет даже неопытным преступникам запускать атаки вымогательства, что увеличивает общее количество и разнообразие атак ransomware.

Цепочки поставок и атаки на третьих сторонах: Киберпреступники нацеливаются на менее защищенные компании в цепочке поставок для получения доступа к более крупным и лучше защищенным сетям.

Глубокие подделки (deepfakes) и манипуляции данными: Использование искусственного интеллекта для создания фальсифицированных аудио

и видео записей может подорвать доверие и распространять дезинформацию, что может быть использовано для манипулирования индивидами или рынками.

Угрозы интернета вещей (IoT): Увеличение количества подключенных устройств расширяет поверхность атак и создает новые уязвимости, особенно когда эти устройства недостаточно защищены.

Квантовые вычисления и криптография: хотя квантовые компьютеры все еще находятся в разработке, их потенциал может поставить под угрозу существующие методы криптографической защиты, что требует разработки новых подходов к шифрованию.

Справиться с этими и другими новыми угрозами требует от организаций постоянного мониторинга, обновления безопасности и адаптации к меняющейся среде киберугроз.

Методы и технологии для защиты информационных систем

Выявление и противодействие новым угрозам информационной безопасности — это комплексная задача, которая включает в себя ряд методов и технологий для защиты информационных систем и данных от нежелательных и вредоносных атак.

Выявление угроз: это первый и основной шаг, который включает в себя мониторинг сетевого трафика, анализ уязвимостей системы, а также использование систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS). Современные технологии искусственного интеллекта и машинного обучения также используются для выявления аномалий и потенциально вредоносных действий.

Анализ угроз: после идентификации потенциальной угрозы следует её анализ. Это включает в себя определение типа угрозы, источника, потенциальных целей и способов её устранения. Для анализа могут использоваться различные инструменты и методики, включая форензику данных и анализ поведения.

Обновление и адаптация защитных мер: Угрозы информационной безопасности постоянно эволюционируют, поэтому важно регулярно обновлять системы безопасности и адаптировать стратегии защиты к новым

условиям. Это может включать обновление программного обеспечения, регулярное тестирование уязвимостей и реализацию новых технологических решений.

Обучение и осведомленность: Важным аспектом противодействия угрозам является повышение уровня осведомленности и обучение сотрудников. Многие атаки успешны из-за человеческого фактора, такого как фишинг или небрежное обращение с данными. Регулярное обучение и проведение тренировок помогают снизить вероятность успешных атак.

Использование комплексного подхода, сочетание технологий, процессов и образовательных программ позволяют эффективно выявлять и противостоять новым и развивающимся угрозам информационной безопасности.

Заключение

В заключение, можно отметить, что данная статья подчеркивает важность непрерывного анализа и адаптации к новым угрозам информационной безопасности. Это требует постоянного обновления знаний, инструментов и методик для защиты информационных активов и поддержания устойчивости в меняющемся цифровом мире. Важно призывать к дальнейшему исследованию в этой области и к активному взаимодействию между академическими, промышленными и правительственными организациями для разработки новых решений, направленных на обеспечение информационной безопасности на глобальном уровне.

Список литературы

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 266–270.
2. Гельфанд А. М. и др. Оценка рисков и угроз безопасности в среде «умный дом» //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 316–321.

3. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации //Инновационные технологии, экономика и менеджмент в промышленности.— 2021. — С. 203–204.
4. Шемякин С. Н. и др. Использование теории графов для моделирования безопасности облачных систем //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2021.— № . 2. — С. 31–35.
5. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. — Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015.— 63 с. — EDN CMMEML.

ДЛЯ ЗАМЕТОК

Журнал «Научный аспект №4 2024»
Эл. почта редакции: public@na-journal.ru
Подробнее на сайте: https://na-journal.ru