НАУЧНЫЙ АСПЕКТ

na-journal.ru

2023

№11

ТОМ 28

УДК 001.8(082)

ББК 1
Н 34

Периодичность – 12 раз в год

Свидетельство ПИ № ФС 77-84349

ISSN 2226-5694

Состав ред. коллегии и сведения об учредителе
приведены на сайте https://na-journal.ru

Н 34 НАУЧНЫЙ АСПЕКТ № 11 2023. – Самара: Изд-во ООО «Аспект», 2023 . – Т28 . – 130 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 14.12.2023

Бумага ксероксная. Печать оперативная. Заказ № .
Формат 60×84 /16. Объем 7,8 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

УДК 004.72

Проприетарные протоколы канального уровня компании Cisco и их аналоги

Макшанский Анатолий Романович

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

***Аннотация**: Данная статья посвящена исследованию проприетарных протоколов канального уровня компании Cisco и их аналогов. Рассматриваются основные характеристики данных протоколов, а также их особенности и возможности использования в сетевых технологиях. Также приводится сравнение популярных проприетарных протоколов с открытыми аналогами, что поможет определиться с выбором подходящего решения для конкретной сетевой инфраструктуры. В статье также обсуждаются преимущества и недостатки использования проприетарных протоколов на примере компании Cisco, которая является одним из лидеров в области сетевых технологий.*

***Abstract**: This article is devoted to the study of Cisco proprietary link layer protocols and their analogs. The main characteristics of these protocols, as well as their features and possibilities of their use in network technologies are considered. It also provides a comparison of popular proprietary protocols with their open analogs, which will help to decide on the choice of a suitable solution for a particular network infrastructure. The article also discusses advantages and disadvantages of using proprietary protocols on the example of Cisco, which is one of the leaders in the field of network technologies.*

***Ключевые слова**: CISCO, сетевые протоколы, проприетарные протоколы, сетевая инфраструктура.*

***Keywords**: CISCO, network protocols, proprietary protocols, network infrastructure.*

В настоящее время сети являются неотъемлемой частью нашей жизни и используются для передачи различных типов данных. Существует множество протоколов, которые регулируют передачу данных в этих сетях.

Одним из таких типов протоколов являются проприетарные протоколы канального уровня и их аналоги.

Проприетарные протоколы канального уровня отличаются тем, что они разработаны конкретными компаниями и предназначены для использования только в их продуктах. Эти протоколы обеспечивают определенный уровень безопасности и производительности, но, в то же время, они часто несовместимы с другими устройствами и протоколами.

Аналоги проприетарных протоколов канального уровня — это открытые протоколы, которые могут быть использованы в различных устройствах и приложениях. Такие протоколы обеспечивают большую гибкость и расширяемость, что позволяет им быть более универсальными.

Цель данной статьи — исследование проприетарных протоколов канального уровня и их аналогов, оценка их преимуществ и недостатков, а также анализ возможных сфер применения.

Для достижения поставленной цели были проведены исследования проприетарных протоколов канального уровня и их аналогов. В ходе аналитического исследования были проанализированы основные характеристики проприетарных протоколов, такие как безопасность, производительность, совместимость и расширяемость. Также были рассмотрены примеры проприетарных протоколов, таких как CDP, VTP, HSRP, PVST, PAgP.

Сравнение

- CDP (Cisco Discovery Protocol) и LLDP (Link Layer Discovery Protocol) — это протоколы канального уровня, которые используются для обнаружения соседних устройств в компьютерных сетях. Несмотря на то, что они выполняют похожую функцию, они имеют некоторые отличия.

Основное отличие между CDP и LLDP заключается в том, что CDP является проприетарным протоколом, разработанным Cisco Systems, и поддерживается только на устройствах Cisco, тогда как LLDP — открытым протоколом, который поддерживается большинством производителей сетевых устройств.

CDP может передавать информацию об устройствах Cisco, таких как модель, серийный номер, версия ПО, IP-адрес и другие характеристики.

Он также может передавать сведения о VLAN'ах, связанных с портами, и информацию о наличии и конфигурации PoE (Power over Ethernet). LLDP, с другой стороны, предоставляет возможность передавать информацию о соседних устройствах, включая тип устройства, идентификатор, параметры порта и другие характеристики. Он также может передавать информацию о VLAN'ах, связанных с портами, и других параметрах.

CDP имеет более широкий функционал в отношении обнаружения устройств Cisco, включая информацию о PoE и других конфигурационных параметрах. Тем не менее, LLDP является более гибким протоколом, так как он поддерживается большинством производителей сетевых устройств и может быть использован в более разнообразных сетевых средах.

LLDP передает информацию в виде TLV (Type-Length-Value) пакетов, которые содержат соответствующую информацию. Эта информация может включать в себя тип устройства (например, маршрутизатор или коммутатор), идентификатор устройства, поддерживаемые протоколы, параметры порта (например, скорость, дуплексный режим) и другие характеристики.

LLDP является стандартом IEEE 802.1AB и поддерживается большинством производителей сетевых устройств, поэтому он может быть использован в различных сетевых средах. Кроме того, LLDP является открытым протоколом, что позволяет его использование без ограничений на различных устройствах.

- VTP (VLAN Trunking Protocol) и GVRP (GARP VLAN Registration Protocol) — это протоколы, используемые для настройки виртуальных локальных сетей (VLANы) в компьютерных сетях. Они могут быть использованы для обеспечения управления VLANами, что может упростить процесс настройки и снизить затраты на администрирование.

VTP позволяет автоматически настраивать VLANы на всех коммутаторах в сети. Он может быть настроен в трех режимах: сервер, клиент или прозрачный. Коммутатор, работающий в режиме сервера, может создавать, изменять и удалять VLANы, а остальные коммутаторы получают обновления от сервера. Коммутатор, работающий в режиме клиента, не может создавать, изменять или удалять VLANы и получает информацию только от сервера. Коммутатор, работающий в режиме прозрачный, пере-

сылает VTP-фреймы, но не обрабатывает их. VTP также поддерживает три режима передачи данных: transparent, client и server.

GVRP является открытым протоколом, который используется для динамической настройки VLANы на коммутаторах. GVRP может обнаруживать и регистрировать VLANы на коммутаторе, в зависимости от того, какие порты подключены. Коммутаторы, поддерживающие GVRP, могут обмениваться информацией о VLANы и создавать новые VLANы, когда это необходимо. GVRP также может использоваться для удаления VLANы, которые больше не используются.

Основное отличие между VTP и GVRP заключается в том, что VTP является проприетарным протоколом, который поддерживается только на устройствах Cisco, тогда как GVRP — это открытый протокол, который поддерживается многими производителями сетевого оборудования. Кроме того, VTP позволяет настраивать VLANы статически и динамически, а GVRP используется только для динамической настройки VLANов.

- HSRP (Hot Standby Router Protocol) и VRRP (Virtual Router Redundancy Protocol) — это протоколы, используемые для обеспечения высокой доступности в компьютерных сетях. Они позволяют группе роутеров работать в режиме резервирования, чтобы обеспечить непрерывность работы сети.

HSRP — это проприетарный протокол, который разработан компанией Cisco. Он используется для настройки двух или более роутеров в группу, которая работает в режиме резервирования. Один из роутеров в группе выбирается в качестве активного (primary), который обрабатывает все трафик и выполняет функции шлюза по умолчанию в сети. Остальные роутеры работают в режиме ожидания (standby mode) и мониторят доступность активного роутера. Если активный роутер выходит из строя, то один из роутеров в режиме ожидания автоматически становится активным и продолжает обрабатывать трафик.

VRRP является открытым протоколом, который используется для настройки нескольких роутеров в группу, которая работает в режиме резервирования. Один из роутеров в группе выбирается в качестве виртуального (virtual), который обрабатывает все трафик и выполняет функции шлюза по умолчанию в сети. Остальные роутеры работают в режиме ожидания

(backup mode) и мониторят доступность виртуального роутера. Если виртуальный роутер выходит из строя, то один из роутеров в режиме ожидания автоматически становится виртуальным и продолжает обрабатывать трафик.

Основное отличие между HSRP и VRRP заключается в том, что HSRP — это проприетарный протокол, разработанный компанией Cisco, тогда как VRRP — это открытый протокол, который может использоваться на разном оборудовании от разных производителей. Кроме того, HSRP использует свой собственный MAC-адрес для виртуального роутера, в то время как VRRP использует виртуальный MAC-адрес, который зависит от номера группы.

- PVST (Per-VLAN Spanning Tree), PVST+ (Per-VLAN Spanning Tree Plus) и RPVST+ (Rapid Per-VLAN Spanning Tree Plus) — это варианты протокола STP (Spanning Tree Protocol), который используется для обеспечения отказоустойчивости и предотвращения петель в компьютерных сетях. STP/RSTP/MSTP являются стандартными реализациями протокола STP.

Основное отличие между STP/RSTP/MSTP и PVST/PVST+/RPVST+ заключается в том, что STP/RSTP/MSTP работают на уровне всех VLANs в сети, тогда как PVST/PVST+/RPVST+ используют отдельное дерево для каждого VLAN. Это означает, что PVST/PVST+/RPVST+ могут поддерживать различные конфигурации портов для каждого VLAN, тогда как STP/RSTP/MSTP требуют одинаковые конфигурации портов для всех VLANs.

PVST был первоначально разработан компанией Cisco для работы с VLANs. Он использует отдельное дерево для каждого VLAN и может поддерживать отдельную конфигурацию портов для каждого дерева. PVST+ был создан для улучшения производительности и внедрения RSTP. Он использует тот же формат кадров, что и PVST, но поддерживает быстрое восстановление деревьев для каждого VLAN. RPVST+ — это улучшенная версия PVST+, которая также поддерживает быстрое восстановление деревьев для каждого VLAN.

STP (Spanning Tree Protocol) — это стандартный протокол, который предотвращает петли в сети, блокируя один из портов на коммутаторе. STP требует времени для сходимости после изменения топологии сети, поскольку

вся сеть должна быть пересчитана. RSTP (Rapid Spanning Tree Protocol) — это улучшенная версия STP, которая может быстрее переключаться на новый путь при изменении топологии сети. MSTP (Multiple Spanning Tree Protocol) — это расширение RSTP, которое позволяет группировать несколько VLANs в единую группу и использовать одно дерево для этой группы.

- PAgP (Port Aggregation Protocol) и LACP (Link Aggregation Control Protocol) — это протоколы, используемые для создания агрегированных линков (link aggregation) в компьютерных сетях. Они позволяют комбинировать несколько физических портов для создания одного логического канала с большей пропускной способностью и высокой отказоустойчивостью.

PAgP — это проприетарный протокол, разработанный компанией Cisco. Он используется для настройки агрегированных линков между устройствами Cisco. PAgP может использоваться для создания только одного логического канала между двумя коммутаторами, и он поддерживает режимы активного (active) и пассивного (passive). В режиме активного устройство отправляет запросы на создание агрегированного линка, в то время как в режиме пассивного оно принимает такие запросы.

LACP — это открытый протокол, который был стандартизован IEEE. Он также используется для настройки агрегированных линков между устройствами. LACP поддерживает создание нескольких логических каналов между коммутаторами, и он использует режимы активного и пассивного, аналогичные PAgP. Однако, LACP также поддерживает дополнительный режим, называемый «On», который позволяет устройству создавать логический канал без необходимости отправлять запросы.

Основное отличие между PAgP и LACP заключается в том, что PAgP — это проприетарный протокол, который можно использовать только на устройствах Cisco, тогда как LACP — это открытый стандартный протокол, который поддерживается различными производителями сетевого оборудования. Кроме того, LACP поддерживает создание нескольких логических каналов между коммутаторами, тогда как PAgP может использоваться только для создания одного логического канала.

Результаты исследования показали, что проприетарные протоколы канального уровня обладают определенными преимуществами, такими

как более высокий уровень безопасности и производительности. Однако, они также имеют недостатки, такие как ограниченность в совместимости и расширяемости. В то же время, аналоги проприетарных протоколов канального уровня обеспечивают большую гибкость и расширяемость, при этом сохраняя достаточный уровень безопасности и производительности.

В заключении исследования были предложены рекомендации для выбора протоколов канального уровня в зависимости от задач и конкретных условий сетевой инфраструктуры. Было выделено, что для сетевых систем, требующих высокого уровня безопасности и производительности, лучше использовать проприетарные протоколы, в то время как для более гибких и универсальных систем лучше использовать открытые аналоги.

Кроме того, в исследовании было выявлено, что применение проприетарных протоколов канального уровня может быть оптимальным в случаях, когда существует необходимость в использовании специфических функций или возможностей, которые не поддерживаются открытыми аналогами. Также было отмечено, что эти протоколы могут обеспечить высокий уровень защиты данных в условиях повышенной угрозы кибератак.

Однако, стоит также учитывать, что использование проприетарных протоколов канального уровня может иметь негативные последствия для различных сторон, таких как пользователи, производители оборудования и разработчики программного обеспечения. Например, они могут ограничить выбор пользователя в плане выбора оборудования и ПО, а также повысить затраты на его приобретение.

Таким образом, в статье были проанализированы проприетарные протоколы канального уровня и их аналоги, оценены их преимущества и недостатки, а также проанализированы возможные сферы применения. Результаты исследования могут быть полезны для производителей оборудования и разработчиков ПО, а также для пользователей, которые выбирают протоколы для своих нужд.

Список литературы

1. Красов А.В., Салита А.С., Пешков А.И., Ушаков И. А. Программа детектирования сетевой стеганографии в блоках данных протокола TCP //

Свидетельство о регистрации программы для ЭВМ RU 2023663566, 26.06.2023. Заявка № 2023662332 от 14.06.2023.
2. Волкогонов В.Н., Преображенский А.И., Ушаков И. А. Уязвимости программно-определяемых сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференцияи: в 4 т.. 2019. С. 279–284.
3. Красов А.В., Гельфанд А.М., Фадеев И.И., Казанцев А. А. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры // Свидетельство о регистрации программы для ЭВМ RU 2020617705, 10.07.2020. Заявка № 2020616731 от 29.06.2020.
4. Алехин Р.В., Катасонов А.И., Лесневский М.В., Смирнов Д. Н. Исследование критической уязвимости сервиса аутентификации и последствий для медицинских учреждений, относящихся к субъектам критической информационной инфраструктуры // Офтальмохирургия. 2022. № S4. С. 115–122.
5. Красов А.В., Косов Н.А., Холоденко В. Ю. Исследование методов провижининга безопасной сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации // Colloquium-Journal. 2019. № 13–2 (37). С. 243–247.

УДК 004

Как проводить аудит безопасности информационных систем: основные этапы и методы

Макшанский Анатолий Романович

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

***Аннотация**: Аудит безопасности информационных систем является ключевым инструментом защиты данных от кибератак. В статье рассматриваются основные этапы проведения аудита: анализ требований, идентификация рисков, оценка рис-*

ков, разработка рекомендаций и контроль их выполнения. На каждом этапе используются различные методы, такие как анализ кода, тестирование на проникновение, сканирование уязвимостей и обучение персонала. Внедрение этих мер способствует повышению уровня безопасности информационных систем и снижению вероятности кибератак.

***Abstract**: Information systems security audit is a key tool to protect data from cyberattacks. The article discusses the main stages of auditing: requirements analysis, risk identification, risk assessment, development of recommendations and control of their implementation. Each stage utilizes various techniques such as code analysis, penetration testing, vulnerability scanning, and staff training. Implementing these measures helps improving the security of information systems and reduce the likelihood of cyberattacks.*

***Ключевые слова**: аудит, безопасность, информационные системы, этапы, методы, защита данных, кибератака, риски, анализ, идентификация, контроль, тестирование.*

***Keywords**: audit, security, information systems, stages, methods, data protection, cyber attack, risks, analysis, identification, control, testing.*

Аудит безопасности информационных систем (ИС) является одним из важнейших инструментов для обеспечения защиты данных и предотвращения кибератак. Он позволяет оценить текущее состояние безопасности системы, выявить уязвимости и слабые места, а также разработать рекомендации по их устранению. В этой статье мы рассмотрим основные этапы аудита безопасности ИС и применяемые при этом методы.

Основные этапы проведения аудита безопасности информационных систем:

1. Анализ требований является одним из ключевых этапов в процессе проведения аудита. На этой стадии необходимо тщательно проработать и определить цели и основные задачи аудита, чтобы обеспечить его эффективность и результативность. Это также позволяет команде специалистов определить состав команды и ресурсы, необходимые для успешного выполнения поставленных задач.

Одним из важных аспектов данного этапа является сбор информации о той системе или процессе, который будет подвергнут аудиту. Это включает в себя получение подробных сведений о структуре системы, ее функ-

циональности, используемых технологиях, а также изучение документации и отчетов о предыдущих аудитах, если таковые имеются.

На основе полученной информации проводится анализ системы на предмет соответствия требованиям и стандартам, определение потенциальных рисков и слабых мест, а также выработка рекомендаций по улучшению системы и повышению ее эффективности.

Таким образом, анализ требований на этапе аудита играет ключевую роль в определении стратегии и тактики проведения аудита, определении состава команды и ресурсов, а также в сборе необходимой информации для проведения качественного

2. Идентификация рисков является важным этапом в аудите безопасности информационных систем. Риски определяются как потенциальные угрозы или уязвимости, которые могут негативно повлиять на работу системы или привести к нарушению ее безопасности. Для идентификации рисков используются различные методы анализа:

Анализ кода: Этот метод предполагает изучение исходного кода системы на наличие уязвимостей или ошибок, которые могут привести к нарушению безопасности.

Тестирование на проникновение: Этот метод заключается в имитации действий злоумышленника, пытающегося получить доступ к системе. Это позволяет выявить уязвимости в системе защиты.

Сканирование уязвимостей: Этот метод использует базы данных уязвимостей для поиска потенциальных уязвимостей в системе.

Каждый из этих методов имеет свои преимущества и недостатки, и их использование зависит от конкретной ситуации и целей аудита. Важно использовать комбинацию методов для более полного и точного определения рисков.

3. Оценка рисков. После того, как были выявлены уязвимости в информационной системе, необходимо провести оценку рисков, связанных с этими уязвимостями. Оценка рисков позволяет определить, насколько критичными являются эти уязвимости и какие меры необходимо принять для их устранения или снижения их воздействия на систему.

Оценка рисков может проводиться с использованием различных методов, таких как анализ воздействия уязвимостей на систему, оценка вероят-

ности их использования злоумышленниками, а также анализ возможных последствий их использования. На основе результатов оценки рисков определяются меры по устранению уязвимостей, такие как обновление программного обеспечения, изменение настроек системы или внедрение

4. На основании проведенного аудита информационной системы разрабатываются рекомендации по улучшению ее безопасности. Рекомендации могут включать в себя изменения в конфигурации системы, внедрение дополнительных средств защиты, проведение обучения персонала и другие меры, направленные на повышение уровня безопасности системы.

Рекомендации должны быть основаны на результатах аудита и оценке рисков, связанных с уязвимостями системы. Они должны быть конкретными, измеримыми, достижимыми, релевантными и ограниченными во времени (SMART).

После разработки рекомендаций они должны быть обсуждены с заинтересованными сторонами, такими как руководство организации, специалисты по информационной безопасности и пользователи системы. Затем рекомендации должны быть реализованы и контролироваться для обеспечения их эффективности.

5. Контроль выполнения рекомендаций: после разработки рекомендаций, они внедряются и контролируются, чтобы убедиться в их эффективности. Это включает отслеживание изменений в системе, оценку результатов внедрения рекомендаций и корректировку мер по необходимости. Также важно обучать персонал использованию новых средств защиты и обеспечивать их осведомленность о новых процедурах безопасности. Наконец, необходимо проводить периодические аудиты для оценки текущего состояния системы безопасности и определения необходимости в дополнительных мерах защиты.

Список литературы

1. Дойникова Е.В., Котенко И. В. Оценивание защищенности и выбор контрмер для управления кибербезопасностью.
2. Бирих Э.В., Ферапонтова С.С. К вопросу об аудите персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и об-

разовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С. В. Бачевского. 2018. С. 111–114.
3. Пестов И. Е. Методика автоматизированного противодействия несанкционированным воздействиям на инстансы облачной инфраструктуры с использованием безагентного метода сбора метрик // диссертация на соискание ученой степени кандидата технических наук / Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. Санкт-Петербург, 2022
4. Гайфулина Д.А., Котенко И.В., Федорченко А. В. Методика лексической разметки структурированных бинарных данных сетевого трафика для задач анализа протоколов в условиях неопределенности // Системы управления, связи и безопасности. 2019. № 4. С. 280–299.
5. Котенко И. В. Аналитическая обработка больших массивов гетерогенных данных о событиях кибербезопасности в интересах оценки состояния, поддержки принятия решений и расследования компьютерных инцидентов в критически важных инфраструктурах // Отчет о НИР № 21–71–20078. Российский научный фонд. 2021.

УДК 004

Влияние видеокарты на музыкальное производство: роль и необходимость графического компонента в работе музыкального компьютера

Бабушкина Полина Алексеевна

преподаватель Инженерной школы одежды (колледжа) структурного подразделения Санкт-Петербургского государственного университета промышленных технологий и дизайна; студентка Российского государственного педагогического университета имени А. И. Герцена

***Аннотация**: Рассматривается влияние видеокарты на процессы музыкального производства, фокусируя внимание на роли и значимости графического компонента в функционировании музыкального компьютера. Анализируется необходимость наличия*

видеокарты даже в сценариях, где основное внимание уделяется обработке аудиоданных. В статье подчеркивается взаимосвязь между производительностью видеокарты и эффективностью использования программных инструментов музыкального производства, а также рассматривает возможные сценарии, в которых мультимедийные функции видеокарты могут оказаться существенными при создании и редактировании музыкальных проектов. Предоставляются практические рекомендации для выбора и оптимизации видеокарты в системах музыкального компьютера.

***Abstract**: The impact of the graphics card on music production processes is examined, focusing on the role and importance of the graphics component in the functioning of a music computer. The necessity of a graphics card is analyzed even in scenarios where the focus is on audio data processing. The paper emphasizes the relationship between graphics card performance and the effective use of music production software tools, and examines possible scenarios in which the multimedia functions of a graphics card may be essential in the creation and editing of music projects. Practical guidelines for video card selection and optimization in music computer systems are provided.*

***Ключевые слова**: AMD, NVIDIA, DAW, GTX, музыкальное производство, создание музыки, видеокарта, графический интерфейс, программное обеспечение.*

***Keywords**: AMD, NVIDIA, DAW, GTX, music production, music creation, video card, graphical interface, software.*

Современные технологии тесно переплетаются в сфере музыкального производства, и, казалось бы, видеокарта, предназначенная для обработки видеоизображений, несущественна в работе музыкальных компьютеров. Однако, стоит лишь коснуться вопроса о влиянии видеокарты на музыкальное творчество, и становится ясным, что графический компонент играет значимую функциональную роль.

Основной аргумент в пользу наличия видеокарты в музыкальном компьютере связан с графическим интерфейсом программ для музыкального производства. Программы, такие как Digital Audio Workstations (DAW), обеспечивают пользователей интуитивно понятным визуальным интерфейсом для создания, редактирования и управления звуковыми данными. Это включает в себя окна редактирования, треки, визуализации спектрограмм и другие графические элементы, которые позволяют музыкантам визуализировать и манипулировать своим творчеством. Графический интерфейс становится своеобразным полотном для артиста, предоставляя

удобный и наглядный способ взаимодействия с музыкальным материалом. Отображение треков, звуковых волн, а также возможность моментального визуального редактирования спектрограмм существенно упрощают творческий процесс и позволяют музыкантам более эффективно воплощать свои звуковые концепции. Таким образом, графические элементы, которые видеокарта способна обеспечить, содействуют удобству и эффективности в работе музыкальных профессионалов.

Для Digital Audio Workstations (DAW) не всегда необходима мощная видеокарта, так как основная нагрузка ложится на центральный процессор (CPU) и звуковую карту. Однако, в зависимости от конкретных требований и предпочтений пользователя, уровня сложности проектов и визуальных компонентов DAW, выбор видеокарты может быть различным. Вот несколько примеров видеокарт, которые могут подойти для известных программ DAW:

1. Avid Pro Tools — профессиональное ПО для звукозаписи, музыкального производства и звукового дизайна, применяемое в индустрии для создания, редактирования и сведения музыки и звуков в различных мультимедийных проектах. Обеспечивает высокоточные инструменты для обработки аудиосигналов и поддерживает использование виртуальных инструментов и плагинов. Pro Tools славится своей стабильностью и широким функционалом, устанавливая стандарты в индустрии звукозаписи.

Для данного ПО рекомендуется следующая видеокарта: NVIDIA GeForce GTX 1050 Ti или AMD Radeon RX 560.

Для профессиональных нужд в работе с программой Avid Pro Tools рассматриваются видеокарты высокого уровня, такие как NVIDIA Quadro P2000 или AMD Radeon Pro WX 5100. Это профессиональное оборудование обеспечивает дополнительные вычислительные мощности и высокую надежность, что является существенным фактором в условиях звукозаписи и музыкального производства.

2. Apple Logic Pro X — профессиональное программное обеспечение для создания музыки и звукозаписи на платформе macOS. Обладает обширными инструментами, виртуальными эффектами и удобным интерфейсом, подходящим для домашнего использования и профессиональных студий.

Для использования данного ПО необходима интегрированная графика на MacBook Pro, так как Logic Pro X хорошо оптимизирован для работы с встроенными графическими решениями Apple.

3. Steinberg Cubase — это профессиональное программное обеспечение для создания музыки и звукозаписи. Предоставляет мощные инструменты для композиции, аранжировки и обработки аудио, а также включает в себя виртуальные инструменты и эффекты. Широко используется в индустрии звукозаписи и студийном производстве.

Для достижения оптимальной производительности вам рекомендуется уделить внимание видеокартам более высокого класса, например, NVIDIA GeForce GTX 960 или AMD Radeon RX 480. В случае профессиональных задач, таких как работа в графических приложениях, предпочтение стоит отдать более специализированным моделям, например, NVIDIA Quadro P1000 или AMD Radeon Pro WX 4100.

4. Ableton Live — это программное обеспечение для создания музыки и проведения живых выступлений. Обладает уникальными функциями для создания, записи, редактирования и аранжировки звуков. Интуитивный интерфейс и широкий выбор виртуальных инструментов делают Ableton Live популярным среди продюсеров и диджеев. Программа также предоставляет возможность для реального времени обработки звука и создания уникальных эффектов во время выступлений.

Для достижения лучших результатов рекомендуется использовать видеокарты, такие как NVIDIA GeForce GTX 660 или AMD Radeon HD 7850. В сфере профессионального использования стоит рассмотреть более специализированные модели, такие как NVIDIA Quadro K1200 или AMD Radeon Pro WX 3100.

5. FL Studio — это программное обеспечение для создания музыки и аудио-производства. Он предоставляет обширный набор инструментов и функций для создания, редактирования, аранжировки и записи музыки. FL Studio поддерживает виртуальные инструменты, эффекты и автоматизацию параметров для творческого процесса. Сочетание интуитивного интерфейса и мощных возможностей делает FL Studio популярным выбором как для начинающих, так и для опытных музыкантов и продюсеров.

Для эффективной работы в программе FL Studio рекомендуется использовать видеокарты, такие как NVIDIA GeForce GTX 770 или AMD Radeon R9 290. В случае профессионального применения, возможно, имеет смысл рассмотреть более специализированные модели, например, NVIDIA Quadro P600 или AMD Radeon Pro WX 2100.

Важно отметить, что конкретные рекомендации могут меняться в зависимости от версии программы, обновлений и требований, установленных производителем. При выборе видеокарты также необходимо учитывать разрешение монитора, количество используемых экранов, а также возможность расширенных функций, таких как поддержка CUDA или OpenCL, если они важны для потребностей в производстве музыки.

Влияние видеокарты на музыкальное производство нельзя недооценивать. Несмотря на первичную роль в обеспечении графического интерфейса, видеокарта также может способствовать более эффективному взаимодействию с программными инструментами и визуализации звуковых данных. В мире музыкального творчества, где слияние звука и визуализации становится все более важным, графический компонент оказывается неотъемлемой частью технологического арсенала музыкантов и продюсеров.

Список литературы

1. PRO TOOLS [Электронный ресурс] — URL: https://goo.su/ioxv (дата обращения 01.12.2023)
2. Logic Pro [Электронный ресурс] — URL: https://www.apple.com/logic-pro/ (дата обращения 01.12.2023)
3. Cubase: Music Production Software [Электронный ресурс] — URL: https://www.steinberg.net/cubase/ (дата обращения 01.12.2023)
4. Ableton Live [Электронный ресурс] — URL: https://www.ableton.com/en/live/ (дата обращения 01.12.2023)
5. FL STUDIO 21 [Электронный ресурс] — URL: https://www.image-line.com/fl-studio/ (дата обращения 01.12.2023)

УДК 004

Сравнение программного обеспечения Adobe и Figma. Проблемы и перспективы в мире графического дизайна

Бабушкина Полина Алексеевна

преподаватель Инженерной школы одежды (колледжа) структурного подразделения Санкт-Петербургского государственного университета промышленных технологий и дизайна; студентка Российского государственного педагогического университета имени А. И. Герцена

***Аннотация**: Представляется систематическое исследование, посвященное сравнению двух ведущих платформ для графического дизайна — Adobe Creative Cloud и Figma. Проводится анализ актуальных проблем, с которыми сталкиваются пользователи Adobe, предлагая детальный обзор технических и пользовательских аспектов использования программы. Особое внимание уделяется перспективам развития Figma, включая инновационные подходы и тенденции в области графического дизайна. Исследование предоставляет научное основание для понимания технологических вызовов и прогнозирования будущего развития инструментов графического дизайна, способствуя обсуждению и развитию в данной области.*

***Abstract**: A systematic study comparing two leading platforms for graphic design, Adobe Creative Cloud and Figma, is presented. An analysis of current problems faced by Adobe users is carried out, offering a detailed overview of the technical and user aspects of using the program. Particular attention is paid to Figma's future prospects, including innovative approaches and trends in graphic design. The study provides a scholarly basis for understanding technological challenges and predicting the future development of graphic design tools, contributing to discussion and development in the field.*

***Ключевые слова**: графический дизайн, совместная работа, векторная графика, ядро процессора, дизайнер, изображение, инструмент.*

***Keywords**: graphic design, collaboration, vector graphics, processor core, designer, image, tool.*

В мире графического дизайна существует несколько ключевых инструментов, которые играют важную роль в работе дизайнеров. Два из наиболее популярных и широко используемых инструментов — Adobe Creative Cloud и Figma — предлагают различные подходы к созданию дизайна,

имеют свои преимущества и недостатки. В данной статье рассматриваются проблемы и перспективы использования этих инструментов в графическом дизайне.

Adobe Creative Cloud, с безоговорочным лидерством в области графического дизайна, утвердил свою репутацию благодаря влиятельным программам, таким как Photoshop, Illustrator и InDesign. Эти инструменты предоставляют дизайнерам полный спектр возможностей, включая работу с графикой, векторной графикой, макетами и видеоредакцией. Однако, с появлением новых технологий и эволюцией требований рынка, Adobe сталкивается с рядом актуальных проблем.

Модель подписки Adobe Creative Cloud, стала одной из главных проблем, с которой сталкиваются пользователи. Эта система подписки, хотя и предоставляет доступ ко всем программам Adobe, может оказаться финансово недоступной для индивидуальных дизайнеров и малых студий. Это вызвало неудовлетворенность среди пользователей, и они ищут более доступные и гибкие альтернативы.

Кроме того, для работы с программами Adobe часто требуются значительные вычислительные ресурсы. Это становится проблемой для тех, кто использует менее мощные компьютеры, что ограничивает доступность программ для широкого круга пользователей.

Например, Adobe Photoshop использует многозадачные вычисления и способен использовать несколько ядер процессора для увеличения производительности в некоторых задачах. В частности, многие операции в Photoshop, такие как фильтры, могут быть распараллелены для использования нескольких ядер, что позволяет программе работать быстрее на многоядерных процессорах.

Однако, не все задачи в Photoshop могут быть полностью распараллелены, и некоторые функции, такие как некоторые инструменты рисования и манипуляции с изображениями, могут зависеть от одного ядра процессора. Поэтому, хотя Photoshop может использовать многие ядра в некоторых случаях, эффективность использования многозадачности может варьироваться в зависимости от конкретной задачи.

В свете этих проблем, появляется растущий интерес к альтернативным платформам, которые предоставляют более гибкие модели оплаты и менее

жесткие требования к аппаратному обеспечению. Это ставит под сомнение будущее доминирования Adobe Creative Cloud и стимулирует поиск инновационных и более доступных решений в области графического дизайна.

А Figma, вступив в область графического дизайна, действительно представила собой значительные инновации в области совместной работы и гибкости творческого процесса. Это веб-приложение, в отличие от традиционных программ, обеспечивает возможность совместной работы в реальном времени, что облегчает командную работу и устраняет проблемы географического удаления.

Однако, несмотря на многочисленные преимущества, Figma не лишено определенных ограничений. Одной из значимых проблем является ограниченный оффлайн-режим. Поскольку Figma в значительной степени зависит от интернет-соединения, работа в условиях низкой связи или отсутствия интернета может быть затруднительной. Это особенно актуально в ситуациях, когда стабильность интернета не гарантирована, что может привести к потере доступа к данным и ухудшению производительности.

Более того, возможности Figma при работе с растровыми изображениями ограничены по сравнению с специализированными растровыми редакторами, такими как Adobe Photoshop.

Одной из основных ограничений Figma в работе с растровыми изображениями является ограниченный инструментарий для редактирования и обработки пиксельной графики. В Figma можно добавлять и встраивать растровые изображения в дизайн, выполнять их изменение по размеру и обрезку, но при этом функционал для сложных манипуляций и коррекции, характерных для растровых редакторов, ограничен.

Еще одним важным аспектом является ограниченная поддержка цветов в растровых изображениях в Figma. Например, программы, такие как Photoshop, обеспечивают более широкий спектр цветовых коррекций, фильтров и эффектов.

Таким образом, хотя Figma может быть удобным инструментом для работы с векторной графикой и дизайном интерфейсов, он не является идеальным выбором для полноценной работы с растровой графикой. В таких случаях, где требуется более глубокое редактирование и манипуляции

с растровыми изображениями, рекомендуется использовать специализированные растровые редакторы.

Еще одним важным вопросом является проблема безопасности данных в облаке. Поскольку Figma базируется на облачных технологиях, возникают определенные опасения относительно конфиденциальности и безопасности хранимой информации. Для некоторых компаний и дизайнеров, особенно работающих с чувствительными данными, это может быть препятствием при выборе инструмента.

Таким образом, хотя Figma предоставляет множество преимуществ в области графического дизайна, необходимо учитывать как позитивные, так и негативные аспекты при принятии решения о его использовании, особенно в зависимости от конкретных потребностей и требований пользователя.

Таким образом, развитие веб-приложения Figma становится объектом пристального внимания, поскольку оно не только предоставляет решения для текущих задач, но и стремится адаптироваться к меняющимся потребностям и требованиям пользователей.

Вопрос о выборе между Adobe и Figma становится ключевым, учитывая разнообразие потребностей конечных пользователей. Переход от традиционных программных решений, таких как Adobe Creative Cloud, к современным и гибким веб-приложениям типа Figma, становится отражением тенденции к более удобному и коллаборативному дизайну.

Анализ предоставляет не только обзор текущего состояния инструментов графического дизайна, но и научное основание для понимания вызовов, с которыми сталкиваются дизайнеры. Результаты исследования могут послужить основой для прогнозирования будущего развития инструментов графического дизайна, включая тенденции в использовании веб-технологий, методов совместной работы и визуальных подходов.

Важность активного обсуждения и инновационного развития в этой области несомненна, поскольку она способствует эволюции инструментария и открывает новые перспективы для дизайнеров. Путем стимулирования диалога и обмена идеями исследование поощряет разработку более эффективных и адаптивных инструментов, соответствующих потребностям современного графического дизайна.

Список литературы

1. Adobe Creative Cloud [Электронный ресурс] — URL: https://www.adobe.com (дата обращения 01.12.2023)
2. Adobe Photoshop [Электронный ресурс] — URL: https://ru.wikipedia.org/wiki/Adobe_Photoshop (дата обращения 01.12.2023)
3. Figma [Электронный ресурс] — URL: https://www.figma.com/ (дата обращения 01.12.2023)

УДК 004.056.53

Отдельные вопросы мониторинга безопасности в IoT-сетях

Алтынбаев Артур Фларитович

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

***Аннотация**: В данной статье рассмотрены вопросы мониторинга в сетях Интернета вещей (IoT), сосредотачивая внимание на применении мониторинга для контроля процессов, происходящих внутри IoT-сетей. Проанализированы преимущества мониторинга сетей IoT по сравнению с традиционными методами контроля и рассмотрены, в частности, возможности использования систем мониторинга IoT для обеспечения безопасности данных в этих сетях. Кроме того, выделены проблемы и пути решения, связанные с мониторингом безопасности в IoT-сетях.*

***Abstract**: This paper discusses monitoring in Internet of Things (IoT) networks, focusing on the application of monitoring to control processes occurring within IoT networks. The advantages of monitoring IoT networks compared to traditional control methods are analyzed and the possibilities of using IoT monitoring systems to ensure data security in these networks are discussed. In addition, problems and solutions related to security monitoring in IoT networks are highlighted.*

***Ключевые слова**: мониторинг, IoT-сети, безопасность, несанкционированный доступ, данные, угрозы.*

***Keywords**: monitoring, IoT networks, security, unauthorized access, data, threats.*

Концепция «Интернет вещей» (или Internet of Things, сокращенно IoT) представляет собой идею о передаче данных между физическими объектами, оборудованными различными модулями для взаимодействия через сети передачи данных.

В области умных домов, включая системы безопасности, возникает ряд серьезных проблем с безопасностью. Статистика свидетельствует о том, что 65% устройств IoT имеют легко эксплуатируемые уязвимости. Для предотвращения использования этих уязвимостей предлагается внедрение концепции мониторинга сетей IoT.

Процесс мониторинга начинается с сбора данных из соответствующей сети, что позволяет контролировать удаленные устройства и оборудование. Все «умные» подключенные устройства объединяются для совместной работы, автоматизации и управления другим оборудованием с центра обработки данных.

Целью исследования является анализ вопросов мониторинга безопасности в IoT-сетях, определение путей решения проблемных вопросов, связанных с данным мониторингом.

Исследованием вопросов мониторинга безопасности в IoT-сетях занимались такие ученые как Д. В. Сахаров, А. М. Гельфанд, А. А. Казанцев, И. Е. Пестов и др.

Система мониторинга интернета вещей требует определенной функциональности для достижения высокой эффективности. Основные функции включают в себя сбор и обработку обширной информации о сети, а также оперативное оповещение и фильтрацию сигналов тревоги.

Мгновенное оповещение предполагает своевременное получение информативных уведомлений о важных изменениях статуса или условий для обеспечения правильной и быстрой реакции на потенциальные угрозы безопасности.

Имеется два основных метода сбора данных: «push-based» (на основе толчка) и опрос. Для систем мониторинга интернета вещей, метод «push-based» может быть более удобным, но необходимо учесть возможные компромиссы, связанные с протоколом связи.

Важно, чтобы протокол, используемый устройствами сети, обеспечивал эффективный сбор данных. Открытые протоколы также важны для

обеспечения совместимости между различными устройствами и обеспечения полной видимости сети.

Мониторинг безопасности Интернета вещей отличается от мониторинга общей ИТ-безопасности, требуя другого программного и аппаратного обеспечения, а также учитывая различные компоненты и протоколы связи, что делает подход к безопасности IoT устройств уникальным [1, с. 7].

Системы обнаружения вторжений (IDS) представляют собой распространенное решение для обеспечения мониторинга безопасности.

В мире быстро развивающихся технологий Интернета вещей (IoT) вопросы мониторинга безопасности становятся неотъемлемой частью обеспечения устойчивости и надежности сетей. IoT-устройства представляют собой широкий спектр умных устройств, взаимодействующих между собой и с окружающей средой для улучшения комфорта и эффективности. Однако с ростом количества подключенных устройств возрастает и потенциальная угроза для безопасности. Отдельные вопросы мониторинга в IoT-сетях охватывают несколько ключевых аспектов.

Первым из них является мгновенное обнаружение аномалий. Поскольку множество устройств IoT постоянно взаимодействуют друг с другом, важно иметь механизмы, способные оперативно выявлять необычные или подозрительные активности. Мгновенные оповещения и реакция на аномалии играют ключевую роль в предотвращении возможных угроз.

Другим важным аспектом является обеспечение целостности данных. Учитывая, что устройства IoT собирают и передают разнообразные данные, включая личную информацию, целостность этих данных становится первостепенной задачей. Эффективные механизмы мониторинга должны гарантировать, что данные не подвергаются вмешательству и сохраняют свою неприкосновенность.

Также стоит обратить внимание на аутентификацию и авторизацию устройств. Каждое устройство в IoT-сети должно быть четко идентифицировано, а его права доступа должны быть строго ограничены. Мониторинг безопасности должен включать в себя проверку подлинности устройств и контроль их прав доступа, чтобы предотвратить несанкционированный доступ.

Интеграция систем обнаружения вторжений (IDS) также является важным компонентом мониторинга безопасности в IoT-сетях. Эти системы способны выявлять необычные активности и атаки, предоставляя ценную информацию для предотвращения потенциальных угроз.

В целом, отдельные вопросы мониторинга безопасности в IoT-сетях требуют комплексного подхода, объединяя мгновенное обнаружение аномалий, обеспечение целостности данных, аутентификацию и авторизацию устройств, а также использование современных систем обнаружения вторжений. Эффективное решение этих вопросов содействует созданию устойчивых и безопасных сетей, способствуя развитию Интернета вещей в более надежном и защищенном направлении [2, с. 88].

Можно выделить следующие ключевые проблемы мониторинга безопасности в IoT-сетях и возможные пути их решения.

Первая проблема связана с мгновенным обнаружением аномалий. Множество взаимодействующих устройств создает сложную среду, в которой необычные активности могут оставаться незамеченными. Эффективный мониторинг должен обеспечивать мгновенное обнаружение подозрительных событий и оперативное реагирование. Это достигается внедрением систем, способных анализировать потоки данных в режиме реального времени и выявлять аномалии.

Второй важной проблемой является обеспечение целостности данных. Устройства IoT собирают и обмениваются разнообразной информацией, включая конфиденциальные данные. Гарантировать, что эти данные остаются неприкосновенными и не подвергаются вмешательству, можно с помощью применения криптографических методов и тщательного контроля целостности при передаче и хранении данных.

Третья проблема касается аутентификации и авторизации устройств. Каждое устройство в сети должно быть однозначно идентифицировано, а его права доступа должны строго соответствовать установленным политикам безопасности. Мониторинг должен включать в себя системы проверки подлинности и управления доступом, чтобы предотвратить несанкционированный доступ к сети.

Интеграция систем обнаружения вторжений (IDS) представляет собой еще один аспект решения проблем мониторинга безопасности в IoT-сетях.

IDS способны выявлять подозрительные паттерны и активности, предоставляя операторам информацию для предотвращения возможных угроз [3, с. 91].

Таким образом, одним из ключевых аспектов обеспечения безопасности в IoT-сетях является управление доступом. Регулирование прав доступа к устройствам и данным играет решающую роль в предотвращении несанкционированного доступа и потенциальных атак. Необходимость строгой аутентификации и авторизации в среде IoT подчеркивает важность тщательного мониторинга этих мер безопасности.

Еще одним аспектом, требующим внимания, является обеспечение конфиденциальности данных. Устройства IoT часто собирают и обрабатывают большое количество чувствительной информации. Эффективное шифрование данных на всех этапах их передачи и хранения является критическим моментом, который следует учитывать при разработке и эксплуатации устройств IoT.

Мониторинг целостности системы также становится неотъемлемым элементом обеспечения безопасности в IoT. Отслеживание необычных активностей, изменений в программном обеспечении и попыток вторжения требует постоянного внимания и анализа. Раннее обнаружение потенциальных угроз позволяет предпринимать меры до того, как возникнут серьезные последствия.

Кроме того, важно осознавать, что обеспечение безопасности в IoT — это постоянный процесс, требующий регулярного обновления и адаптации. С развитием технологий появляются новые угрозы, и, следовательно, необходимо постоянно совершенствовать стратегии мониторинга безопасности.

Список литературы

1. Котенко И. В. Архитектура системы параллельной обработки больших данных для мониторинга безопасности сетей Интернета вещей / И. В. Котенко, И. Б. Саенко, А. Г. Кушнеревич // Труды СПИИРАН.— 2018.— № 4, Вып. 59. — С. 5–30.
2. Сахаров Д. В. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //

Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России».— 2020.— № 2. — С. 86–94.

3. Соколов М. Н. Проблемы безопасности Интернет вещей: обзор / М. Н. Соколов К. А. Смолянинова, Н. А. Якушева // Вопросы кибербезопасности.— 2015.— № 5. — С. 85–96.
4. Гельфанд А. М. и др. Интернет вещей (IoT): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 215–220.
5. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика» РИ-2018».— 2018. — С. 149–149.
6. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 590–595.
7. Гельфанд А. М. и др. Области применения аналитики больших данных в критических информационных инфраструктурах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 438–440.
8. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //Proceedings of the 4th International Conference on Future Networks and Distributed Systems.— 2020. — С. 1–6.

УДК 336.76 (075.8)

Особенности анализа больших данных в информационных базах предприятий

Алтынбаев Артур Фларитович

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

***Аннотация**: Настоящее исследование посвящено анализу и характеристике особенностей анализа больших данных в информационных базах предприятий. В статье выделены проблемы и пути решения, связанные с анализом больших данных в информационных базах предприятий. Анализ больших данных в информационных базах предприятий представляет сложную задачу, требующую применения инновационных подходов. Также в статье представлены перспективы развития больших данных.*

***Abstract**: The present study is devoted to analyzing and characterizing the features of big data analysis in enterprise information bases. The paper highlights the problems and solutions related to big data analysis in enterprise information bases. Analyzing big data in enterprise information bases is a complex task that requires the use of innovative approaches. The article also presents the perspectives of big data development.*

***Ключевые слова**: большие данные, информация, предприятия, анализ, технологии.*

***Keywords**: big data, information, enterprises, analysis, technology.*

В нашу эпоху большие данные стали неотъемлемой частью успешного функционирования предприятий. Информационные базы, насыщенные огромным объемом данных, предоставляют бесценные инсайты и возможности для оптимизации бизнес-процессов. Однако анализ таких объемов информации требует специальных подходов и инструментов.

Одной из особенностей анализа больших данных в информационных базах предприятий является необходимость эффективного управления объемом информации. Сложность заключается не только в обработке огромного количества данных, но и в выделении значимой информации среди всего множества. Это требует применения специализированных ал-

горитмов и методов машинного обучения. Вышеуказанное и обусловило актуальность темы исследования.

Целью исследования является выявление особенностей анализа больших данных в информационных базах предприятий.

Вопросами анализа больших данных в информационных базах предприятий, занимались такие ученые как, Д. А. Струнин, Н. И. Касперская, И. Ф. Михалевич, Я. О. Фролов, В. Л. Сидоренко, С. И. Азаров и др.

Еще одной важной особенностью является обеспечение безопасности данных. Поскольку большие данные часто содержат чувствительную информацию, предприятия должны принимать меры для защиты от утечек и несанкционированного доступа. Это включает в себя использование современных технологий шифрования, контроля доступа и мониторинга активности пользователей.

Также важным аспектом анализа больших данных является необходимость интеграции данных из различных источников. Предприятия могут иметь информацию, распределенную по разным системам и форматам. Специализированные инструменты для интеграции данных позволяют создавать единый, цельный обзор всей доступной информации.

Существенную роль в анализе больших данных играют технологии облачных вычислений. Они позволяют предприятиям масштабировать свою вычислительную мощность по мере необходимости, избегая при этом значительных капитальных затрат на обновление инфраструктуры.

Понятие Big Data, согласно многим источникам, включая исследовательскую компанию IDC, обычно охватывает четыре основных аспекта, известных как «четыре V»: объем (Volume), разнообразие (Variety), скорость (Velocity) и ценность (Value). IDC предоставляет следующее определение для Big Data: «Это технологии и архитектуры нового поколения, предназначенные для эффективного извлечения ценности из данных большого объема различных форматов, достигаемое через быстрый захват, обработку и анализ».

Таким образом, Big Data представляет собой не только объем информации, но и ее разнообразие, требующее быстрого анализа для извлечения ценности. Это подразумевает использование новейших технологий и архитектур, спроектированных для эффективной обработки и анализа данных различных форматов.

Большие данные, или Big Data, представляют собой масштабные и сложные наборы данных, выходящие за пределы традиционных баз данных и стандартных методов анализа. Эти данные обладают тремя ключевыми характеристиками, известными как «три В»: объем (громадные объемы данных), разнообразие (различные типы данных, такие как тексты, изображения, видео, геоданные и т. д.) и скорость (быстрое поступление и передача данных) [1, с. 439].

Приведем пример из области электронной коммерции: магазины активно собирают информацию о каждом клиенте, включая их предпочтения, историю покупок, время, проведенное на сайте и многое другое. Хотя объем данных огромен, анализ этих данных может значительно улучшить понимание потребностей клиентов и позволить компаниям более гибко адаптировать свои предложения.

Анализ больших данных в информационных базах предприятий представляет собой важное направление, ставшее ключевым фактором для успешного управления и развития бизнеса. Однако с этим подходом возникают различные проблемы, требующие внимательного рассмотрения и поиска эффективных путей их решения.

Одной из основных проблем является объем данных. В современном бизнесе информационные базы предприятий накапливают огромные объемы данных, и их анализ становится сложной задачей. Для решения этой проблемы необходимо использовать специализированные инструменты и технологии, способные эффективно обрабатывать большие объемы данных и выделять из них значимую информацию.

Еще одной проблемой является разнообразие данных. Информация в информационных базах может представляться в различных форматах, включая текст, изображения, видео и другие. Это требует разработки методов анализа, способных обрабатывать и объединять данные различных типов, чтобы создать полный и целостный обзор.

Следующей важной проблемой является скорость обработки данных. Современный бизнес требует мгновенных решений на основе актуальной информации. Поэтому необходимо использовать технологии, способные обеспечивать быстрый сбор, обработку и анализ данных для оперативного принятия решений [2, с. 127].

Безопасность данных также стоит перед вызовом в контексте анализа больших данных. С увеличением объема информации растет и риск утечек или несанкционированного доступа. Использование современных методов шифрования и систем контроля доступа помогает минимизировать этот риск.

Решение проблем анализа больших данных в информационных базах предприятий требует комплексного подхода, включающего в себя технологические инновации, разработку эффективных методов анализа и стратегии обеспечения безопасности информации. Внимательное рассмотрение этих аспектов открывает новые возможности для оптимизации бизнес-процессов и принятия обоснованных решений.

Big Data имеют потенциал стать сильным инструментом диалога между государством и бизнесом, обеспечивая всестороннее их внедрение. Для ускорения этого процесса важны следующие факторы:

1. Доверие к облачным хранилищам. Улучшение механизмов безопасности и прозрачности в облачных хранилищах способствует увеличению доверия и, следовательно, ускоряет внедрение Big Data.
2. Стабильность экономики. Экономическая стабильность является важным фактором, создающим благоприятные условия для внедрения инновационных технологий, таких как анализ больших данных.
3. Наличие квалифицированных кадров: Обученные специалисты способны эффективно работать с данными, что является ключевым фактором для успешного анализа больших данных.
4. Открытость компаний. Большая открытость и готовность компаний к сотрудничеству в области обмена данных способствует развитию Big Data.

Компании, успешно управляющие данными и процессами их жизненного цикла, будут основными выигрывающими от внедрения Big Data.

Однако анализ больших данных сталкивается с рядом проблем:

- Разнородность данных. Необходимость анализа разнообразных форматов данных требует разработки универсальных методов обработки.
- Накопление шума. Избыточная информация и параметры оценки могут создать шум, затрудняющий точный анализ [3, с. 41].

- Ложная корреляция. Неправильные выводы могут возникнуть из-за ложных корреляций, что подчеркивает важность точности в анализе данных.
- Случайная эндогенность. Высокая размерность данных может привести к случайной эндогенности, что также требует особого внимания.

Сценарии развития Big Data могут варьироваться:

1. Пессимистичный. Ограничения на использование данных приводят к низкому вкладу в ВВП и ограниченному росту.
2. Бездействия. Существующие ограничения поддерживают низкий, но стабильный рост.
3. Базовый. Упрощенный доступ и обработка, средний прирост и значительный вклад в ВВП.
4. Оптимистичный. Обмен данными, инновации и финансовая поддержка приводят к высокому приросту и существенному увеличению вклада в экономику.
5. Сверхоптимистичный. Крупномасштабный обмен данными, государственная поддержка и значительный экономический рост.

Анализ и решение указанных проблем в сочетании с правильными стратегиями развития могут максимизировать потенциал Big Data в различных областях бизнеса и государственного управления [4, с. 9].

Таким образом, особенности анализа больших данных в информационных базах предприятий подчеркивают сложность и важность этого процесса в контексте современного бизнеса. Профессиональное владение этим инструментом становится ключевым фактором для успешного управления и принятия обоснованных решений.

Первой значимой особенностью является объем данных, который в современных информационных базах предприятий может достигать колоссальных масштабов. Обработка и анализ такого объема требует не только высокотехнологичных инструментов, но и гибких стратегий, способных эффективно справляться с множеством переменных.

Другой важной особенностью является разнообразие данных. В информационных базах предприятий накапливаются информация различных типов — тексты, изображения, видео, геоданные и другие. Это требует

от аналитиков умения обрабатывать и анализировать множество форматов, создавая единый взгляд на информацию.

Список литературы

1. Гельфанд А. М. Области применения аналитики больших данных в критических информационных инфраструктурах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 438–440.
2. Ильяшенко О. Ю. Роль BI–систем в совершенствовании процессов обработки и анализа бизнес информации: учебник / И. В. Ильин, Д. Д. Болобонов. — Наука и бизнес: пути развития, № 6, 2017.— 124–131 с.
3. Соловьев В. В. Улучшение защищенности распределенной информационной системы персональных данных на основе технологии VPN и терминального доступа / В. В. Соловьев // Информационные технологии и проблемы математического моделирования сложных систем.— 2017.— № 18. — С. 39–44.
4. Струнин Д. А. Бизнес-аналитика и большие данные / Д. А. Струнин // Молодой ученый.— 2023.— № 32 (479). — С. 8–10.
5. Гельфанд А. М. и др. Интернет вещей (IoT): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 215–220.
6. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика» РИ-2018».— 2018. — С. 149–149.
7. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 590–595.
8. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России».— 2020.— № . 2. — С. 86–94.

9. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //Proceedings of the 4th International Conference on Future Networks and Distributed Systems.— 2020. — С. 1–6.

УДК 004.7

Некоторые аспекты построения корпоративного Security Operations Center

Алтынбаев Артур Фларитович

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

***Аннотация**: Настоящее исследование посвящено выявлению отдельных аспектов построения корпоративного Security Operations Center. Также в статье представлены меры, необходимые для обеспечения эффективной работы будущего SOC. Кроме того, выделены проблемы и пути решения, связанные с построением корпоративного Security Operations Center. Данное исследование подчеркивает важность масштабирования инфраструктуры SOC для улучшения отказоустойчивости, обработки данных и эффективного выявления угроз.*

***Abstract**: This study focuses on identifying certain aspects of building an enterprise Security Operations Center. Also, the paper presents the measures necessary to ensure the effective operation of the future SOC. In addition, the challenges and solutions associated with building an enterprise Security Operations Center are highlighted. This study emphasizes the importance of scaling the SOC infrastructure to improve fault tolerance, data processing, and effective threat detection.*

***Ключевые слова**: Security Operations Center, реагирование, аспекты, технологии, информация, информационные системы.*

***Keywords**: Security Operations Center, aspects, response, technologies, information, information systems.*

Мировые эксперты единодушно подчеркивают, что эффективное управление ИТ-активами требует постоянного и внимательного мони-

торинга. Это не только снижает риски киберугроз, но и обеспечивает оперативную реакцию на возможные взломы с последующими мерами по минимизации ущерба. Внедрение методов работы Security Operation Center (SOC) является наиболее результативным подходом в данном контексте.

При разработке плана развития системы информационной безопасности (ИБ), организации должны учесть несколько ключевых факторов, оказывающих существенное влияние на эффективность будущего SOC. Среди этих факторов выделяются:

1. Экспертиза и квалификация группы реагирования. Наличие квалифицированных специалистов в группе реагирования становится фундаментальным элементом успешной работы SOC. Их опыт и умения напрямую влияют на скорость и эффективность реагирования на потенциальные угрозы.
2. Технологии обнаружения компьютерных атак и обработки больших потоков информации. Использование передовых технологий в обнаружении атак и обработке больших объемов данных становится неотъемлемой частью современных SOC. Эффективные средства мониторинга и анализа данных позволяют выявлять угрозы на ранних этапах и предотвращать их распространение.
3. Практики и процессы реагирования. Разработка четких и эффективных практик и процессов реагирования помогает оптимизировать действия SOC. Это включает в себя быструю и координированную реакцию на инциденты, а также систематический анализ прошлых случаев для улучшения стратегий и тактик в будущем.

Целью исследования является выявление отдельных аспектов построения корпоративного Security Operations Center.

Эффективная работа Security Operation Center (SOC) сильно зависит от грамотного выбора технологий. При планировании создания SOC необходимо предвидеть долгосрочные результаты и четко определить цели, которых следует достичь. Процесс начинается с разработки концепции, где должны быть четко сформулированы цели, задачи, этапы развития и требуемый уровень достижения [1, с. 592].

Важным этапом в концепции является определение функций, которые будут реализовываться на технологическом уровне. Эти функции включают:

- Инвентаризацию ИТ-активов и обновление информации. Гарантирует наличие актуальных данных обо всех информационных активах.
- Анализ уязвимостей и их управление. Обеспечивает постоянный контроль за уязвимостями и их своевременное устранение.
- Обработку событий безопасности и их корреляцию. Анализирует и связывает события для выявления потенциальных угроз.
- Анализ сетевого трафика и файлов на вредоносную активность. Выполняет мониторинг сетевой активности и файлов на предмет вредоносных действий.
- Поведенческий анализ файлов. Идентифицирует необычное поведение файлов для выявления потенциальных угроз.
- Анализ действий пользователей. Оценивает активность пользователей с целью выявления подозрительных действий.
- Резервирование данных. Обеспечивает возможность восстановления данных в случае повреждения или шифрования.
- Обработку информации об инцидентах. Включает обогащение данных о инцидентах и анализ актуальных угроз.
- Проверку устойчивости ресурсов к внешним воздействиям. Проводит тесты на проникновение для обеспечения надежности информационных систем.

Не менее важно предусмотреть масштабирование ИТ-инфраструктуры SOC, учитывая увеличение объемов хранения данных, повышение отказоустойчивости и ускорение обработки данных. В случае распределенной системы SOC необходимо также оценить пропускную способность коммуникаций до удаленных площадок и рассмотреть варианты их расширения. Это обеспечит гибкость и эффективность SOC в долгосрочной перспективе.

В настоящее время большинство стандартных Security Operation Center ориентированы на обнаружение атак в реальном времени, но часто не учитывают новые методы и тактики злоумышленников, что делает сложным выявление атак в момент их осуществления. Поэтому важно развивать

навыки работы с индикаторами компрометации и другими признаками угроз, которые необходимо включать в анализ прошлых событий для выявления проникновений и закрепления в ИТ-инфраструктуре [2, с. 47].

Для обеспечения эффективной работы будущего SOC рекомендуется предпринять следующие меры заранее:

1. Настройка парольных политик. Установка надежных паролей и регулярное их обновление являются первым шагом к повышению безопасности.
2. Внедрение двухфакторной аутентификации. Дополнительный слой защиты через двухфакторную аутентификацию существенно укрепляет систему.
3. Минимизация привилегий и доступов. Ограничение привилегий и доступов помогает предотвратить распространение угроз в случае компрометации.
4. Настройка контроля конфигураций. Регулярный мониторинг и обновление конфигураций снижают риски нарушений безопасности.
5. Организация резервного копирования. Регулярные резервные копии обеспечивают возможность быстрого восстановления после инцидентов.
6. Сегментация сети с использованием межсетевых экранов. Разделение сети на сегменты с помощью межсетевых экранов помогает контролировать трафик и минимизировать распространение атак внутри сети.

Развивая компетенции в области ретроспективного анализа и предпринимая проактивные шаги по укреплению базовой безопасности, будущее SOC сможет эффективно справляться с вызовами современной кибербезопасности.

Создание Security Operation Center (SOC) представляет собой сложную задачу, успешное решение которой часто затрудняется из-за типичных ошибок и просчетов:

- Недостаточный уровень зрелости системы ИБ. Обеспечение адекватной защиты информации требует соответствующего уровня зрелости системы информационной безопасности в организации. Проблема часто заключается в использовании только базовых средств защиты, что делает создание SOC преждевременным.
- Небольшая команда. SOC — это не только технические средства, но и команда для выполнения аналитических функций и работы первой

линии. Размер команды SOC играет ключевую роль в обеспечении эффективности оперативных мероприятий.

- Неверное толкование SOC. Часто SOC путают с системами типа Security Information and Event Management (SIEM). Такие системы способны лишь выявлять инциденты и предоставлять базовую информацию для расследования, в то время как функции SOC охватывают более широкий спектр задач.

Решение этих проблем важно для эффективного внедрения SOC и обеспечения комплексной безопасности информационной среды. Важно правильно оценивать готовность и потребности организации, предварительно подготавливая необходимые ресурсы и команду для успешной работы SOC [3].

Таким образом, современный ИТ-ландшафт стремительно развивается, при этом объем событий в области информационных и защитных систем растет соответственно. В большинстве организаций сложно человеку самостоятельно анализировать этот поток событий и выделять важную информацию. Оперативное выявление и быстрая реакция на инциденты играют ключевую роль в современной безопасности. Здесь на помощь приходит Security Operation Center (SOC), автоматизируя процессы реагирования на инциденты ИБ. Таким образом, SOC становится неотъемлемой частью эффективной операционной структуры организации, способной эффективно выполнять разнообразные задачи в области информационной безопасности, такие как мониторинг и анализ событий, реагирование на инциденты, threat hunting и многое другое.

Список литературы

1. Казанцев А. А. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 590–595.
2. Лисецкий Ю.М., Бобров С. И. Новые угрозы информационной безопасности или оружие массового заражения // Машины и системы.— 2018.— № 1. — С. 41–50.

3. Muniz J., McIntyre G., Al Fardan N. Security Operations Center: Building, Operating, and Maintaining your SOC // Cisco Press. Nov 2, 2015. URL: http://www.ciscopress.com/store/security-operations-center-building-operating-and-maintaining-9780134052076 (дата обращения: 24.11.2023).
4. Гельфанд А. М. и др. Интернет вещей (IoT): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 215–220.
5. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика» РИ-2018».— 2018. — С. 149–149.
6. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России».— 2020.— № . 2. — С. 86–94.
7. Гельфанд А. М. и др. Области применения аналитики больших данных в критических информационных инфраструктурах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 438–440.
8. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //Proceedings of the 4th International Conference on Future Networks and Distributed Systems.— 2020. — С. 1–6.

УДК *004.056.57*

Угрозы кибербезопасности в 2023 году: анализ проблем и возможностей

Токарев Евгений Валерьевич

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

***Аннотация**: Статья посвящена анализу актуальных киберугроз 2023 года, а также рассмотрению проблем, вызываемых ими и возможностей их пресечения. Оценки основаны на анализе, синтезе и обобщении зарубежных и российских статистических данных, результатов официальных и журналистских расследований, мнений авторитетных экспертов в области кибербезопасности. Данные собраны за первые три квартала 2023 года.*

***Abstract**: The article is devoted to analyzing the current cyber threats of 2023, as well as to considering the problems caused by them and the possibilities of their suppression. The assessments are based on the analysis, synthesis and generalization of foreign and Russian statistical data, results of official and journalistic investigations, and opinions of authoritative cybersecurity experts. The data is collected for the first three quarters of 2023.*

***Ключевые слова**: кибербезопасность, кибератаки, киберугрозы, киберпространство, киберпреступность.*

***Keywords**: cybersecurity, cyberattacks, cyberthreats, cyberspace, cybercrime.*

В сфере изучения кибербезопасности и противодействия киберпреступности представляется особо важным исследовать и тщательно анализировать киберугрозы прошедшего года, чтобы прогнозировать возможные направления активации действий киберпреступников в будущем, вырабатывая эффективные меры пресечения их намерений. Текущий год ещё не закончился, однако об общих тенденциях и трендах возникновения киберугроз в 2023 году на данный момент уже можно сделать некоторые выводы. Также мы имеем возможность опираться на полугодичные и поквартальные исследования и аналитические статьи экспертов в вопросах информационной безопасности [5].

Рассмотрим, какие актуальные угрозы в области кибербезопасности выделяли эксперты в течение 2023 года и обозначим основные проблемы, с которыми столкнулись из-за действий киберпреступников организации и частные пользователи, а также оценим возможности противодействия киберпреступникам.

В первую очередь, необходимо отметить, что киберугрозы для организаций и частных пользователей нельзя назвать однородными. Так, например, для частных пользователей основной угрозой остаётся использование киберпреступниками методов социальной инженерии (92% атак), в то время как для кибератак на организации она применяется лишь в 37% случаев [5]. В связи с этим представляется необходимым отмечать, на кого ориентированы рассматриваемы инструменты киберпреступной деятельности.

Методы социальной инженерии в 2023 году продолжают оставаться главной киберугрозой для частных лиц, причём можно отметить, что если значительно эволюционируют и развиваются инструменты киберпреступных схем с применением социальной инженерии, то каналы стабильно используются практически те же, что и несколько лет назад. Одним из самых популярных каналов по-прежнему остаётся электронная почта, где киберпреступниками рассылаются фишинговые письма. Тематика писем может быть разной: чаще всего это предложения о трудоустройстве с якобы ссылками на вакансии, заманчивые обещания лёгкого и быстрого заработка, якобы рекламные предложения от известных сервисов и компаний, для активации которых нужно перейти по ссылке, поддельные сообщения от служб доставки, извещающие о том, что вам была отправлена посылка. Также в 2023 году киберпреступники стали активно прибегать к эксплуатации горячей политической тематики, отправляя сообщения со срочными новостями о военных действиях и политических решениях высшего руководства государств [3].

Для обмана частных лиц также активно используется рассылка фишинговых писем в социальных сетях и мессенджерах, создание фишинговых сайтов, имитирующих сайты известных сервисов, онлайн-платформ и компаний. Не теряют популярность и телефонные звонки как один из каналов мошенничества. Обычно целью телефонных мошенников является кража персональных и банковских данных для хищения финансовых средств.

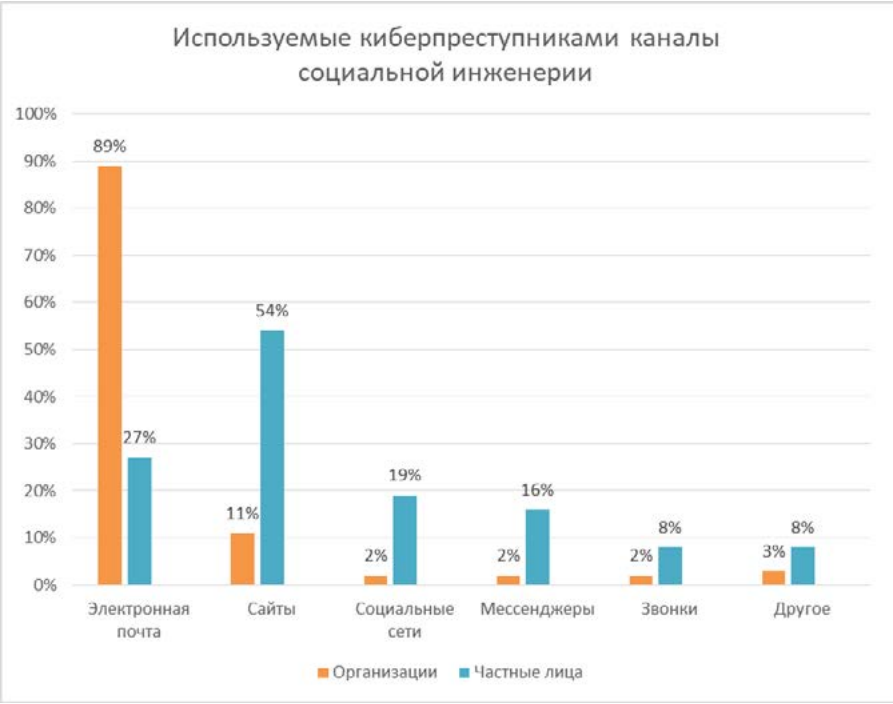

Рисунок 1. **Используемые киберпреступниками каналы социальной инженерии**

Исследователи киберпреступности методами социальной инженерии отмечают новый тренд, появившийся в 2023 году — персонализация фишинговых рассылок в организации таким образом, чтобы жертвами кибермошенничества становились или высшие руководители, или те сотрудники, которые имеют доступ к распоряжению финансовыми средствами, либо обладают какой-либо важной конфиденциальной информацией [1]. Таким образом, кибератаки на организации становятся более изощрёнными, приобретают индивидуальный характер. Известны случаи, когда киберпреступники заранее проводили своеобразную разведку интересов тех руководителей и сотрудников, которым собирались послать письма с фишинговыми ссылками по электронной почте, для того чтобы верно определиться с их тематикой, чтобы жертвы точно открыли их [1].

Ещё одним инструментом фишинга с использованием каналов социальной инженерии, получившим значительную популярность в 2023 году, стало применение PDF-файлов для реализации возможностей скрытого фишинга. Многие пользователи уже знают, что не стоит открывать подозрительные ссылки, поэтому обмануть их таким образом становится всё труднее, кроме того, сервисы электронных почт сами стараются активно бороться с такими рассылками. По этим причинам киберпреступники стали переходить на отправку скрытых фишинговых вложений, маскируя их под обычные PDF-файлы. В третьем квартале текущего года фишинг через PDF-файлы впервые вышел на стабильно лидирующую позицию для распространения вредоносных ссылок [3]. Также для того, чтобы обходить успешно защиту электронной почты, киберпреступники стали маскировать фишинговые ссылки с помощью QR-кодов, встраиваемых в PDF-файлы, а также вставлять текстовые документы Word внутрь PDF-вложений [3]. Последняя схема рассчитана на то, что пользователь откроет вложение, но из-за наличия в нём содержания Word-формата произойдёт открытие в текстовом редакторе, а не в программах для просмотра PDF-файлов.

Новшеством в 2023 году стали многоступенчатые и длительные пути применения методов социальной инженерии для хищения персональных данных пользователей и/или отправления им вредоносных ссылок и программ. Суть их состоит в том, чтобы сначала внушить доверие жертве киберпреступления, убедив в её безопасности взаимодействия. Например, пользователь получает несколько раз по электронной почте или в социальных сетях рекламное предложение от сервиса бронирования отелей, продажи билетов и т.п. в виде рекламного буклета в формате PDF. Для создания эффекта достоверности используются реальные предложения настоящих компаний. И только в 3–4 раз пользователь получает буклет со встроенной в него скрытой фишинговой ссылкой. В социальных сетях и мессенджерах могут для этого использоваться переписки с фейковых аккаунтов. Наиболее сложные виды подобного кибермошенничества заключаются в противодействии даже возможным попыткам жертвы раскрыть обман. К примеру, известны случаи, когда киберпреступники не только создавали поддельные приложения настоящих сервисов для распростра-

нения вредоносных программ, но и с их помощью собирали данные пользователей и перенаправляли звонки тех в колл-центры банков и служб техподдержки компаний к себе, когда те замечали подозрительные списания средств у себя в приложениях. Далее они убеждали звонивших, что средства вскоре вернутся, а иногда им удавалось выманить у жертв ещё больше денег и узнать ещё какие-либо персональные данные [2].

Актуальным трендом 2023 года стало применение нейросетей для совершения киберпреступлений. Злоумышленники могут использовать их по-разному, в зависимости от необходимости в конкретной ситуации. Благодаря применению нейросетей составляются тексты для рассылок фишинговых писем, создаются дипфейки, имитируются диалоги в соцсетях и мессенджерах. Более того, киберпреступниками была создана даже специальная нейросеть для автоматизации написания фишинговых рассылок — WormGPT [4].

Помимо кибератак с использованием методов социальной инженерии актуальны атаки на системы передачи данных, от которых чаще всего страдают пользователи файлообменников. Злоумышленники ищут уязвимости в системах передачи данных, которые можно обойти и добавляют в файлы вредоносное ПО. Хотя основным каналом для распространения вредоносных программ по-прежнему остаётся электронная почта, системы передачи данных становятся всё более частой мишенью для кибератак, направленных не только на частные лица, но и на организации.

В 2023 году в ряде кибератак использовались виртуальные машины для обхода систем защиты. Суть этого метода состоит в том, что запускается другая операционная система под видом обычной операционной. Опасность данного метода состоит в том, что производимую таким образом кибератаку достаточно сложно заметить до того момента, пока не станут очевидными вредоносные последствия [5].

Число использований шифровальщиков для кибератак при этом снижается, что эксперты связывают с распространением дешифраторов [5]. Тем не менее, они до сих пор представляют серьёзную угрозу, особенно для компаний развивающихся стран и частных пользователей.

Стоит отметить, что данные, предоставляемые как организациями, так и частными лицами нельзя назвать абсолютно точными, они являются

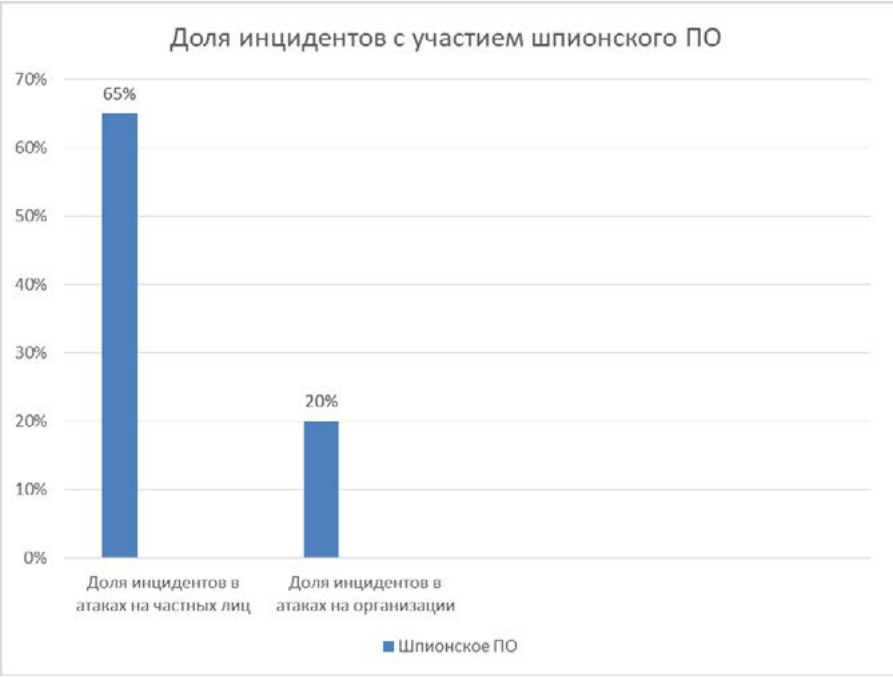

Рисунок 2. **Доля инцидентов с участием шпионского ПО в атаках на частных лиц и организации**

примерными в силу того, что удачные кибератаки зачастую становятся ударами по репутации, могут помешать реализации карьерных и бизнес-планов. Тем не менее, опираясь на имеющиеся сведения, собранные разными исследовательскими группами, можно констатировать, что киберпреступники в 2023 году сохраняют прежние основные каналы для распространения вредоносного ПО, при этом активно развивая отдельные инструменты и технологии. Это свидетельствует о том, что злоумышленникам приходится постоянно усложняться из-за совершенствующейся защиты от киберугроз и роста информированности пользователей. Однако пока сложно оценить, какие механизма противодействия могут выработать социальные сети и почтовые сервисы для борьбы с мошенничествами с использованием нейросетей. Пока в этом вопросе остаётся полагаться,

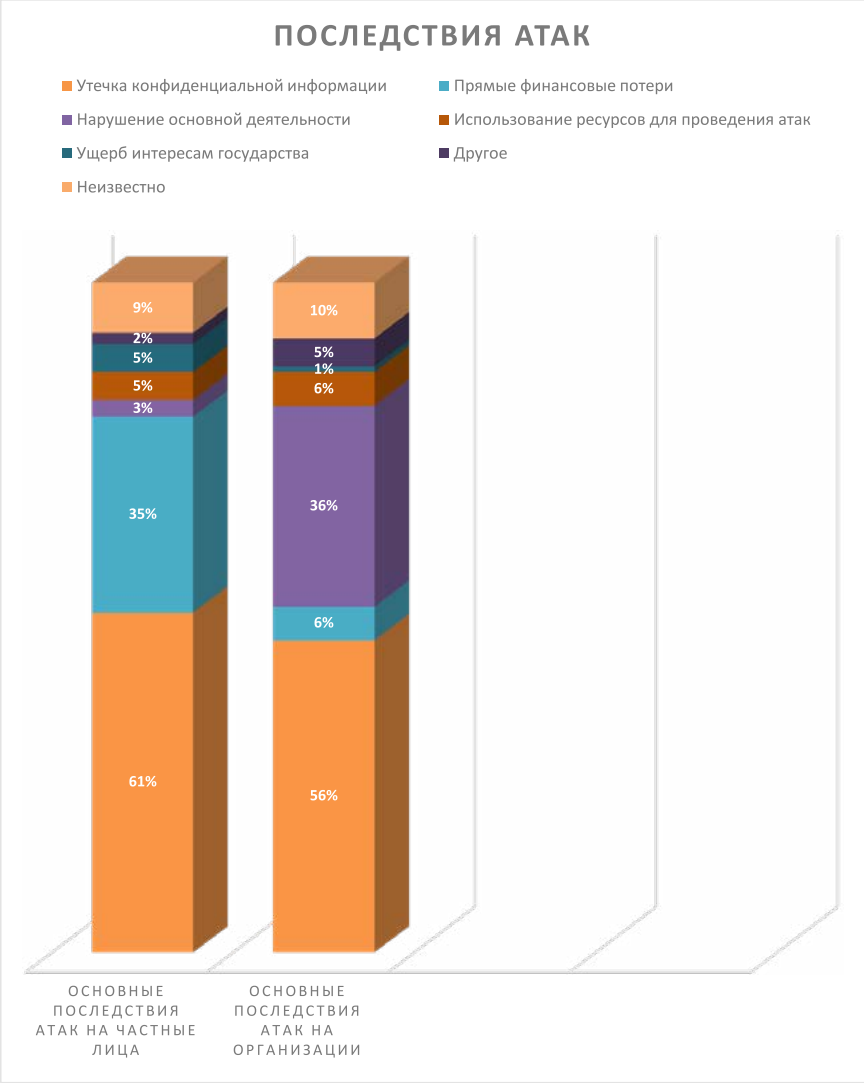

Рисунок 3. **Основные последствия кибератак для организаций и частных лиц**

в первую очередь, на внимательность и информированность самой пользовательской аудитории.

Список литературы

1. Behind the Scenes of a Tailor-Made Massive Phishing Campaign. [Imperva] URL: https://www.imperva.com/blog/analysis-of-a-phishing-campaign/ (date accessed: 21.11.2023).
2. Letscall — new sophisticated Vishing toolset. [Threat Fabric] URL: https://www.threatfabric.com/blogs/letscall-new-sophisticated-vishing-toolset (date accessed: 21.11.2023).
3. VIPRE Security Group's Q3 2023 Email Threat Report Reveals PDFs, Callback Phishing and Malware Via Google Drive Growing in Popularity Among Criminals. [VIPRE Security Group] URL: https://vipre.com/resources/press-releases/vipre-releases-q3–2023-email-threat-trends-report/
4. WormGPT: New AI Tool Allows Cybercriminals to Launch Sophisticated Cyber Attacks. [The Hacker News] URL: https://thehackernews.com/2023/07/wormgpt-new-ai-tool-allows.html (date accessed: 21.11.2023).
5. Актуальные киберугрозы: III квартал 2023 года. [Positive technologies] URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3/ (date accessed: 21.11.2023).
6. Цветков А. Ю., Шалаева М. Е., Юрченко М. А. Обеспечение безопасности в клиент-серверном Java приложении для учета и автоматической проверки лабораторных работ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 756–761.
7. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2020.— № . 2. — С. 50–56.
8. 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.
9. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности ком-

пьютерных сетей //Региональная информатика» РИ-2018».— 2018. — С. 149–149.
10. Гельфанд А. М. и др. Области применения аналитики больших данных в критических информационных инфраструктурах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 438–440.

УДК 004.056.57

Продажа личных данных в даркнете: актуальная киберугроза

Токарев Евгений Валерьевич

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

***Аннотация**: Статья посвящена анализу рынка продажи личных данных в даркнете в 2023 году. В статье представлены виды самых актуальных данных для продажи, а также перечислены некоторые популярные способы завладения личными данными и пути противодействия им. Оценки основаны на анализе, синтезе и обобщении зарубежных и российских статистических данных, результатов официальных и журналистских расследований, мнений авторитетных экспертов в области кибербезопасности.*

***Abstract**: The article is devoted to analyzing the market for the sale of personal data on the darknet in 2023. The article presents the types of the most relevant data for sale, and lists some popular ways to get hold of personal data and ways to counter them. Estimates are based on analysis, synthesis and generalization of foreign and Russian statistical data, results of official and journalistic investigations, and opinions of authoritative experts in the field of cybersecurity.*

***Ключевые слова**: кибербезопасность, киберугрозы, киберпространство, киберпреступность, даркнет, дарквеб, личные данные.*

***Keywords**: cybersecurity, cyberthreats, cyberspace, cybercrime, darknet, dark web; personal data.*

В настоящее время трудно представить жизнь человека без использования Интернета. Развлекательные сервисы, мессенджеры, социальные сети,

маркетплейсы, онлайн-игры, мобильные приложения, электронные библиотеки — всё это уже достаточно давно является привычной частью ежедневного быта современного человека. Рабочие и образовательные процессы в современном мире также неразрывно связаны с использованием Интернета. Однако до сих пор далеко не все рядовые пользователи соблюдают какие-либо меры безопасности для того, чтобы избежать хищения своих личных данных. При этом многие сервисы и сайты вполне легально собирают определённые данные, чтобы анализировать свою аудиторию и её потребности — это всё представляет собой необходимую часть подготовки большинства маркетинговых исследований. Прежде чем говорить о нелегальной продаже персональных данных, необходимо разобраться, что мы относим к ним и какие методы сбора данных о пользователях являются легальными, а какие — нет.

Существуют разные нормативно-правовые документы, которые определяют в различных странах, что относится в соответствии с местным законодательством к персональным данным человека, однако существуют некоторые общие аспекты определения персональных данных, которые едины для правовых систем большинства стран [6]. Исходя из них, к персональным данным человека относятся те виды информации, которые могут быть использованы для того, чтобы установить (идентифицировать) его личность (например, номер паспорта, биометрические данные, а также те данные, которые в сочетании с какой-либо другой личной или связанной с личностью информацией дают привязку к конкретному лицу, к примеру, дата и место рождения) [4]. В Российской Федерации правила сбора и использования персональных данных регулируются Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» [8], положения которого представлены на рисунке 1.

Хотя в России, как и в большинстве других стран, существует законодательная ответственность за хищение и использование чужих персональных данных, эксперты отмечают, что год от года объём мошеннических и иных преступных действий, совершаемых с личной информацией людей, стабильно растёт [7] и нет никаких причин полагать, что в ближайшее время ситуация каким-то образом сможет улучшиться [5]. Кроме того, каждый год возникают новые виды мошеннических манипуляций в киберпро-

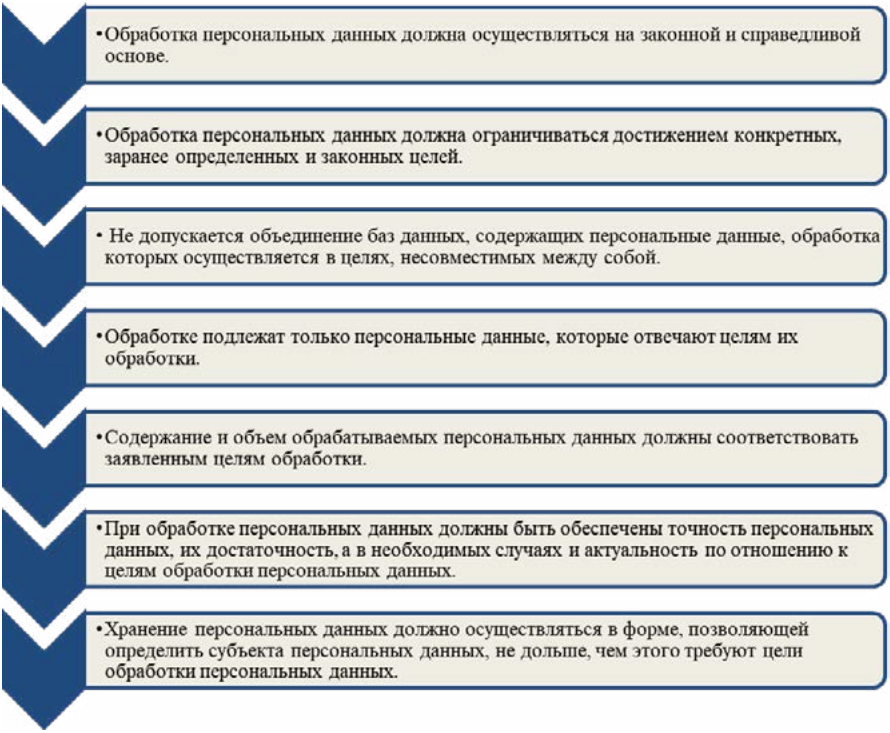

Рисунок 1. **Принципы обработки персональных данных в соответствии с законодательством РФ**

странстве, на которые не успевают оперативно реагировать представители правоохранительных органов, а большинство обычных пользователей Интернета даже не проинформированы об их возникновении и сути существования [3]. Также экспертное сообщество в сфере кибербезопасности отмечает, что в даркнете на сегодняшний день сформирован целый рынок торговли личными данными, а цены на покупку персональных данных снижаются, что делает их всё более доступными для злоумышленников [1].

Рассмотрим, какие виды личных данных являются наиболее популярными для продажи в дарквебе в 2023 году.

Первая категория — это данные, связанные с финансовыми системами, банковскими сервисами и другими подобными системами, связанными

с проведением платежей. Хищение этих данных позволяет злоумышленникам получать доступ к банковским вкладам, платёжным счетам и т.п., даёт возможность незаконно завладеть чужими денежными средствами. В 2023 году в этой категории в дарквебе наибольшей популярностью пользовались выставленные на продажу данные кредитных карт, взломанные доступы к аккаунтам платёжных сервисов и доступы к криптокошелькам. Исследователи из группы «Privacy Affairs» [1] приводят следующие цифры средней стоимости подобных данных в даркнете (рисунок 2).

Вторая категория личных данных, весьма популярная в даркнете для покупки и продажи — это взломанные аккаунты социальных сетей. Как правило, чем больше в аккаунте друзей и подписчиков, тем выше его цена. Кроме того, аккаунты из более популярных соцсетей («для всех») стоят дороже, чем из узкоспециализированных. Также чрезвычайно популярна услуга взлома аккаунта «под ключ», когда заказчик обращается с просьбой взломать чей-либо конкретный аккаунт. Зачастую такие взломы «под ключ» бывают вызваны не только желанием получения финансовой выгоды, но и мотивами личной мести, промышленного шпионажа, ревности и т.п. Дороже всего оцениваются взломы аккаунтов Gmail — в среднем их взлом стоит около 60$. Взломы аккаунтов других популярных социальных сетей и мессенджеров стоят в среднем от 20$ до 30$. Дешевле всего стоит взломать аккаунты в «Pinterest», «Spotify», «Soundcloud», где практически не публикуется какая-либо текстовая информация, не ведутся переписки и у рядовых пользователей практически никогда нет подписчиков (до 10$).

Третья категория — это взлом аккаунтов различных развлекательных и иных сервисов (например, сервисов по поиску жилья, вызову такси, заказу товаров на маркет-плейсах). Так, дороже всего могут стоить взломы и доступы верифицированных аккаунтов по поиску жилья типа AirBNB.com (стоимость их взломов может доходить до 300$). Взломы доступов к годовым платным подпискам развлекательных сервисов и стриминговых платформ (таких, как «Netflix», «Spotify») обычно стоят от 10 до 30$.

Ещё одна категория товаров в дарквебе, в основе которой лежит использование чужих персональных данных — это поддельные документы (как сканы, так и бумажные). Сканы стоят значительно дешевле бумажных поддельных документов для идентификации личности, при этом далеко не все

Данные кредитных карт	Данные кредитной карты, баланс счёта до 5000$ ($110).
	Взломанный аккаунт Card.com ($75).
	Данные кредитной карты, баланс счёта до 1000$ ($70).
	Кража доступов онлайн-банков, баланс счёта минимум 2000$ ($60).
	Кража доступов онлайн-банков, баланс счёта минимум 100$ ($40).
	Копия карты Mastercard с PIN ($20).
	Копия карты VISA с PIN ($20).
Взлом аккаунтов платёжных сервисов	Данные банковского счета ING bank (провереннный счёт) ($4,255).
	HSBC UK Бизнес-аккаунт ($4,200).
	Switzerland, вход в учётную запись ($2,200).
	Revolut, верифицированный аккаунт (UK, USA) ($1,600).
	Верифицированный аккаунт Stripe с платёжным шлюзом ($1,200).
	Верифицированный аккаунт Cashapp ($860).
	TransferGo, вход в учётную запись ($500).
	50 аккаунтов PayPal ($120).
	PerfectMoney, вход в учетную запись ($100).
	Western Union, вход в учётную запись ($39).
Криптоаккаунты	Wirex, верифицированный и взломанный аккаунт ($2,300).
	Zen.com, верифицированный аккаунт ($1,600).
	Binance, верифицированный аккаунт ($410).
	Xcoins, верифицированный аккаунт ($350).
	Bit2me верифицированный аккаунт ($150).
	Blockchain.com, верифицированный аккаунт ($85).
	Paxful.com, верифицированный аккаунт 1 уровня ($20).

Рисунок 2. **Расценки в дарквебе на покупку данных кредитных карт, доступов к аккаунтам платёжных сервисов и криптокошелькам в 2023 году**

документы получится подделать. Например, скан паспорта РФ реально существующего паспорта РФ можно купить в среднем за 80$. Злоумышленники могут использовать его для того, чтобы оформить взятие денежных средств в онлайн-микрозаймах. Однако сделать офлайн-паспорт РФ на

несуществующую личность не представляется возможным, так как это не имеет особого смысла (даже при высоком качестве подделки будет быстро установлено, что паспорта с таким номером и серией не существует, либо что он выдавался другому лицу). Следовательно, злоумышленники должны использовать полные данные настоящего, реально существующего паспорта.

Наконец, существует такая услуга как «пробив личности» какого-либо человека, особой популярностью она пользуется на постсоветском пространстве. Суть её состоит в том, чтобы установить личность человека, пользуясь какой-либо уже известной информацией, а также иногда включает в себя установление возможного местоположения интересующего лица. В 2022 и 2023 году в РФ были прецеденты заведения уголовных дел на коррумпированных сотрудников правоохранительных органов, которые, пользуясь своим служебным положением, торговали персональными данными и результатами биллингов сим-карт, что давало возможность установить местоположение владельца мобильного телефона. Особо громкий скандал был связан с тем, что часть подобных данных была продана украинским военнослужащим, желающим установить персональные данные других российских силовиков, военных и чиновников. В связи с активным противодействием правоохранительных органов подобным коррупционным схемам похищения личных данных, как отмечают исследователи [5], услуги идентификации личности стали единственной категорией в 2023 году, цены на приобретение которой в даркнете в 2023 году не снизились, а возросли. В среднем подобные услуги предлагаются за суммы от 25 до 45 000 рублей. Американские и европейские власти смогли арестовать людей, имевших отношения к их самым крупным магазинам даркнета, предлагавшим такие услуги [2], однако в их случае они быстро заменились новыми, поэтому такого подорожания, как на российском рынке, не произошло. При этом российский сегмент рынка торговли персональными данными отличает стабильный рост спроса на услуги «пробивания» местоположения людей (по экспертным оценкам [5] за шесть месяцев 2023 года спрос в российском сегменте вырос на 1,5 раза).

Также стоит отметить ещё один аспект специфики российского рынки продажи персональных данных. У нас он во многом ушёл в «Telegram», где существует большое количество каналов и чатов, специализирующихся на

продаже личных данных и оказании услуг по взломам. Кроме того, в «Telegram» есть русскоязычные каналы и чаты, распространяющие информацию, как провести такие взломы самостоятельно.

Данные банковских карт российских банков считаются более дешёвыми, чем европейских и американских. В среднем поддельную карту с украденными данными можно приобрести за сумму около 100 000 рублей [5].

Ещё одна специфическая российская услуга, связанная с незаконным использованием персональных данных появилась в 2022 году. Разные продавцы предлагают подделать данные, чтобы избежать мобилизации. При этом ценовой разброс в этой категории чрезвычайно велик. Можно найти предложения за 50 000 рублей, а есть те, кто предлагают «решить проблему» за сумму большую, чем полтора миллиона рублей. По словам таких продавцов в даркнете, они могут помочь с получением нового военного билета со сменой категории годности, получением поддельного военного билета и т.п. Ещё одним специфическим, чисто российским видом услуг является продажа бумажных поддельных санитарных книжек и сканов книжек реальных людей.

Можно отметить, что российские киберпреступники используют во многом те же методы, что и преступники из других стран, при этом у них во многом существует традиция ориентироваться на коррупционные связи (как и у российских преступников в реальной жизни). В целом же развитие российского рынка взлома, хищения и продажи персональных данных соответствует общемировым тенденциям. По-прежнему остаются актуальными рекомендации по кибербезопасности, такие как:

- отказываться от подключения к общественным точкам доступа Wi-Fi без острой необходимости;
- не вводить данные своих карт на неизвестных платформах;
- использовать надёжные пароли и многоступенчатую аутентификацию для мессенджеров и социальных сетей;

не делиться с другими людьми своими персональными данными и не выкладывать их в открытый доступ, не давать доступ к своим аккаунтам;

- удалять сообщения с важной личной информацией и персональными данными (например, если был отправлен скан паспорта по электронной почте, то это сообщение с вложение лучше удалить и из самой переписки, и из корзины сразу);

- устанавливать ограничения доступа на документы и другие файлы с персональными данными.

Обобщая всё вышесказанное, стоит отметить, что киберпреступники на сегодняшний день во многом полагаются на недостаток грамотности и информированности обычных пользователей Интернета в вопросах кибербезопасности. Очень часто личные данные утекают из-за халатного отношения самих пользователей к надёжности защиты своих аккаунтов, финансов и т.п. Поэтому со стороны экспертного сообщества по кибербезопасности остаётся чрезвычайно важным популяризация мер по обеспечению кибербезопасности для обычных пользователей.

Список литературы

1. Dark Web Price Index 2023. URL: https://www.privacyaffairs.com/dark-web-price-index-2023/ [PrivacyAffairs] (date accessed: 21.11.2023).
2. Exclusive: The largest mobile malware marketplace identified by Resecurity in the Dark Web. URL: https://securityaffairs.co/139310/cyber-crime/dark-web-mobile-malware-marketplace.html [Security Affairs] (date accessed: 20.11.2023).
3. Дмитриева Е. Г. Проблемы защиты персональных данных в цифровом мире и пути их решения // Право и бизнес. 2021. № 3. С. 18–23.
4. Куриленко Ю.А., Едигарева Ю.Г., Ле Тхи Ван. Обеспечение информационной безопасности при утечке, разглашении и торговле персональными данными // Криминологический журнал. 2023. № 2. С. 216–221.
5. Рынок данных в даркнете: как купить чужие данные и не потерять свои. URL: https://habr.com/ru/companies/xeovo/articles/769652/ [Хабр] (date accessed: 21.11.2023).
6. Рязанова Е. Н. Ответственность за распространение персональных данных как способ противодействия правонарушениям в сфере информационно-коммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. 2022. № 3 (95). С. 118–123;
7. Устимова С. А. Защита персональных данных субъектов предпринимательской деятельности // Криминологический журнал. 2023. № 1. С. 120–123.

8. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных» // Справочно-правовая система «КонсультантПлюс».
9. Цветков А. Ю., Шалаева М. Е., Юрченко М. А. Обеспечение безопасности в клиент-серверном Java приложении для учета и автоматической проверки лабораторных работ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 756–761.
10. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки.— 2020.— № . 2. — С. 50–56.
11. 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.
12. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика» РИ-2018».— 2018. — С. 149–149.
13. Гельфанд А. М. и др. Области применения аналитики больших данных в критических информационных инфраструктурах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 438–440.

УДК 004.382.7

Возможности перехода программирования и разработки в среду Android

Музыченко Анна Николаевна

студентка магистратуры Донского государственного технического университета

***Аннотация**: В статье рассмотрена проблема, заключающаяся в том, что люди всё чаще и чаще предпочитают воспользоваться смартфоном, нежели чем компьютером, а разработка ведётся на уровне компьютеров. Рассмотрены основные компьютерные программы, используемые разработчиками, и выделены аналоги для разработки на смартфонах (Android). Определено, насколько приближена разработка на Android к разработке на компьютере. Проведена сравнительная характеристика возможностей человека при разработке за компьютером и при разработке за смартфоном.*

***Abstract**: The article considers the problem that people increasingly prefer to use a smartphone rather than a computer, while all the developments are being done at the computer level. The main computer programs used by developers are examined and analogs for development on smartphones (Android) are highlighted. It is determined how close development on Android is to development on a computer. A comparative characterization of human capabilities when developing on a computer and when developing on a smartphone is made.*

***Ключевые слова**: компьютер, смартфон, Android, возможности, переход, аналоги.*

***Keywords**: computer, smartphone, Android, capabilities, transition, analogues.*

Введение

Сейчас большинство программистов и разработчиков для выполнения своей работы используют персональные компьютеры или ноутбуки. Но работа за такими устройствами возможна не всегда. Компьютер нельзя взять с собой в дорогу. Для пользования ноутбуком необходим стол. Ими не получится воспользоваться в дороге. При временном отключении электричества их не получится подключить к портативному зарядному устройству. Долгое нахождение в сидячем положении может вызывать дискомфорт и проблемы со здоровьем. Поэтому актуальна проблема, заключающаяся в том, что большинство людей чаще предпочитают ноутбуку или компью-

теру свой смартфон, а разработка всё ещё ведётся на уровне компьютеров/ноутбуков.

Для решения этой проблемы необходимо задуматься о переходе и возможностях разработки и программирования на смартфонах — а именно на устройствах, базированных на Android. Проблема состоит в том, что большинство сред разработки рассчитаны на персональный компьютер/ноутбук, и не так просто найти программы, предназначенные для разработки на Android.

Поэтому важно сравнить возможности человека при разработке за компьютером и при разработке за смартфоном на базе Android.

Обзор и сравнение возможностей разработки

Для того, чтобы провести сравнительный анализ, выделим основные направления деятельности и соответствующие им программы при разработке за персональным компьютером или ноутбуком: разработка текстовых документов; анализ данных; создание презентаций; написание кода; компиляция программ; создание серверов; программирование контроллеров; выполнение команд; 3d моделирование; моделирование электрических схем; решение математических задач; виртуализация; рисование схем; рисование, редактирование фотографий; инструменты разработчика в браузере; тестирование запросов к API.

В таблице 1 для вышеописанных направлений приведены программы, используемые для работы на персональном компьютере или ноутбуке, с помощью поиска в сети интернет определено количество скачиваний этих программ (с учётом, что в компании может работать ~1000 человек), с помощью данных из приложения Google Play на октябрь 2023 определены их аналоги для работы на Android, определено количество скачиваний этих аналогов, дана оценка ПО для Android от 0 до 2 (где 0 — означает, что аналог не найдет, 1 — означает, что аналогом можно частично заменить компьютерную программу, 2 — означает, что аналогом можно полностью заменить компьютерную программу). [1–11]

Теперь, используя данные из таблицы 1, можно посчитать, на сколько процентов приближена разработка на Android к разработке на компьютере по формуле 1.

Таблица 1. **Компьютерные программы для разработки и их аналоги на Android**

Направление	**ПО для компьютеров и ноутбуков**		**Аналогичное ПО для Android**		**Оценка ПО на Android**
	Название	**Сколько раз скачали**	**Название**	**Сколько раз скачали**	
Разработка текстовых документов	Word	Больше 1,2 млрд.	Word	Больше 1 млрд.	2
Анализ данных	Excel	Больше 1,1 млрд.	Excel	Больше 1 млрд.	2
Создание презентаций	PowerPoint	Больше 1,5 млрд	PowerPoint	Больше 1 млрд.	2
Написание кода	NotePad++; Visual Studio Code	Больше 28 млн.; больше 17 тыс. компаний	Code Editor	Больше 1 млн.	1
Компиляция/интерпретация программ	Visual Studio + компиляторы	Больше 17 тыс компаний => ~15 млн.	Cxxdroid; Kotona Kotlin Compiler	Больше 1 млн.; Больше 50 тыс	1
Создание серверов	OpenServer	~300 тыс.	AWebServer	Больше 100 тыс.	1
Программирование контроллеров	Arduino IDE	Больше 10 тыс. компаний => ~ 10 млн.	ArduinoStudio	Больше 100 тыс.	1
Выполнение команд	Командная строка	Не найдено	Termux	Больше 10 млн.	2
3D-моделирование	AutoCad	Больше 700 млн.	3D Modeling App	Больше 5 млн.	1
Моделирование электрических схем	Multisim	Не найден	Proto	Больше 1 млн.	1

Направление	ПО для компьютеров и ноутбуков		Аналогичное ПО для Android		Оценка ПО на Android
	Название	Сколько раз скачали	Название	Сколько раз скачали	
Решение математических задач	Matlab	Больше 63 тыс. компаний => ~ 63 млн.	Matlab (отсутствует Simulink)	Больше 1 млн.	1
Виртуализация	VMware	Не найдено	Virtual Master — Android Clone	Больше 100 тыс.	1
Рисование схем	CorelDRAW	Больше 31 тыс. компаний => ~ 31 млн.	Scedio	Больше 500 тыс.	1
Рисование; редактирование фотографий	Adobe Photoshop	Не найдено	MediBang Paint	Больше 10 млн.	2
Инструменты разработчика в браузере	DevTools	Не найдено	F12	Больше 100 тыс.	1
Тестирование запросов к API	Postman	Больше 20 млн.	API Tester	Больше 50 тыс.	1

$$P = (\sum \frac{\text{Количество скачиваний ПО для } Android}{\text{Колиечство скачиваний ПО для компьютера}} * \frac{\text{Оценка ПО на } Android}{\text{Максимальная оценка}(2)})/k * 100\%, \quad (1)$$

где k — количество измерений.

Получим значение приближения 24%.

В таблице 2 проведён сравнительный анализ разработки на Android и разработки на компьютере с учётом таких данных как: сколько времени можно проводить сидя без вреда для здоровью[12], возможна ли работа при резком отключении электричества, есть ли наличие нужного ПО, насколько удобно носить с собой устройство, насколько гибкой может быть разработка.

Таблица 2. **Анализ разработки на компьютере и разработки на Android**

Показатель	**Присутствие на компьютере/ ноутбуке**	**Присутствие на смартфоне Android**	**Вывод, что лучше**
Возможность работать не сидя	Нет	Есть	Используя смартфон, можно проработать больше 10 часов без вреда позвоночнику
Возможность автономной работы	Частично	Есть	Смартфон можно несколько раз зарядить от портативного зарядного устройства, вследствие чего его работа продлится дольше, чем отключенного от сети ноутбука
Наличие нужного ПО	Есть	Частично	Как видно из таблицы 1, ПО для разработан на смартфонах пока что слабо развито
Низкий вес и габариты	Нет	Есть	Смартфон удобнее носить с собой, чем ноутбук
Гибкость — возможность разработки под разные операционные системы	Есть	Нет	С компьютера можно разрабатывать ПО и под Windows, и под Linux, и под Android

Заключение

По проведенному анализу можно сделать выводы о возможностях разработке на смартфоне на базе Android:

1. Полноценная разработка на Android пока что невозможна из-за 2 аспектов: по большинству направлений нужное программное обеспечение не развито в полной мере; на Android отсутствует гибкость разработки, код можно интерпретировать в специальных программах, но собрать программу возможности нет.
2. Разработка на Android имеет преимущества в 3 аспектах: возможность работать не сидя за столом, возможность долгой работы смартфона при отключении электричества, низкий вес и габариты.
3. Для всех программ, используемых на компьютере, можно найти частично соответствующие требованиям аналоги для Android.
4. Разработка на Android примерно на 24% приближена к разработке на компьютере.
5. Такие программы как Word, Excel, PowerPoint, командная строка, Adobe Photoshop имеют аналоги со всеми соответствующими желаниям пользователей требованиями — и имеют самое большое среди других направлений количество скачиваний в приложении Google Play — от 10 миллионов до более, чем 1 миллиарда.

Список литературы

1. Осадчий В. Количество пользователей Microsoft Office перевалило за 1,2 миллиарда // Overclockers [Электронный ресурс]. — URL: https://overclockers.ru/softnews/show/75336/kolichestvo-polzovatelej-microsoft-office-perevalilo-za-1–2-milliarda.
2. Gration E. Microsoft Excel Statistics: Spreadsheets by Numbers // Micro Biz Mag [Электронный ресурс]. — URL: https://www.microbizmag.co.uk/microsoft-excel-statistics/.
3. Бугаев В. 30 000 000 презентаций создаются в PowerPoint каждый день! Реально? // Vc.ru [Электронный ресурс]. — URL: https://vc.ru/u/263604-

vladimir-bugaev/176550–30–000–000-prezentaciy-sozdayutsya-v-power-point-kazhdyy-den-realno.
4. Notepad++ // Wikipedia [Электронный ресурс]. — URL: https://en.m.wikipedia.org/wiki/Notepad%2B%2B.
5. Companies using Visual Studio Code // Enlyft [Электронный ресурс]. — URL: https://enlyft.com/tech/products/visual-studio-code.
6. Предложения и пожелания: New! // OSPanel [Электронный ресурс]. — URL: https://ospanel.io/forum/viewtopic.php?t=1030&start=270.
7. Companies using Arduino IDE // Enlyft [Электронный ресурс]. — URL: https://enlyft.com/tech/products/arduino-ide.
8. Количество пользователей Автокада // Dwg [Электронный ресурс]. — URL: https://forum.dwg.ru/showthread.php?t=143307.
9. Companies using MATLAB // Enlyft [Электронный ресурс]. — URL: https://enlyft.com/tech/products/matlab.
10. Companies using Corel CorelDRAW // Enlyft [Электронный ресурс]. — URL: https://enlyft.com/tech/products/corel-coreldraw.
11. Postman (software) // Wikipedia [Электронный ресурс]. — URL: https://en.m.wikipedia.org/wiki/Postman_(software).
12. Медики выяснили, сколько часов в день можно сидеть // Рамблер/доктор [Электронный ресурс]. — URL: https://doctor.rambler.ru/news/34272308-mediki-vyyasnili-skolko-chasov-v-den-mozhno-sidet.

УДК 004.382.7

Исследование внедрения смартфонов в повседневную жизнь человека

Музыченко Анна Николаевна

студент магистратуры Донского государственного технического университета

***Аннотация**: Рассмотрена проблема, заключающаяся в том, что смартфоны всё чаще и чаще используются пользователями в замену компьютерам. Проведён социальный опрос для определения процентного соотношения использования смартфонов и компьютеров в повседневной жизни человека. Приведены результаты социального опроса.*

На основе метода анализа иерархий определено, насколько приближены возможности Android к возможностям персонального компьютера/ноутбука.

***Abstract**: The problem that smartphones are more and more often used by users as a substitute for computers is considered. A social survey is conducted to determine the percentage of smartphone use versus computer use in a person's daily life. The results of the social survey are presented. Based on the method of hierarchy analysis, it is determined how close the capabilities of Android are to those of a personal computer/laptop.*

***Ключевые слова**: компьютер, смартфон, Android, возможности, переход, аналоги, метод анализа иерархий.*

***Keywords**: computer, smartphone, Android, capabilities, transition, analogues, hierarchy analysis method.*

Введение

Сейчас большинство пользователей всё чаще и чаще предпочитают использовать смартфон в замену компьютера. В прождаже появляются смартфоны всё с большим и большим объёмом памяти, быстродействием. Создано много приложений, предназначенных для выполнения бытовых задач на смартфонах. Многие люди для переписки, просмотра новостей, видео уже не используют комаьютеры. Это делает актуальным исследование внедрения смартфонов в повседневную жизнь человека.

Обзор и исследование внедрения смартфонов в жизнь людей

Для того, чтобы провести исследование, был проведён социальный опрос среди людей от 18 до 40 лет. Были заданы вопросы о предпочтении устройства для выполнения бытовых задач. Диаграммы с результатами опроса показаны на рисунках 1–7.

Теперь согласно известному методу анализа иерархий [1], представим задачу в иерархической форме (рисунок 8).

Рассчитаем на основе данных из опросов оценку смартфона по отношению к компьютеру/ноутбуку в критериях К1-времени, выделяемого в день на пользование, и К2 — нуждаемости в разработке/программиро-

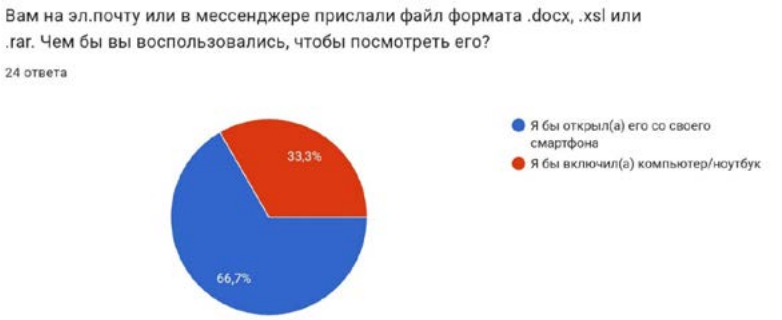

Рисунок 1. **Использование устройств для просмотра документов**

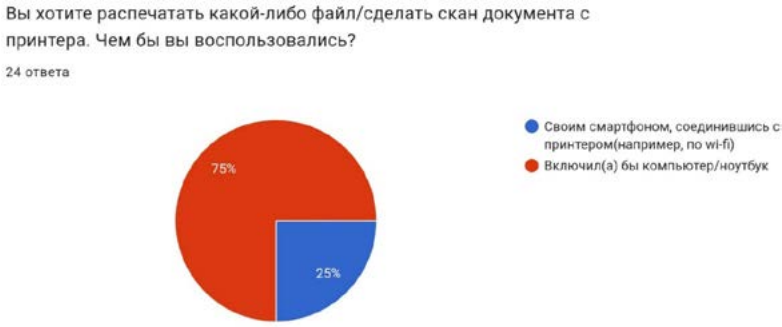

Рисунок 2. **Использование устройств для печати/сканирования**

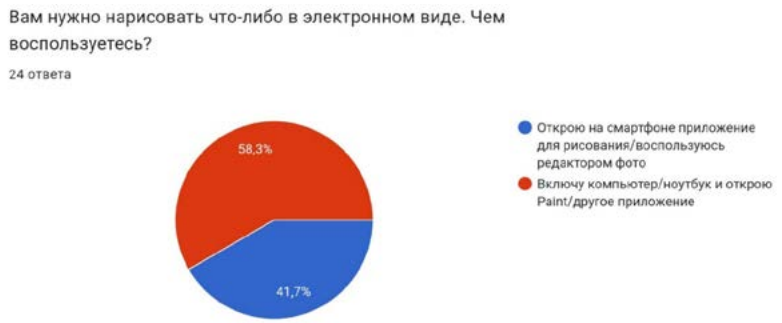

Рисунок 3. **Использование устройств для рисования в электронном виде**

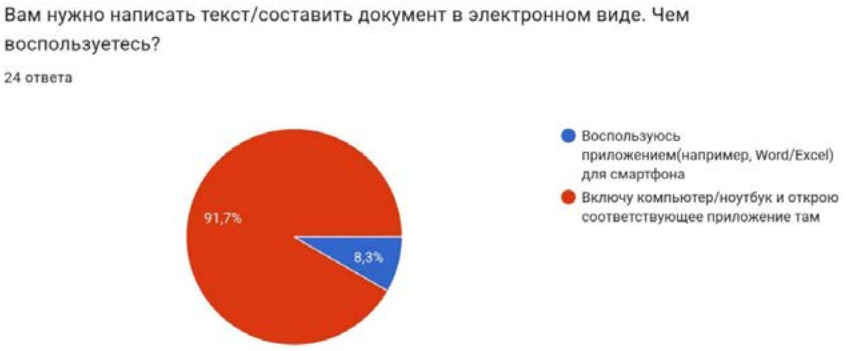

Рисунок 4. **Использование устройств для составления документов**

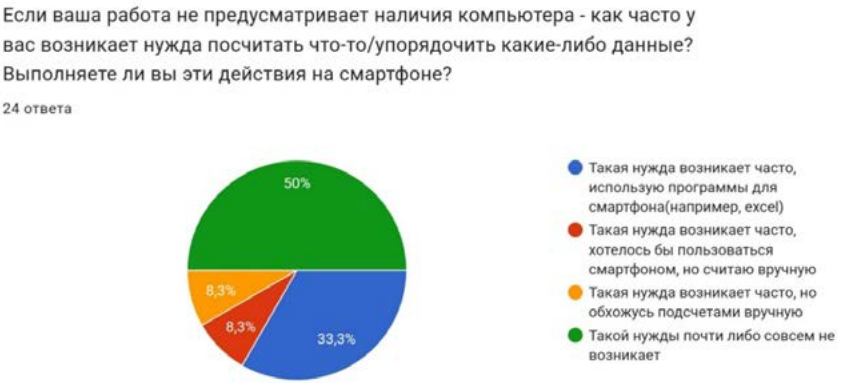

Рисунок 5. **Нуждаемость при работе, не предусматривающей компьютера**

вании на устройстве. K1 посчитаем на основе общей суммы часов, проводимой в день — по выражению 1.

$$K1 = \frac{4 * 4 + 6 * 7 + 9 * 5 + 10 * 5}{0 * 2 + 4 * 8 + 6 * 10 + 9 * 3 + 10 * 3} = 1{,}07 \sim 1 \qquad (1)$$

K2 посчитаем по выражению 2, умножая процент на коэффициенты: если разработчик уже выполняет реальные задачи на смартфоне — процент умножается на 1; если может выполнять задачи на смартфоне при отсутствии компьютера — процент умножается на 0,8; если считает раз-

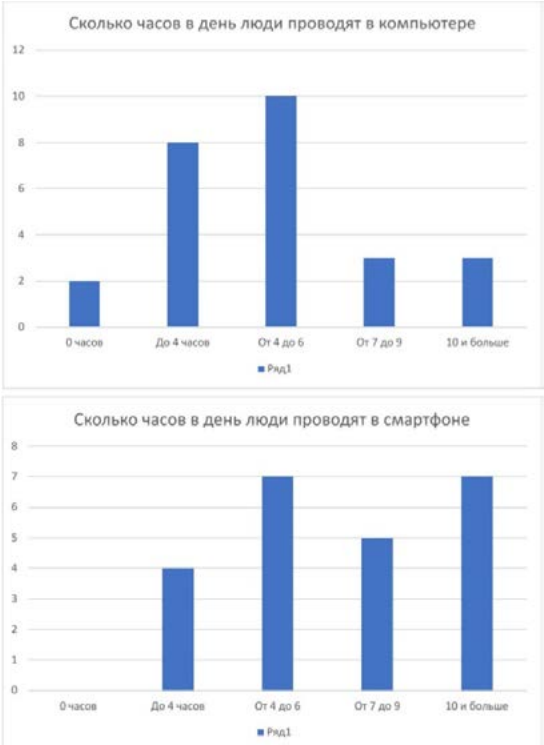

Рисунок 6. **Время, выделяемое на пользование (по горизонтали часы)**

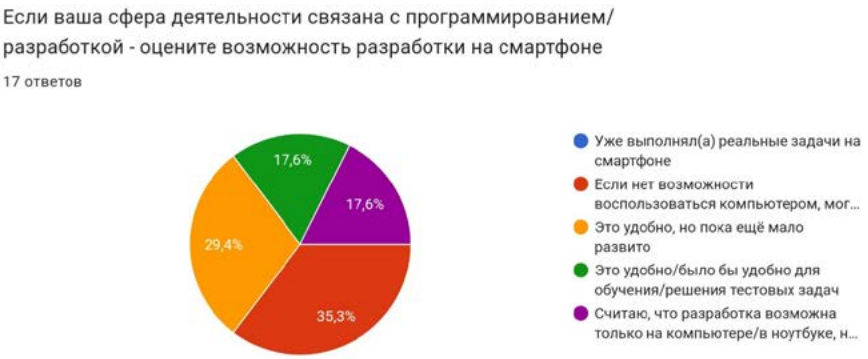

Рисунок 7. **Нуждаемость в разработке/программировании на устройстве**

работку на смартфоне удобной, но мало развитой — процент умножается на 0,5; если считает, что это было бы удобно для обучения — процент умножается на 0,25.

$$K2 = \frac{1}{1 + (50 - 0 * 1 + 35.3 * 0{,}8 + 29{,}4 * 0{,}5 + 17{,}6 * 0{,}25) * \frac{8}{50}} = \frac{1}{1{,}4} \sim 1 \quad (2)$$

Так как коэффициенты равны 1 в обоих случаях, то приоритетные значения в обоих случаях будут равны по 0,5 на каждую альтернативу. Поэтому эти 2 критерия учитывать не будем. Сократим систему иерархий до 5 критериев.

Для вычисления значений по критериям написаны скрипты. [2]

На рисунке 9 представлен скрипт функции в Matlab, которая рассчитывает приоритетные значения и оценку согласованности для матрицы парных сравнений.

```
function result = ierarhii(A, names);
result=sprintf("Значения приоритетов \n");
CC = [0 0 0.58 0.9 1.12 1.24 1.32 1.41 1.45 1.49 1.51 1.53 1.56 1.57 1.59];
N = length(A);
if N<16 SS = CC(N); else SS=CC(15); end;
i = 1;
while i <= N
    B(i) = geomean(A(i,:));
    s(i) = sum(A(:,i));
    i = i + 1;
end;
bi = B./sum(B);
main=s.*bi;
i = 1;
while i <= N
  result = result + sprintf(names(i)+"\t:\t%f \n", bi(i));
  i = i + 1;
end
sum_main = sum (main);
IS = (sum_main-N)/(N-1);
OS = IS/SS*100;
result = result + sprintf("Оценка согласованности: %f ", OS);
end
```

Рисунок 9. **Функция расчета приоритетов для иерархии**

На рисунке 10 представлен скрипт функции нахождения приоритетов иерархий для 2 альтернатив:

```
function [r1, r2] = ierarhii_from2(A);
N = 2;
i = 1;
while i <= N
    B(i) = geomean(A(i,:));
    s(i) = sum(A(:,i));
    i = i + 1;
end;
bi = B./sum(B);
r1 = bi(1); r2 = bi(2);
end
```

Рисунок 10. **Функция нахождения приоритетов для иерархии 2 критериев.**

На рисунке 11 представлен скрипт функции перевода процентов в оценку.

```
function res = proc_to9(proc);
    if proc>=50
        res = round(1+(proc-50)*2*0.08);
    else
        res = 1/round(1+(50-proc)*2*0.08);
    end;
end
```

Рисунок 11. **Функция перевода процентов в оценку.**

Для определения нуждаемости в устройстве при решении бытовых задач, на рисунке 12 приведён скрипт нахождения приоритетов критериев первого уровня, оценки даны субъективно, согласованно. [3]

```
A = [1 4 5 3 5
1/4 1 3 1/3 1
1/5 1/3 1 1/5 1/3
1/3 3 5 1 2
1/5 1 3 1/2 1];
names = ["Просмотр файлов .docx, .xls, .rar" "Печать, сканирование документов" "Рисование в электронном виде"
    "Составление документов" "Нуждаемость при работе, не предусматривающей компьютера"];
r=ierarhii(A,names);
display(r);
```

Рисунок 12. **Скрипт для определения критериев первого уровня.**

Полученный результат показан на рисунке 13.

```
"Значения приоритетов
 Просмотр файлов .docx, .xls, .rar : 0.474371
 Печать, сканирование документов : 0.114890
 Рисование в электронном виде: 0.051316
 Составление документов : 0.240267
 Нуждаемость при работе, не предусматривающей компьютера :
0.119156
 Оценка согласованности: 4.620303 "
```

Рисунок 13. **Приоритетные значения критериев первого уровня для иерархии нуждаемости в устройстве.**

Для вычисления приоритетных значений составлен скрипт, оценка смартфона по отношению к компьютеру/ноутбуку берётся из результатов опроса; в вопросе с несколькими вариантами ответа проценты ответов умножаются на соответствующий вес — если человек пользуется смартфоном при работе, процент умножается на 1, если человек хотел бы пользоваться смартфоном — процент умножается на 0.5, если человек справляется и вручную, но потребность в вычислениях всё-таки есть, процент умножается на 0,25. Скрипт приведён на рисунке 14. [4]

```
names = ["Просмотр файлов .docx, .xls, .rar" "Печать, сканирование документов" "Рисование в электронном виде"
    "Составление документов" "Нуждаемость при работе, не предусматривающей компьютера"];
ves=[0.474371 0.114890 0.051316 0.240267 0.119156];
A = [1 0; 0 1];
names2 = ["Персональный компьютер/ноутбук" "Смартфон"];
k = [proc_to9(66.7) proc_to9(25) proc_to9(41.7) proc_to9(8.3)  proc_to9(33.3*1+8.3*0.5+8.3*0.25)];
i = 1;
while i<=length(names)
    A(2,1) = k(i);
    A(1,2) = 1/k(i);
    [r1(i), r2(i)]=ierarhii_from2(A);
    i = i + 1;
end;
m1 = 0; m2 = 0; i=1;
while i<=length(names)
    m1 = m1 + r1(i)*ves(i);
    m2 = m2 + r2(i)*ves(i);
    i = i + 1;
end;
r1(i) = m1; r2(i) = m2;
names(i)="Итоговые приоритеты";
i = 1;
arr(1,1)="Критерий";arr(1,2)="Вес критериев";arr(1,3)=names2(1); arr(1,4)=names2(2);
while i<=length(names)
    arr(i+1,1)=names(i);
    if i+1<=length(names) arr(i+1,2)=string(ves(i)); end;
    arr(i+1,3)=string(r1(i));
    arr(i+1,4)=string(r2(i));
    i = i + 1;
end;
t=array2table(arr);
writetable(t, "data2.xls");
```

Рисунок 14. **Скрипт нахождения приоритетов критериев второго уровня.**

Полученный результат записан в таблицу 1.

Заключение

По результатам проведенного исследования можно сделать следующие выводы.

1. По результатам проведенного исследования установлено, что эффективность работы на смартфоне составляет примерно 47% от компьютера.

Таблица 1. **Итоговые приоритеты для иерархии нуждаемости в устройстве при решении бытовых задач**

Критерий	Вес критериев	Персональный компьютер/ ноутбук	Смартфон
Просмотр файлов .docx, .xls, .rar	0.47437	0.2	0.8
Печать, сканирование документов	0.11489	0.83333	0.16667
Рисование в электронном виде	0.051316	0.66667	0.33333
Составление документов	0.24027	0.88889	0.11111
Нуждаемость при работе, не предусматривающей компьютера	0.11916	0.75	0.25
Итоговые приоритеты		**0.52776**	**0.47224**

2. По критериям времени, выделяемом в день на пользование устройством, и нуждаемости в разработке/программировании в устройстве получены примерно одинаковые показатели для смартфона и компьютера.
3. По большинству выбранных критериев качества так или иначе просматривается тенденция использования смартфона взамен компьютеру или ноутбуку.

Список литературы

1. Т. Саати, К. Кернс, перевод с английского Р. Г. Вачнадзе, под редакцией И. А. Ушакова, М.: Радио и связь, 1991.— 224 с.
2. MATLAB Solutions [Электронный ресурс]. — URL: https://www.matlab-solutions.com.
3. Дьяконов В. П. MATLAB. Полный самоучитель; ДМК Пресс — Москва, 2010.— 768 с.
4. Курбатова, Е.А. MATLAB 7. Самоучитель; Вильямс — Москва, 2006.— 256 с.

УДК 004

Отдельные аспекты угроз безопасности интернета вещей современное состояние

Алтынбаев Артур Фларитович

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

***Аннотация**: Исследование угроз безопасности в Интернете вещей (IoT). Анализ особенностей и аспектов угроз. Архитектура IoT и ее влияние на отрасли. Проблемы безопасности и ограниченные ресурсы устройств IoT. Защита данных и устройств IoT. Описание процесса работы IoT, выделение пяти ключевых фаз работы. Обсуждение важности разработки всесторонних методов для оценки рисков и угроз, связанных с платформами Интернета вещей.*

***Abstract**: Research on security threats in the Internet of Things (IoT). Analysis of threat features and aspects. IoT architecture and its impact on industries. Security issues and resource constraints of IoT devices. Protecting data and IoT devices. Description of the IoT operation process, highlighting five key phases of operation. Discussing the importance of developing comprehensive methods to assess the risks and threats associated with Internet of Things platforms.*

***Ключевые слова**: интернет вещей, угрозы безопасности, архитектура IoT, проблемы безопасности, защита данных.*

***Keywords**: Internet of Things, security threats, IoT architecture, security problems, data protection.*

Актуальность темы исследования обусловлена тем, что повсеместно присутствующие в нашем обиходе подключенные к Интернету устройства, относящиеся к сфере «Интернет вещей» (IoT), становятся все более важными. Эта область непрерывно расширяется благодаря увеличивающемуся количеству устройств, интегрированных в мировую сеть. Большая часть информации и функций, связанных с этими устройствами, носит конфиденциальный характер и предназначена исключительно для пользователей с соответствующими правами доступа. Программное обеспечение, используемое в IoT, включает в себя приложения, работающие на основе

данных, полученных в реальном времени или в условиях, максимально приближенных к нему, что обеспечивает их надежное функционирование. Эти приложения анализируют потребительские данные и прогнозируют будущие тенденции, используя алгоритмы искусственного интеллекта.

Целью исследования является анализ и выявление особенностей и отдельных аспектов угроз безопасности Интернета вещей, которые распространены в настоящее время.

Исследованием угроз безопасности Интернета вещей занимаются такие ученые как А. В. Власенко, П. С. Киселев, Е. А. Склярова, Х. Х. Пахаев, Т. Г. Айгумов, Э. М. Абдулмукминова и др.

Решения, связанные с Интернетом вещей (IoT), охватывают широкий спектр технологических областей, включая мобильные сети, облачные технологии, обработку данных, кибербезопасность, телекоммуникационные сети и другие. Они также способствуют перекрестному использованию данных в различных отраслях. Например, информация, собранная через умные дома и промышленные системы, находит применение в автомобилестроении. Это создает условия для формирования новых коммерческих партнерств между различными секторами экономики. Таким образом, появляются новые бизнес-модели, связывающие горизонтальные отрасли, такие как телекоммуникационные операторы, с вертикальными отраслями, такими как производители автомобилей.

Архитектура Интернета вещей (IoT) описывается через трехслойную структуру. На первом, периферийном уровне находятся устройства и датчики, задействованные для сбора данных. Следующий слой — это шлюз или сетевой уровень, который связывает датчики с умными устройствами и серверами, а также отвечает за передачу и обработку информации. Завершающий, облачный уровень включает в себя серверные решения для управления, мониторинга и извлечения пользы из системы IoT. Эта технология проникает в повседневную жизнь, оказывая влияние на многие отрасли, включая сельское хозяйство, логистику, отслеживание местоположения, дистанционное наблюдение и мгновенный анализ данных. В связи с растущим интересом к IoT, эта концепция привлекает внимание исследователей и предпринимателей по всему миру. Несмотря на многочисленные преимущества, системы IoT сталкиваются с потенциальными

проблемами, в том числе в области безопасности, что остается ключевым вызовом в этой сфере [1, с. 1123].

Ассоциируемые с IoT устройства обладают ограниченными ресурсами и функциональностью, что делает их уязвимыми для атак типа «Denial of Service» (DoS), при которых злоумышленники могут прекратить работу служб. Кроме того, вредитель может вмешаться в физическую составляющую системы, заменив компоненты на нефункциональные. Ещё одним методом является внедрение поддельных или вредоносных устройств в сеть с целью перехвата контроля. Из-за относительно слабой вычислительной мощности узлов датчиков, они могут быть подвержены атакам типа «brute force», что существенно снижает их защищенность и доступность.

Защита в сфере Интернета вещей должна выходить за рамки лишь самих IoT устройств. Эти устройства часто имеют ограниченные меры безопасности и множество уязвимостей. Преобладает мнение, что производители этих устройств не придают должного значения защите и сохранению конфиденциальности данных. Вопреки существующим проблемам с безопасностью, популярность и распространение IoT продолжает расти. В этом контексте крайне важно, чтобы специалисты в области кибербезопасности и конечные пользователи развивали и применяли более эффективные методы защиты данных и устройств.

Угрозы, с которыми сталкивается Интернет вещей, можно разделить на три основные группы:

1. Общие угрозы, общие для всех интернет-систем.
2. Уникальные угрозы, присущие устройствам Интернета вещей.
3. Риски, связанные с защитой от физического повреждения, например, из-за неправильного использования оборудования и компонентов.

Традиционные методы безопасности, такие как блокировка незащищенных портов на устройствах, попадают в первую категорию. Примером может служить интернет-холодильник, который отправляет данные о содержимом и температуре через незащищенный SMTP-сервер, что делает его уязвимым для атак ботнетов [2, с. 87].

В рамках второй категории угроз Интернета вещей лежат проблемы, специфичные для оборудования IoT. Например, подключаемые устройства могут стать источником опасности для защищенных данных. Многие

мелкие IoT устройства не способны обеспечивать эффективное асимметричное шифрование из-за своих размеров. К тому же, каждое устройство, способное подключаться к Интернету, имеет встроенную операционную систему, интегрированную в его прошивку, и часто эти системы не проектируются с приоритетом на безопасность.

Интернет вещей представляет собой сеть физически идентифицируемых объектов или «вещей», которые способны взаимодействовать друг с другом, с окружающей средой или и тем, и другим одновременно. Эти устройства, соединенные с Интернетом, обмениваются данными через узлы и контроллеры. Благодаря контроллерам и облачным технологиям, эти устройства способны к самостоятельному «мышлению» и действиям, а также к сбору информации по различным причинам. Многие из этих «вещей» полностью интегрированы с операционной системой, в то время как другие могут функционировать и без нее.

В своей основе, Интернет вещей занимается сбором данных в режиме реального времени, используя разнообразные типы сетевых технологий, включая локальные сети (LAN), глобальные сети с низким энергопотреблением (LPWAN), сотовые сети LPWAN (например, узкополосный IoT и LTE-M), а также обычные сотовые сети. Эти сети могут поддерживать как постоянное, так и периодическое подключение к облачным сервисам. Важность данного процесса заключается в необходимости сохранения временных меток данных, измерении физических параметров и способности принимать обоснованные решения на основе информации, собранной данными устройствами. Это ключевое условие для реализации централизованного автоматизированного процесса принятия решений [3, с. 217].

Угрозы безопасности в мире Интернета вещей могут возникать четырьмя основными способами:

1. Через физические нападения.
2. Путем атак, нацеленных на внешнюю среду.
3. С помощью программных вмешательств,
4. И через методы криптоанализа.

Современные IoT платформы разрабатываются с применением технологий от различных производителей. Многие из этих платформ представляют собой смесь повторно используемых компонентов из уже существу-

ющих решений, применяемых на специально разработанных платформах, в надежде на их беспроблемное совместное функционирование. Однако, даже если меры безопасности присутствуют в компонентах IoT, они часто не предусматривают учёт взаимозависимостей, возникающих из-за возможностей подключения IoT. Например, многие промышленные устройства не оснащены адекватными механизмами аутентификации, так как они были спроектированы для работы в физически защищенных и изолированных условиях [6, с. 25].

Необходимо разработать всесторонние методы для оценки рисков и угроз, связанных с платформами Интернета вещей, а также инструменты для их управления. Чтобы эффективно смягчать последствия возможных атак на IoT, важно иметь глубокое понимание различных типов таких атак и порядка событий, происходящих при их активации. Первым шагом в этом направлении является классификация атак на IoT. Глубокий анализ этих атак может дать четкое представление о способах формирования сетей в рамках Интернета вещей, что в свою очередь позволит разрабатывать эффективные стратегии для минимизации их воздействия [4, с. 340].

Общий процесс работы Интернета вещей можно представить как последовательность из пяти этапов, начиная от сбора данных и заканчивая их передачей конечным пользователям. В контексте угроз безопасности, эти этапы разделяются на пять ключевых фаз работы IoT:

- Захват и восприятие данных.
- Хранение данных.
- Интеллектуальный анализ данных.
- Трансмиссия или передача информации.
- Последовательная доставка данных до конечного пользователя.

Сложность вопросов конфиденциальности в системах IoT усугубляется тем, что система представляет собой не просто набор отдельных компонентов, а единую целостность. Проблемы конфиденциальности на уровне базовых устройств могут сильно различаться от тех, что возникают на этапе анализа данных. Однако нарушение конфиденциальности на любом из этих уровней оказывает влияние на всю систему. Умные устройства способны собирать обширные объемы личных данных, при этом во многих современных IoT технологиях контроль за этой информацией остается не-

достаточным. Часто данные собираются без активного участия пользователей, что приводит к тому, что некоторые нарушения конфиденциальности могут оставаться незамеченными на протяжении долгих периодов времени [5, с. 78].

Таким образом, внедрение IoT технологий влечет за собой как новые возможности, так и значительные риски в области безопасности, делая проблемы безопасности устройств IoT критически важными. Необходима тщательная оценка рисков безопасности до начала любого использования IoT для того, чтобы убедиться в выявлении всех ключевых уязвимостей. Без адекватных мер по обеспечению безопасности и защите данных, успех IoT в долгосрочной перспективе становится под вопросом. Производители IoT обязаны включать стратегии безопасности на всех этапах от разработки до эксплуатации оборудования. В последующих исследованиях и разработках важно сформулировать и применить структуру для анализа и оценки рисков безопасности в сфере IoT, обеспечивая конфиденциальность, целостность и доступность.

Список литературы

1. Баев Д.А., Волков Р.О., Зонов А. Д. Мониторинг безопасности в IOT-сетях // StudNet.— 2021.— № 6. — С. 1122–1130.
2. Власенко А. В. Безопасность интернета вещей / А. В. Власенко, П. С. Киселев, Е. А. Склярова // Молодой ученый.— 2021.— № 21 (363). — С. 86–89.
3. Гельфанд А. М. Интернет вещей (IoT): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 215–220.
4. Калинин А. С. Интернет вещей. Принципы, технологии, перспективы развития / А. С. Калинин // Молодой ученый.— 2019 — № 2 (240). — С. 341–342.
5. Росляков А. В. Интернет вещей // Известия РАН: Теория и системы управления.— 2015.— № 5. — С. 75–88.
6. Тайшибаев Т. Б. Разработка системы онтологий Интернета вещей Т. Б. Тайшибаев // Молодой ученый.— 2020.— № 2 (292). — С. 22–27.

7. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика» РИ-2018».— 2018. — С. 149–149.
8. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 590–595.
9. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России».— 2020.— № . 2. — С. 86–94.
10. Гельфанд А. М. и др. Области применения аналитики больших данных в критических информационных инфраструктурах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 438–440.
11. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //Proceedings of the 4th International Conference on Future Networks and Distributed Systems.— 2020. — С. 1–6.

УДК 004

Особенности применения адаптивного сенсорного интерфейса в приложениях информационной безопасности

Алтынбаев Артур Фларитович

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

***Аннотация**: Исследование применения адаптивного сенсорного интерфейса в приложениях информационной безопасности. Анализ особенностей и преимуществ использования визуализации данных для анализа безопасности. Роль моделей визуализации*

в анализе и управлении доступом. Применение различных методов визуализации для представления компьютерных сетей и анализа атак. Возможности адаптивного сенсорного интерфейса в улучшении скорости и качества принятия решений.

***Abstract**: Exploring the use of adaptive touch interface in information security applications. Analysis of the features and benefits of using data visualization for security analysis. The role of visualization models in access analysis and management. Application of various visualization techniques for computer network representation and attack analysis. The potential of adaptive touch interface in improving the speed and quality of decision making.*

***Ключевые слова**: адаптивный сенсорный интерфейс, визуализация данных, информационная безопасность, модели визуализации, компьютерные сети.*

***Keywords**: adaptive touch interface, data visualization, information security, visualization models, computer networks.*

Один из методов анализа безопасности заключается в использовании техник визуальной аналитики. Этот подход включает в себя применение визуализации данных для выявления аномалий, толкования инцидентов и разработки ответных мер. В области информационной безопасности, визуализация находит широкое применение, включая мониторинг и управление доступом в разнообразных системах безопасности, оценку состояния сетей, связанных с IoT-устройствами, и изучение показателей безопасности.

Для эффективного анализа данных используются различные модели визуализации, которые опираются на классические пользовательские интерфейсы. Однако, с усложнением этих моделей возникает необходимость в новых, более интуитивно понятных формах взаимодействия, чтобы улучшить скорость и качество принятия решений. Сенсорные экраны могут предложить такое решение, но они редко используются в качестве основного средства взаимодействия между аналитиками и инструментами визуализации данных, что и обусловило актуальность темы исследования.

Целью исследования является анализ и выявление особенностей применения адаптивного сенсорного интерфейса в приложениях информационной безопасности.

Методами исследования являются метод анализа, сравнительного исследования, теоретического анализа.

Вопросами применения адаптивного сенсорного интерфейса в приложениях информационной безопасности, занимаются такие ученые как К. Н. Жернова, М. В. Коломеец, И. В. Котенко, А. А. Чечулин и др.

Модели визуализации, используемые в взаимодействии человека с компьютерными системами, определяют структуру интерфейсов. В зависимости от конкретной задачи выбираются соответствующие типы визуализаций. Например, для представления компьютерных сетей, сканирования портов, анализа атак и планирования сценариев атак часто используются графические модели, включая графы. Также возможно комбинирование различных методов визуализации, например, использование иерархических деревьев для отображения физической структуры сети, радиальных деревьев для визуализации атак, диаграмм Корда для одновременного представления физической и логической структуры сети, а также матриц для показа доступности сегментов сети для атакующих.

Различные способы визуализации применяются также для контроля и управления доступом, отображая взаимоотношения между субъектами и объектами в разных моделях прав доступа. Матрицы используются для дискретных моделей доступа, графы — для моделей Take-Grant, а TreeMaps — для иерархических моделей управления доступом на основе ролей (RBAC). Существуют также более сложные модели визуализации для анализа в комбинированных моделях безопасности, такие как треугольные матрицы, которые могут использоваться для визуализации и матриц, и деревьев.

Каждая модель визуализации применяется в соответствии с конкретной целью анализа и управления правами доступа. С ростом сложности модели безопасности увеличивается необходимость в более продвинутых методах взаимодействия для аналитиков. Например, в матрицах доступа применяются механизмы фильтрации и группировки, а в TreeMaps можно фильтровать данные, показывая только определенную часть дерева [1, с. 874].

При анализе состояния сетей также используются графы, TreeMaps, матрицы и другие визуализации. Графы особенно универсальны для визуализации любых структур сетей, TreeMaps подходят для иерархических сетей, а матрицы — для топологий типа «каждый с каждым». Карты Вороного используются для отображения сетей, формирующих планарные

структуры, например, в самоорганизующихся сенсорных сетях. У каждого метода есть свои преимущества и недостатки, поэтому их часто сочетают для достижения лучших результатов.

Адаптивный сенсорный интерфейс в приложениях информационной безопасности предлагает уникальный подход к защите и взаимодействию с данными. Можно выделить следующие особенности применения адаптивного сенсорного интерфейса в приложениях информационной безопасности:

1. Персонализированная безопасность. Адаптивные сенсорные интерфейсы могут настраиваться под индивидуальные особенности пользователя, такие как отпечатки пальцев, рисунок радужки глаза или паттерны жестов. Это обеспечивает более высокий уровень безопасности, поскольку данные методы биометрической идентификации сложнее подделать.
2. Динамическая адаптация. Интерфейс может адаптироваться к изменяющимся условиям окружающей среды или поведению пользователя. Например, в условиях слабой освещенности интерфейс может автоматически переключаться на использование биометрии, основанной на звуке или жестах.
3. Улучшенный пользовательский опыт: Адаптивные интерфейсы упрощают взаимодействие с системой безопасности, делая его более интуитивным и менее навязчивым. Это повышает вероятность того, что пользователи будут соблюдать протоколы безопасности.
4. Обучение и эволюция. Со временем система может обучаться и адаптироваться к поведению пользователя, улучшая точность и эффективность безопасных процедур. Это особенно полезно в динамически меняющихся средах безопасности.
5. Многофакторная аутентификация. Использование адаптивных сенсорных интерфейсов позволяет легко интегрировать многофакторную аутентификацию, объединяя что-то, что известно пользователю (пароль), с чем-то, что у пользователя есть (биометрические данные), и чем-то, что он делает (жесты) [2, с. 240].
6. Активное обнаружение угроз. Адаптивные системы могут активно мониторить необычные паттерны поведения или попытки несанкцио-

нированного доступа, предупреждая о возможных угрозах в реальном времени.

При разработке визуальных моделей обычно учитываются классические методы управления, такие как экран, мышь и клавиатура. Тем не менее, существует потенциал для визуального анализа с использованием планшетов, смартфонов и других сенсорных устройств. Эти устройства становятся все более популярными и предоставляют дополнительную мобильность, особенно в промышленных условиях. В сфере информационной безопасности, учитывая сложность данных и необходимость сложной визуализации, простое копирование действий мыши и клавиатуры может быть недостаточным. В то же время, жесты не должны быть излишне запутанными или неудобными для повседневного использования. В этом исследовании предложен подход, включающий модели взаимодействия между пользователем и элементами визуализации, алгоритмы адаптации, а также методы соответствия жестов оптимальным практикам.

Для понимания работы интерфейсов в области информационной безопасности важно учитывать их уникальные характеристики. Такие интерфейсы обычно включают следующие элементы:

- Применение цветовой кодировки для отображения уровней угроз: зеленый цвет обозначает безопасность, желтый — умеренный риск, красный — высокий уровень угрозы.
- Иерархическая структура: возможность вызова дополнительной информации по запросу, например, детальное отображение характеристик устройства на диаграмме [3, с. 149].
- Обработка больших объемов данных, таких как маршруты сетевого трафика.
- Обеспечение актуальной информации пользователю, связанной с временем и местоположением, например, при мониторинге сетевой активности.
- Наглядное представление данных, включая различные сетевые топологии.

Эти элементы являются ключевыми для приложений в области информационной безопасности, но способ их визуализации и взаимодействия с ними может варьироваться. К примеру, при постоянных оповещениях

о высокой степени угрозы, обозначенных красным цветом, возможно снижение внимания пользователя к таким уведомлениям. Решить эту проблему можно путем адаптивного изменения интерфейса, например, периодически меняя оттенки красного до маджента. Это поможет привлечь внимание пользователя к важным уведомлениям. Так, адаптация интерфейса к потребностям пользователя и его поведению при работе с приложением становится важной частью проектирования [4, с. 32].

Применение адаптивного сенсорного интерфейса в приложениях информационной безопасности включает в себя несколько ключевых механизмов:

1. Биометрическая идентификация. Адаптивные сенсорные интерфейсы могут использовать биометрические данные пользователя, такие как отпечатки пальцев, распознавание лица или ретины, для обеспечения безопасного доступа к системам и данным.
2. Персонализированное взаимодействие. Сенсорные интерфейсы адаптируются к индивидуальным предпочтениям пользователя, например, к расположению элементов управления или к настройкам жестов, обеспечивая более удобное и эффективное взаимодействие.
3. Динамическая адаптация. Интерфейс способен адаптироваться к изменяющимся условиям окружающей среды или контексту работы, например, переключаясь на альтернативные методы ввода в условиях недостаточного освещения или шума.
4. Многофакторная аутентификация. Комбинация биометрических данных и традиционных методов аутентификации (как пароли или PIN-коды) повышает безопасность системы [5, с. 79].

Таким образом, адаптивные сенсорные интерфейсы повышают уровень безопасности за счет индивидуальной биометрической идентификации и многофакторной аутентификации, что делает системы менее уязвимыми для несанкционированного доступа. Благодаря способности адаптироваться к индивидуальным особенностям и предпочтениям пользователя, такие интерфейсы обеспечивают более интуитивное и эффективное взаимодействие. Интерактивная визуализация и манипуляция данными упрощают анализ больших объемов информации, что критически важно в области информационной безопасности.

Список литературы

1. Коломеец М., Чечулин А., Дойникова Е., Котенко И. Методика визуализации метрик кибербезопасности // Изв. вузов. Приборостроение, Т. 61, № 10.— 2018. — С. 873–880.
2. Коломеец М., Чечулин А., Котенко И. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН.— 2015. — Вып. 42. — С. 232–257.
3. Котенко И. В. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей // Региональная информатика «РИ-2018».— 2018. — С. 149–149.
4. Котенко И., Левшун Д., Чечулин А., Ушаков И., Красов А. Комплексный подход к обеспечению безопасности киберфизических систем на системе микроконтроллеров // Вопросы кибербезопасности.— 2018.— № 3 (27). — С. 29–38.
5. Милославская Н., Толстой А., Бирюков А. Визуализация информации при управлении информационной безопасностью информационной инфраструктуры организации // Научная визуализация.— 2014. — Т. 6., № . 2.— С. 74–91.
6. Гельфанд А. М. и др. Интернет вещей (IoT): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 215–220.
7. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).— 2019. — С. 590–595.
8. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России».— 2020.— № . 2. — С. 86–94.
9. Гельфанд А. М. и др. Области применения аналитики больших данных в критических информационных инфраструктурах //Актуальные

проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022).— 2022. — С. 438–440.
10. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //Proceedings of the 4th International Conference on Future Networks and Distributed Systems.— 2020. — С. 1–6.

УДК 51:004

Симбиотические отношения между математикой и информатикой

Ли Ифэй

ученик Средней школы провинции Шаньси (Китай, Провинция Шаньси)

Джен Ван

магистр, преподаватель информатики Средней школы провинции Шаньси (Китай, Провинция Шаньси)

***Аннотация**: В этой статье исследуются сложные и симбиотические отношения между математикой и информатикой, подчеркивая, как достижения в одной области часто способствуют прогрессу в другой. Переплетенная история этих дисциплин демонстрирует фундаментальную роль, которую математические принципы играют в основании и развитии информатики. От алгоритмов и структур данных до криптографии и искусственного интеллекта — математические концепции служат основой вычислительных инноваций. В этой статье рассматриваются ключевые точки пересечения математики и информатики, подчеркиваются взаимные выгоды и совместный характер этих двух областей.*

***Abstract**: This article explores the complex and symbiotic relationship between mathematics and computer science, highlighting how advances in one field often foster progress in the other. The intertwined history of these disciplines demonstrates the fundamental role that mathematical principles play in the founding and development of computer science. From algorithms and data structures to cryptography and artificial intelligence, mathematical concepts serve as the foundation of computational innovation. This article examines key points of intersection between mathematics and computer science, highlighting the mutual benefits and collaborative nature of those two fields.*

***Ключевые слова**: математика, информатика, алгоритмы, компьютерная наука, симбиоз.*

***Keywords**: mathematics, computer science, algorithms, computer science, symbiosis.*

В начале XIX века наблюдается существенное расширение области применения математического анализа. Если до этого момента механика и оптика были основными разделами физики, требующими обширного математического аппарата, то сейчас к ним добавляются электродинамика, теория магнетизма и термодинамика. Механика непрерывных сред также получает широкое развитие. С технической стороны активно растут математические запросы. Основные инструменты для новых областей механики и математической физики становятся теории обыкновенных дифференциальных уравнений, теории дифференциальных уравнений с частными производными и уравнений математической физики.

Теория дифференциальных уравнений, вдохновленная трудами французского математика Анри Пуанкаре (1854–1941) и русского математика А. М. Ляпунова (1857–1918), становится отправной точкой для исследований в области топологии многообразий. Здесь зарождаются «комбинаторные», «гомологические» и «гомотопические» методы в алгебраической топологии. Другое направление в топологии формируется на основе теории множеств и функционального анализа, что приводит к систематическому формированию теории общих топологических пространств.

Важным дополнением к методам дифференциальных уравнений в изучении природы и решении технических задач являются методы теории вероятностей. Если в начале XIX века вероятностные методы применялись преимущественно в теории артиллерийской стрельбы и теории ошибок, то к концу XIX и началу XX века теория вероятностей находит новые применения в создании теории случайных процессов и развитии математической статистики.

Теория чисел, изначально представлявшая собой набор отдельных результатов и идей, с XIX века начинает развиваться в стройную и систематизированную теорию.

В XXI веке информационные технологии становятся неотъемлемой частью всех сфер общественной жизни, проникая и трансформируя различные отрасли народного хозяйства. На сегодняшний день трудно представить себе какую-либо область без влияния информационных и коммуникацион-

ных технологий (ИКТ). Они выступают в качестве неотъемлемой основы и эффективного инструмента для современных педагогических технологий, улучшая качество учебного процесса и раскрывая теоретический и практический потенциал, а также развивая компетентность будущих специалистов.

Сегодня важно, чтобы любой профессионал владел различными ИКТ в своей повседневной деятельности. Особенно это касается связи между математикой и информатикой, что подчеркивается многолетним опытом работы кафедры математики и информатики в высшем образовании. Использование современных информационных и коммуникационных технологий в учебном процессе эффективно объединяет эти две дисциплины. Таким образом, ИКТ служат не только инструментом для развития математических и информатических знаний, но и движущей силой для взаимосвязи между ними.

Это подчеркивает необходимость того, чтобы математики, физики, экономисты и другие специалисты обладали базовыми знаниями в области информационных и коммуникационных технологий. Они должны уметь успешно применять современные технологии для улучшения своей профессиональной деятельности и активного участия в современном информационном обществе.

Математика и информатика, хотя и являются разными дисциплинами, имеют глубокую и взаимосвязанную историю. Эволюция информатики глубоко укоренена в математических теориях и принципах. Цель этой статьи — изучить симбиотические отношения между этими двумя областями, подчеркнув их совместный характер и влияние математических достижений на развитие информатики.

1. Математические основы информатики

а. Теория множеств и логика

Теория множеств и математическая логика составляют основу информатики. Работа Джорджа Буля по булевой алгебре заложила основу для логических операций, используемых в компьютерном программировании. Концепция множеств имеет фундаментальное значение для структур данных, алгоритмов и представления информации в вычислениях.

б. Алгоритмы и сложность

Изучение алгоритмов, раздела математики, имеет решающее значение в информатике. Алгоритмический анализ эффективности и сложности включает математические методы для оценки производительности алгоритмов. Математические модели помогают прогнозировать и оптимизировать требования алгоритмов к ресурсам, влияя на общую эффективность вычислительных систем.

2. Применение математики в информатике

а. Криптография

Криптография во многом опирается на теорию чисел и абстрактную алгебру. Криптография с открытым ключом, краеугольный камень безопасной связи, использует математические свойства, такие как сложность факторизации больших чисел. Например, алгоритм RSA зависит от математических свойств простых чисел.

б. Искусственный интеллект

Математика, особенно линейная алгебра и исчисление, играет ключевую роль в машинном обучении и искусственном интеллекте. Такие модели, как нейронные сети, по сути представляют собой математические конструкции, в которых алгоритмы используют математические функции для обучения и прогнозирования на основе данных.

3. Совместные достижения

а. Математическое моделирование в информатике

Совместные усилия математиков и ученых-компьютерщиков привели к разработке математических моделей, моделирующих явления реального мира. Прогноз погоды, гидродинамика и моделирование в различных на-

учных дисциплинах используют возможности обеих областей для достижения точных и эффективных результатов.

b. Комбинаторика в информатике

Комбинаторная математика находит применение в информатике посредством изучения комбинаций и перестановок. Комбинаторные алгоритмы необходимы для решения таких задач, как оптимизация сети, планирование, а также обнаружение и исправление ошибок.

Один из эффективных методов для организации интегрированного и междисциплинарного обучения в области информатики и математики заключается в создании уроков, объединяющих обе дисциплины. Этот подход способствует разностороннему взаимодействию и делает учебный процесс более увлекательным, интенсивным и интересным. Интерактивные комментарии и взаимная поддержка во время урока дополняют друг друга, обогащая математический и информативный контекст, что содействует более эффективному процессу обучения.

Такой подход к обучению позволяет учащимся более глубоко понимать свои собственные способности, развивать интерес к учебному процессу и стимулировать творческое мышление. Интегрированный стиль обучения является тем полем, где педагоги могут проявить свою творческую инициативу, проверить и улучшить свои методы преподавания и педагогический опыт.

На уроках с интегрированным подходом можно пояснить ключевые моменты, модули и концепции, используя современные средства, такие как слайды, диаграммы, анимации и звуковые эффекты. Это позволяет студентам развивать аналитическое мышление, видеть результаты своей работы в режиме реального времени и чувствовать вовлеченность в процесс обучения. Несмотря на множество преимуществ, сопутствующих активному обучению, существуют и недостатки, такие как отсутствие опыта учителя математики в программировании и недостаточное количество компьютеров для индивидуальной работы.

Данный анализ интегрированных компьютеризированных уроков, осуществленный при использовании современных образовательных тех-

нологий, подчеркивает важность активного внедрения новых педагогических подходов. Если учитель заинтересован в создании стимулирующей и полезной образовательной среды, соответствующей требованиям современных информационных технологий, и способен эффективно применять свои знания в практике, то использование интегрированных компьютеризированных уроков может быть эффективным инструментом для индивидуализации обучения, повышения мотивации и улучшения обратной связи.

Математика предоставляет исследователям широкий спектр математических методов, которые не только позволяют получить числовые характеристики изучаемого объекта, но и способны моделировать его поведение под воздействием различных факторов. Это имеет значительное значение в научных исследованиях.

Информатика, предлагает обширный инструментарий, который способствует существенному ускорению процесса проведения исследований. Применение специализированного программного обеспечения позволяет улучшить точность и сократить трудозатраты, делая возможным проведение многовариантных анализов сложных мероприятий, которые были бы непосильными при использовании традиционных «ручных» методов.

Таким образом, взаимодействие математики и информатики в процессе исследований существенно повышает уровень качества проводимых исследований. Это позволяет получать результаты, максимально приближенные к реальности, и экономить время как на самом исследовании, так и на обработке полученных данных.

В заключение отметим, что сложная взаимосвязь между математикой и информатикой неоспорима. Историческое и постоянное сотрудничество между этими двумя дисциплинами привело к революционным достижениям, которые формируют наш технологический ландшафт. От основополагающих принципов теории множеств и логики до приложений в криптографии, искусственном интеллекте и т. д. — математика остается незаменимым инструментом для ученых-компьютерщиков. Поскольку обе области продолжают развиваться, синергия математики и информатики, несомненно, приведет к дальнейшим инновациям и революционным прорывам.

Список литературы

1. Буль, Г. (1854). Исследование законов мышления, на которых основаны математические теории логики и вероятностей.
2. Кормен Т.Х., Лейзерсон К.Э., Ривест Р.Л. и Стейн К. (2009). Введение в алгоритмы. МТИ Пресс.
3. Кнут, Д. Э. (1968). Искусство компьютерного программирования, Том 1: Фундаментальные алгоритмы. Аддисон-Уэсли.
4. Рассел С. и Норвиг П. (2009). Искусственный интеллект: современный подход. Прентис Холл.
5. Столлингс, В. (2017). Криптография и сетевая безопасность: принципы и практика. Пирсон.
6. Трефетен Л. Н. и Бау Д. (1997). Численная линейная алгебра. СИАМ.
7. Кормен Т.Х., Стейн К., Ривест Р.Л. и Лейзерсон К.Е. (2001). Введение в алгоритмы. МТИ Пресс.

УДК 004.4

Достижения и проблемы в разработке компьютерного программного обеспечения

Ли Синьюэ

выпускница Экспериментальной средней школы Чжуншань (Китай, Провинция Гуандонг)

Лян Яньин

магистр, преподаватель информационных технологий Экспериментальной средней школы Чжуншань (Китай, Провинция Гуандонг)

***Аннотация**: В данной статье представлен обзор текущего состояния разработки компьютерного программного обеспечения с упором на последние достижения и текущие проблемы в этой области. Опираясь на ряд соответствующей литературы, в статье исследуются тенденции в разработке программного обеспечения, включая гибкие методологии, DevOps и микросервисы. В нем также обсуждаются новые технологии, такие как искусственный интеллект, блокчейн и квантовые вычисления, и их потен-*

циальное влияние на разработку программного обеспечения. Кроме того, в документе освещаются текущие проблемы в разработке программного обеспечения, такие как безопасность, надежность и масштабируемость, и исследуются стратегии решения этих проблем. В конечном счете, в документе утверждается, что разработка компьютерного программного обеспечения остается динамичной и быстро развивающейся областью, и что эффективные ответы на возникающие проблемы требуют постоянного сотрудничества и инноваций.

***Abstract**: This paper provides an overview of the current state of computer software development, focusing on recent advances and current challenges in the field. Drawing on a range of relevant literature, the paper explores trends in software development, including agile methodologies, DevOps, and microservices. It also discusses emerging technologies such as artificial intelligence, blockchain and quantum computing and their potential impact on software development. In addition, the paper highlights current challenges in software development, such as security, reliability, and scalability, and explores strategies to address these challenges. Ultimately, the paper argues that computer software development remains a dynamic and rapidly evolving field, and that effective responses to emerging challenges require continuous collaboration and innovation.*

***Ключевые слова**: программирование, инновации, технологии, проблемы разработки ПО, качество кода.*

***Keywords**: programming, innovation, technology, software development problems, code quality.*

Введение

Разработка компьютерного программного обеспечения — это динамичная и быстро развивающаяся область, обусловленная рядом факторов, включая достижения в области технологий, меняющиеся потребности пользователей и развивающиеся бизнес-модели. Инженеры-программисты отвечают за проектирование, разработку, тестирование и поддержку программных систем, поддерживающих различные приложения и отрасли. В последние годы произошли значительные успехи в разработке программного обеспечения, такие как гибкие методологии разработки, DevOps и микросервисы. Также появились новые технологии, такие как искусственный интеллект, блокчейн и квантовые вычисления, которые могут трансформировать разработку программного обеспечения. Несмотря на эти достижения, разработка программного обеспечения также

сталкивается с рядом постоянных проблем, включая безопасность, надежность и масштабируемость. В этой статье представлен обзор последних достижений и текущих проблем в разработке компьютерного программного обеспечения, опираясь на ряд литературы и тематических исследований.

Инженерия программного обеспечения представляет собой обширную область, сочетающую в себе компьютерную науку и технологии. Ее основная задача заключается в разработке программных систем, настолько масштабных и сложных, что для их создания требуется совместная работа больших команд разработчиков с различными специализациями и уровнем квалификации. Эти системы не только существуют в течение долгих лет, но и постоянно эволюционируют, проходя через версии, в процессе которых вносятся многочисленные изменения. Эти изменения включают в себя улучшение существующих функций, добавление новых возможностей, удаление устаревших элементов, а также адаптацию к новым средам и устранение дефектов.

Основная концепция методологии программной инженерии заключается в использовании систематизированного, научного и предсказуемого процесса, охватывающего планирование, проектирование, разработку и сопровождение сложных программных продуктов.

Исследования и опыт, накопленные в области программной инженерии в 90-е годы, послужили основой для формирования методологической концепции и комплекса знаний в этой сфере. Специалисты из IEEE Computer Society Professional Practices Committee провели необходимую селекцию и концентрацию основных проблем, методов и публикаций. Этот процесс завершился в 2004 году с публикацией соответствующего документа, который в 2005 году был принят в качестве международного стандарта ISO.

Программные средства все более интегрируются в разнообразные сложные системы. Работа с такими проектами требует от программных инженеров широкого понимания общих проблем проектирования систем. Они должны участвовать в формулировке требований для всей системы, понимать область применения программного обеспечения еще до начала проектирования абстрактных компонентов и их интерфейсов. Поиск компромиссов между задачами и функциями проекта становится важным аспектом инженерной деятельности.

Гибкие методологии

Гибкие методологии — это набор практик разработки, в которых приоритет отдается гибкости, сотрудничеству и реагированию на меняющиеся потребности пользователей. В гибких методологиях особое внимание уделяется итеративной разработке, непрерывному тестированию и интеграции, а также сотрудничеству между разработчиками и заинтересованными сторонами. Гибкие методологии получили широкое распространение в разработке программного обеспечения, и было доказано, что они повышают производительность, качество и удовлетворенность клиентов.

DevOps

DevOps — это набор практик, направленных на интеграцию разработки и эксплуатации программного обеспечения для повышения эффективности, качества и скорости доставки. DevOps делает упор на автоматизацию, непрерывный мониторинг и связь между командами разработки и эксплуатации. Было доказано, что DevOps повышает эффективность, качество и удовлетворенность клиентов, и он становится все более популярным в разработке программного обеспечения.

Микросервисы

Микросервисы — это архитектурный подход к разработке программного обеспечения, при котором приложения разбиваются на небольшие независимые модули, которые можно разрабатывать и развертывать независимо. Микросервисы подчеркивают модульность, масштабируемость и гибкость, и было показано, что они сокращают время разработки, повышают масштабируемость и улучшают удобство обслуживания.

Новые технологии

Новые технологии, такие как искусственный интеллект (ИИ), блокчейн и квантовые вычисления, могут изменить разработку программного

обеспечения. Искусственный интеллект и машинное обучение можно использовать для разработки интеллектуальных программных систем, способных обучаться и адаптироваться к меняющимся потребностям пользователей. Технологии блокчейна могут повысить безопасность, прозрачность и целостность данных в программных системах. Квантовые вычисления обладают потенциалом для решения сложных проблем, которые выходят за рамки возможностей классических компьютеров.

Проблемы

Несмотря на эти достижения, разработка программного обеспечения сталкивается с постоянными проблемами в области безопасности, надежности и масштабируемости. Безопасность остается серьезной проблемой, поскольку программные системы должны быть способны противостоять все более изощренным атакам. Надежность является важнейшей проблемой, поскольку программные системы становятся все более сложными и взаимосвязанными, что приводит к увеличению риска ошибок и сбоев. Масштабируемость также является серьезной проблемой, поскольку программные системы должны быть способны обрабатывать возрастающие объемы данных и трафика.

Стратегии решения проблем

Чтобы решить эти проблемы, инженеры-программисты должны принять ряд стратегий, включая лучшие практики в области проектирования и разработки программного обеспечения, тестирования и отладки, а также интеграции и развертывания. Они также должны быть в курсе новых технологий и тенденций в этой области, а также работать совместно с заинтересованными сторонами и другими инженерами для разработки эффективных решений. Также важно учитывать вопросы безопасности, надежности и масштабируемости в процессе разработки программного обеспечения, от проектирования до развертывания и обслуживания.

Методы успешного создания сложных программных комплексов высокого качества отечественных специалистов в 60–80-е годы были основа-

ны, главным образом, на опыте работы в сфере оборонной промышленности. Этот опыт, хотя и ценимый, сегодня в значительной степени утрачен и частично устарел. Новое поколение специалистов вынуждено создавать и осваивать методологии промышленной программной инженерии для разработки масштабных программных продуктов высокого качества практически с нуля. Задача заказчиков и пользователей становится более сложной в связи с острой нехваткой квалифицированных подрядчиков, способных эффективно создавать сложные программные системы и базы данных в сжатые сроки и при ограниченных ресурсах.

Большинство вузов ограничивают свою программу обучения, фокусируясь на основах программирования и создания простых программ. Студенты не получают достаточно подготовки в области системного анализа, проектирования, и управления проектами программного обеспечения, интеграции, тестирования и обеспечения качества для крупных программных комплексов реального времени. Выпускники не знакомы с современными промышленными методами, технологиями и международными стандартами программной инженерии, регулирующими жизненный цикл программных продуктов, инструментальные системы обеспечения качества, верификацию, тестирование и сертификацию сложных программных продуктов. Это приводит к низкой квалификации многих предприятий, занимающихся созданием крупных программных систем. Результатом становится неконкурентоспособность, недостаточное качество и долгосрочная доработка проектов для устранения системных и технических дефектов и ошибок.

Отсутствие обучения студентов методам программной инженерии и обеспечению требуемого качества программных комплексов при их практической деятельности создает широкие возможности для произвольной оценки качества программных продуктов и проявления многочисленных дефектов и ошибок. С ростом сложности и ответственности задач, решаемых программными комплексами реального времени, а также возможных потерь из-за недостаточного качества, актуальность освоения методов полного и стандартизированного описания требований к характеристикам качества на различных этапах жизненного цикла этих программных систем значительно возрастает. Студентам и специалистам

необходимо освоить понятия, определения и методы оценки реальных характеристик качества программных продуктов, систематизировать эти характеристики, а также научиться применять стандарты для выбора из них и адаптации соответствующих значений для конкретных проектов программных комплексов.

Заключение

Разработка компьютерного программного обеспечения остается динамичной и развивающейся областью, обусловленной достижениями в области технологий и меняющимися потребностями пользователей. Последние достижения в области гибких методологий, DevOps и микросервисов, а также новые технологии, такие как искусственный интеллект, блокчейн, и квантовые вычисления могут изменить разработку программного обеспечения. Однако эта область также сталкивается с постоянными проблемами в области безопасности, надежности и масштабируемости. Чтобы решить эти проблемы, инженеры-программисты должны принять ряд стратегий, включая лучшие практики в проектировании и разработке программного обеспечения, а также быть в курсе новых технологий и совместно работать над разработкой эффективных решений.

Список литературы

1. Фаулер, М. (2010). Непрерывная интеграция. Пирсон Образование.
2. Ларман К. и Базили В.Р. (2003). Итеративная и инкрементная разработка: краткая история. Компьютер IEEE, 36(6), 47–56.
3. Мелл П. и Гранс Т. (2011). Определение облачных вычислений NIST. Национальный институт стандартов и технологий.
4. Прессман, Р.С. (2014). Программная инженерия: подход практика. Макгроу-Хилл Образование.
5. Шталь, Ф. (2017). Искусственный интеллект и программная инженерия. Спрингер.

УДК 338.12.017

Цифровизация сферы образования как элемент экономики

Евстраткин Кирилл Сергеевич

студент Российского государственного социального университета

Кобилянский Станислав

студент Российского государственного социального университета

***Аннотация**: В этой статье рассматривается роль цифровизации в современном образовании и то, как она может принести пользу экономике. Цифровизация предлагает экономически эффективный способ предоставления качественного образования, расширения доступа к образовательным ресурсам и улучшения результатов учащихся. В статье исследуется, как цифровизация может стимулировать экономический рост, создавая образованную и производительную рабочую силу. В статье также рассматриваются риски цифровизации и то, как ими можно управлять.*

***Abstract**: This article discusses the role of digitalization in modern education and how it can benefit the economy. Digitalization offers a cost-effective way of delivering quality education, increasing access to educational resources and improving student outcomes. The article explores how digitalization can stimulate economic growth by creating an educated and productive workforce. The article also discusses the risks of digitalization and how they can be managed.*

***Ключевые слова**: цифровизация, образование, экономика, технологии, IT.*

***Keywords**: digitalization, education, economy, technology, IT.*

Цифровая трансформация экономики — это долгосрочная тенденция, которая ещё больше ускорилась в результате пандемии Covid-19 [2]. Цифровизация охватывает все секторы, особенно систему образования, где цифровые технологии стали важнейшими компонентами процессов преподавания и обучения. Поскольку цифровизация продолжает расширяться и революционизировать сектор образования, она становится все более важным компонентом экономики в целом.

Первый и, вероятно, наиболее очевидный способ, с помощью которого цифровизация образования стимулирует экономику, — это повыше-

ние производительности [6]. Цифровые технологии обеспечивают более быструю и эффективную коммуникацию, управление данными и процессы обучения. Например, использование платформ онлайн-обучения позволило преподавателям сократить время, затрачиваемое на разработку планов уроков, организацию занятий и проведение тестов. Это позволило преподавателям больше сосредоточиться на процессе обучения, а также на предоставлении обратной связи и персонализированной помощи учащимся. Все эти повышенные показатели эффективности позволяют преподавателям повышать свою производительность.

Цифровизация также способствует экономическому росту, создавая новые рабочие места. Цифровая трансформация сектора образования создала спрос на новые должности, такие как редакторы онлайн-контента, разработчики цифровых учебных программ и администраторы платформ онлайн-обучения [5]. Спрос на эти новые роли, вероятно, возрастёт в будущем, поскольку все больше и больше образовательных учреждений внедряют цифровые технологии. Кроме того, использование цифровых технологий может позволить преподавателям охватить более широкую аудиторию, что может открыть новые возможности для получения дохода от услуг преподавания и профессиональной подготовки.

Внедрение цифровых технологий также потенциально может снизить стоимость образования [3]. Стоимость предоставления образования, как правило, высока из-за накладных расходов на материалы и инфраструктуру, а также расходов на заработную плату преподавателей. Цифровые технологии обладают потенциалом для снижения этих затрат, позволяя более эффективно использовать материалы и инфраструктуру, а также предоставляя доступ к более широкому спектру ресурсов, которые, как правило, более экономичны, чем традиционные. Например, цифровые учебники часто дешевле традиционных учебников и могут использоваться более широким кругом учащихся.

Повышение эффективности образовательного процесса также имеет потенциал для обеспечения экономического роста в долгосрочной перспективе. Предоставляя обучающимся лучший образовательный опыт, цифровизация может привести к улучшению результатов с точки зрения успеваемости учащихся и возможностей трудоустройства [4]. Улучшение результатов образования может привести к более высоким заработкам

выпускников и более высоким налоговым поступлениям, что, в свою очередь, может привести к более высокому экономическому росту.

Цифровизация образования сопряжена с целым рядом потенциальных рисков. Сбор, хранение и передача данных — все это уязвимо для кибератак, взлома и утечки данных. Онлайн-занятия часто требуют от учащихся использования персональных устройств, что создает дополнительные риски, такие как вредоносное ПО и нарушения конфиденциальности. Чтобы управлять этими рисками, школьные системы и учреждения должны внедрять политику безопасности и процедуры сбора, хранения и передачи данных. Они также должны обеспечить актуальность и безопасность своей сетевой инфраструктуры и поощрять своих студентов использовать только безопасные веб-сайты и приложения. Они также должны разработать всеобъемлющую политику конфиденциальности и проводить регулярные тренинги по передовым методам кибербезопасности.

Поскольку общество продолжает двигаться в направлении цифровизации, важно внедрить руководящие принципы, которые помогут обеспечить использование цифровых технологий таким образом, чтобы это было выгодно как для качества образования, так и для экономики [1]. Во-первых, цифровизация должна справедливо применяться ко всем учащимся, независимо от пола, расы или социально-экономического статуса. Это означает обеспечение надёжной инфраструктуры с достаточным количеством устройств и доступом в Интернет для каждого учащегося в образовательной группе. Кроме того, учителей следует обучать и поддерживать в использовании цифровых инструментов, чтобы убедиться, что они обладают необходимыми навыками для надлежащего применения их в образовательной группе. Кроме того, цифровизация должна использоваться значимым и увлекательным образом, который предоставляет учащимся доступ к разнообразным источникам, идеям и опыту. Наконец, образовательным организациям следует сотрудничать с предприятиями и другими заинтересованными сторонами, чтобы обеспечить разработку необходимых технологий и нормативных актов. При наличии этих руководящих принципов цифровизацию можно использовать для повышения качества образования и экономики.

Таким образом, цифровизация образования является важным компонентом экономики в целом. Это потенциально может повысить производительность и создать новые рабочие места, а также снизить стоимость

предоставления образования. Кроме того, это может привести к улучшению результатов в области образования и ускорению экономического роста в долгосрочной перспективе. Поскольку цифровые технологии продолжают революционизировать сектор образования, они будут становиться все более важной частью экономики в целом.

Список литературы

1. Блинов В.И., Биленко П. Н., Дулинов М.В., Есенина Е.Ю., Кондаков А.М., Сергеев И. С. Педагогическая концепция цифрового профессионального образования и обучения // Российская академия народного хозяйства и государственной службы при президенте российской федерации федеральный институт развития образования, 2020. URL: https://firo.ranepa.ru/files/docs/spo/cifrovaya_didactika/pedagogicheskaya_koncepciya_cifrovogo_prof_obr_i_obuch_jan2020.pdf (дата обращения 05.11.2023).
2. Ван Цзинвэнь, Симоненко Е. С. Влияние COVID-19 на развитие цифровой образовательной среды // РСЭУ. 2022. № 1 (56). URL: https://cyberleninka.ru/article/n/vliyanie-covid-19-na-razvitie-tsifrovoy-obrazovatelnoy-sredy (дата обращения: 05.11.2023).
3. Гурулева Татьяна Леонидовна, Бедарева Наталия Игоревна. Сотрудничество России и Китая в области создания сетевых университетов и совместных образовательных учреждений // Высшее образование в России. 2019. № 4. URL: https://cyberleninka.ru/article/n/sotrudnichestvo-rossii-i-kitaya-v-oblasti-sozdaniya-setevyh-universitetov-i-sovmestnyh-obrazovatelnyh-uchrezhdeniy (дата обращения: 05.11.2023).
4. Первова Татьяна Петровна. Повышение эффективности образовательного процесса через применение современных подходов к организации образовательной деятельности. // Мультиурок. URL: https://multiurok.ru/files/povyshenie-effektivnosti-obrazovatelnogo-protses-3.html (дата обращения 05.11.2023).
5. Строков Алексей Александрович Цифровизация образования: проблемы и перспективы // Вестник Мининского университета. 2020. № 2 (31). URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-obrazovaniya-problemy-i-perspektivy (дата обращения: 05.11.2023).

6. Ерпелев, А. В. Социально-экономическое развитие региона, как основной фактор для улучшения жизни региона в процессе цифровизации экономики (на примере Москвы и Московской области) / А. В. Ерпелев, А. Н. Малолетко // OpenScience.— 2023. — Т. 5, № 3. — С. 113–123. — DOI 10.51632/2658–7939_2023_5_3_113. — EDN IUBHMQ.

УДК 004.8

Искусственный интеллект и его влияние на жизнь человека

Евстраткин Кирилл Сергеевич

студент Российского государственного социального университета

Кобилянский Станислав

студент Российского государственного социального университета

***Аннотация**: Статья посвящена понятию искусственного интеллекта и созданию новых технологий.*

***Abstract**: The article focuses on the concept of artificial intelligence and the creation of new technologies.*

***Ключевые слова**: машинное обучение, искусственный интеллект, нейронные сети, глубокое обучение.*

***Keywords**: machine learning, artificial intelligence, neural networks, deep learning.*

Понятие «интеллект» впервые появилось в психологии. Психологи утверждают, что интеллект — это черта личности, выражающаяся в способности глубоко и точно отражать в сознании объекты и явления объективной реальности в их существенных связях и закономерностях, а также в творческом преобразовании опыта.

Искусственный интеллект является одной из самых передовых областей исследований учёных. Системы, разработанные с его частичным использованием: распознавание текста, бытовые роботы для искусственного

замещения возможности творческой работы человека. Эта область возникла на стыке различных дисциплин: информатики, философии, кибернетики, математики, психологии, физики, химии и др [6].

Целью создания полноценного искусственного интеллекта является улучшение жизни человека и повышение уровня автоматизации производства. Людям оставалось бы заниматься высокоразвитой творческой работой, которая доставляла бы удовольствие.

Разработка интеллектуальных информационных систем или систем, основанных на знаниях. Это одно из основных направлений искусственного интеллекта. Основной целью создания таких систем является выявление, исследование и применение знаний высококвалифицированных специалистов для решения сложных задач, возникающих на практике. При построении систем, основанных на знаниях, используются знания, накопленные экспертами в виде конкретных правил для решения определённых задач. Это направление направлено на имитацию человеческого искусства анализа неструктурированных и плохо структурированных проблем. В этой области исследований разрабатываются модели представления, извлечения и структурирования знаний, а также изучаются проблемы создания баз знаний, составляющих ядро систем, основанных на знаниях [1].

ИИ, машинное обучение, нейронные сети

Машинное обучение — это специализированный способ обучения компьютерам, не прибегая к программированию.

В компьютер встроен алгоритм независимого поиска решений за счёт комплексного использования статистических данных, на основе которых выводятся закономерности и на основе которых делаются прогнозы.

Задачи машинного обучения:

1. Задача регрессии представляет собой прогноз, основанный на выборке объектов с различными характеристиками.
2. Задача классификации состоит в получении категорического ответа, основанном на наборе признаков.
3. Задачей кластеризации является распределение данных по группам: разделение всех клиентов мобильного оператора по уровню пла-

тёжеспособности, отнесение космических объектов к определённой категории.

4. Задача уменьшения размерности состоит в том, чтобы уменьшить большое количество объектов до меньшего для удобства их последующей визуализации.
5. Задача обнаружения аномалий состоит в том, чтобы отделить аномалии от стандартных случаев.

Искусственный интеллект (ИИ) — обширная отрасль информатики, фокусирующаяся на создании интеллектуальных машин, способных выполнять интеллектуальные задачи.

Область искусственного интеллекта пересекается со многими другими областями, включая математику, статистику, теорию вероятностей, физику, обработку сигналов, машинное обучение, компьютерное зрение, психологию, лингвистику и науку о мозге.

Мотивация для развития технологий искусственного интеллекта заключается в том, что задачи, зависящие от множества переменных факторов, требуют очень сложных решений, которые трудно понять и трудно алгоритмизировать вручную. Программирование алгоритмов отнимает у разработчиков много времени [2].

Основные проблемы ИИ

1. Машинное обучение возможно только на основе массива данных. Это означает, что любые неточности в информации сильно влияют на конечный результат.
2. Интеллектуальные системы ограничены определённым видом деятельности. То есть интеллектуальная система, настроенная на выявление мошенничества в сфере налогообложения, не сможет обнаружить мошенничество в банковском секторе. Мы имеем дело с узкоспециализированными программами, которые все ещё далеки от человеческой многозадачности.
3. Интеллектуальные машины не являются автономными. Для обеспечения их «жизнедеятельности» необходима целая команда специалистов и большие ресурсы.

Приложения искусственного интеллекта

1. Распознавание речи: технология, которая использует обработку естественного языка для записи человеческой речи в виде текста.
2. Обслуживание клиентов: почти везде человеческие операторы заменяются онлайн-чат-ботами. Они могут ответить на частые вопросы по определённой теме.
3. Компьютерное зрение: данная технология позволяет компьютерам и системам извлекать значимую информацию из цифровых изображений, видеоматериалов и других визуальных данных и в дальнейшем принимать решения на основе этой информации.
4. Модули рекомендаций: алгоритмы искусственного интеллекта могут анализировать данные о поведении клиентов в прошлом и выявлять тенденции, которые помогут повысить эффективность стратегий перекрёстных продаж. Благодаря этому клиенты получают дополнительные рекомендации при оформлении заказов в интернет-магазине.
5. Автоматизация биржевой торговли: высокочастотные торговые платформы на основе искусственного интеллекта не только оптимизируют портфели акций, но и совершают тысячи и даже миллионы сделок без малейшего вмешательства человека.

Искусственные нейронные сети

Нейронная сеть — одно из направлений искусственного интеллекта, целью которого является моделирование аналитических механизмов, осуществляемых человеческим мозгом. Задачи, которые решает типичная нейронная сеть — классификация, прогнозирование и распознавание.

Нейронные сети используются для решения сложных задач, требующих аналитических вычислений, аналогичных тем, что делает человеческий мозг. Наиболее распространёнными областями применения нейронных сетей являются [3]:

1. Классификация — распределение данных по параметрам. Например, на входе даётся набор людей, и вам нужно решить, кому из них давать кредит, а кому нет. Эта работа может быть выполнена с помощью ней-

ронной сети, анализирующей такую информацию, как: возраст, платёжеспособность, кредитная история и т.д.

2. Прогнозирование — способность предсказать следующий шаг. Например, рост или падение акций, в зависимости от ситуации на фондовом рынке.
3. Распознавание в настоящее время является наиболее распространённым применением нейронных сетей. Он используется в Google при поиске фотографий или в камерах телефонов, когда он определяет положение вашего лица и выделяет его, и многое другое.

Искусственные нейронные сети — математические модели, созданные по аналогии с биологическими нейронными сетями. INS способны моделировать и обрабатывать нелинейные взаимосвязи между входными и выходными сигналами. Адаптивное взвешивание сигналов между искусственными нейронами достигается благодаря алгоритму обучения.

Для повышения производительности INS используются различные методы оптимизации. Оптимизация считается успешной, если INS может решить проблему за время, не превышающее установленные временные рамки.

INS моделируется с использованием нескольких слоёв нейронов. Структура этих слоёв называется архитектурой модели. Нейроны — отдельные вычислительные блоки, способные принимать входные данные и применять к ним некоторую математическую функцию, чтобы определить, стоит ли передавать эти данные дальше.

В простой трёхслойной модели первым слоем является входной слой, за которым следует скрытый слой, а затем выходной слой. Каждый слой содержит по крайней мере один нейрон. С усложнением структуры модели из-за увеличения количества слоёв и нейронов возрастает потенциал для решения задач INS. Если модель окажется слишком «большой» для этой задачи, оптимизировать ее до желаемого уровня может оказаться невозможным [4].

Модели часто характеризуются функцией активации. Он используется для преобразования взвешенных входных данных нейрона в его выходные данные. Существует множество различных преобразований, которые можно использовать в качестве функций активации.

INS — мощный инструмент для решения проблем. Однако, хотя математическая модель небольшого числа нейронов довольно проста, модель нейронной сети становится довольно запутанной по мере увеличения числа ее компонентов. Выбор INS для решения проблемы должен быть тщательно продуман, так как во многих случаях полученное окончательное решение невозможно разобрать на части и проанализировать, почему оно стало таким.

Глубокое обучение

Глубокое обучение используется для описания нейронных сетей и используемых в них алгоритмов, которые принимают «необработанные» данные. Эти данные обрабатываются прохождением через слои нейронной сети для получения выходных данных.

Неконтролируемое обучение — область, где работают методы глубокого обучения. Правильно настроенный INS может определять характеристики входных данных и получать результат обработки. Модель глубокого обучения способна находить способ обработки данных. В то время, когда система обучается, требования к вычислительной мощности, памяти и энергии для поддержания работы модели снижаются.

Глубокое обучение используется для решения задач и считается одной из инновационных технологий искусственного интеллекта. Существуют и другие виды обучения: контролируемое обучение и контролируемое обучение, которые отличаются введением дополнительного контроля человека над промежуточными результатами обучения нейронной сети обработке данных.

Теневое обучение — данный термин, используется для описания упрощённой формы глубокого обучения, при которой поиску ключевых характеристик данных предшествует обработка человеком и ввод в систему информации, специфичной для области, к которой относятся эти данные.

Подводя итог данной работы, можно сказать, что искусственный интеллект — одновременно наука, помогающая создавать «умные» машины, и способность компьютера учиться и принимать решения.

Искусственный интеллект превосходит традиционные алгоритмы, созданные программистами, потому что он обрабатывает данные и предо-

ставляет решения намного быстрее, но если люди могут расширить свое внимание, запоминание с помощью мнемоники и других тренировок мозга, то это работает по-другому [5].

Искусственный интеллект — мощный инструмент обработки данных и может находить решения сложных проблем быстрее, чем традиционные алгоритмы, написанные программистами. Методы INS и глубокого обучения могут помочь решить ряд различных проблем.

Машинное обучение — одна из областей искусственного интеллекта. МОД использует алгоритмы для анализа данных и вывода выводов.

Глубокое обучение — один из методов машинного обучения, при котором компьютер обучается без учителя, неявно используя данные.

К 2022 году прогнозируемый объем рынка искусственного интеллекта достигнет 52 миллиарда долларов.

Рынок искусственного интеллекта демонстрирует беспрецедентно высокие темпы роста — по некоторым оценкам, он увеличивается примерно на 30% ежегодно.

Список литературы

1. Корбут, А. М. Спектр искусственных интеллектов: от сильного ИИ к социальному ИИ / А. М. Корбут // История науки и техники. Музейное дело. периодическая таблица технологий: человеческий фактор: Материалы XIII Международной научно-практической конференции, Москва, 03–05 декабря 2019 года. — Москва: Федеральное государственное бюджетное учреждение культуры «Политехнический музей», 2020. — С. 520–521. — EDN SIEMVF.
2. Искусственный интеллект для науки и наука для искусственного интеллекта / К. В. Анохин, К. С. Новоселов, С. К. Смирнов [и др.] // Вопросы философии.— 2022.— № 3. — С. 93–105. — DOI 10.21146/0042–8744–2022–3–93–105. — EDN NBENRC.
3. Окунева, Н. В. Мировой рынок искусственного интеллекта его влияние искусственного интеллекта на облик рынка труда / Н. В. Окунева, Е. С. Туманова, И. А. Шипулина // Современный специалист-профессионал: теория и практика: Материалы 10-й международной науч-

ной конференции студентов и магистрантов, посвящённой 100-летию Финуниверситета в рамках IX Международного научного студенческого конгресса «Цифровая экономика: новая парадигма развития», Барнаул, 22–23 марта 2018 года / Под общей редакцией Т. Е. Фасенко, Д. В. Коханенко. — Барнаул: Типография «Графикс», 2018. — С. 13–16. — EDN YTBFQL.

4. Рязанов, С. И. Искусственный интеллект как множество — классификация искусственных интеллектов / С. И. Рязанов // Вузовская наука в современных условиях: сборник материалов 54-й научно-технической конференции: в 3 ч., Ульяновск, 27 января — 01 2020 года. — Ульяновск: Ульяновский государственный технический университет, 2020. — С. 72–75. — EDN GKDKDG.
5. Применение случайных чисел при проектировании информационных систем / М. К. Каторгин, Д. Ю. Селютин, А. И. Воробьева [и др.] // Современные информационные технологии в образовании, науке и промышленности: XX Международная конференция, XVIII Международный конкурс научных и научно-методических работ, Международный конкурс «Нейросетевой рисунок»: сборник трудов, Москва, 11–12 ноября 2021 года. — Москва: Общество с ограниченной ответственностью «Издательство «Экон-Информ», 2021. — С. 31–34. — EDN RJYVED.
6. Искусственный интеллект в технологии Интернета-вещей / Р. В. Жуков, В. С. Васильева, А. Г. Корысткина [и др.] // Современные информационные технологии в образовании, науке и промышленности: Сборник трудов конференций: XXII Международная конференция «Современные информационные технологии в образовании, науке и промышленности». XX Международный конкурс научных и научно-методических работ. VIII Международный конкурс «Научное школьное сообщество», Москва, 28–29 апреля 2022 года. — Москва: Общество с ограниченной ответственностью “Издательство “Экон-Информ”, 2022. — С. 32–39. — EDN QERJUP.

УДК 629.7.05

Краткий анализ алгоритма динамической системной модуляции для улучшения навигации беспилотных летательных аппаратов

Еремина Виктория Владимировна

кандидат физико-математических наук, доцент кафедры Информационных и управляющих систем Амурского государственного университета

Мокронос Кирилл Константинович

аспирант Амурского государственного университета

***Аннотация**: В данной статье проводится анализ метода избегания преград через применение динамической системной модуляции. Эта часть исследования фокусируется на изучении эффективности и надежности использования этого метода для улучшения производительности и надежности исходного алгоритма 3DVFH+.*

***Abstract**: This paper analyzes a method of obstacle avoidance through the use of dynamic system modulation. This part of the research focuses on investigating the effectiveness and robustness of using this method to improve the performance and robustness of the original 3DVFH+ algorithm.*

***Ключевые слова**: 3DVFH, избегание препятствий, динамическая система, модуляция, беспилотные летательные аппараты.*

***Keywords**: 3DVFH+, obstacle avoidance, dynamic system, modulation, unmanned aerial vehicles.*

Введение

В первой части статьи были обсуждены широко используемые методы автоматического избегания преград [1], применяемые в программировании беспилотных летательных аппаратов (БПЛА) и базирующиеся на алгоритме 3DVFH+ [2–4]. Этот алгоритм активно используется в навигации и управлении БПЛА благодаря его способности эффективно создавать безопасные маршруты вокруг препятствий. Однако все еще существуют трудности, связанные с избеганием препятствий в реальном времени,

планированием маршрута и навигацией. Алгоритм динамической системной регулировки (DSM) представляет собой потенциальное решение этих проблем, предлагая более адаптивный и гибкий подход к автономному управлению БПЛА.

Алгоритм динамической системной модуляции

Алгоритм динамической системной модуляции [5], сочетает низкую вычислительную сложность алгоритма искусственного потенциального поля и решает проблему локального минимума. Скорость динамической системы модулируется матрицей модуляции, чтобы устранить проникающую составляющую скорости около поверхности препятствия. Алгоритм сохраняет сходимость системы и предотвращает столкновения. Существует алгоритм обхода препятствий на основе DSM, использующий относительное расстояние между роботом и препятствием [6], а векторное поле функции Ляпунова [7] модулируется для получения желаемого поля скорости слежения. Так же в систему управления DSM было добавлено управление с прогнозированием моделей для оптимизации траектории движения [8].

Рассмотрим переменную состояния $\xi \in R^d$, которая определяет состояние роботизированной системы. Его временная эволюция может регулироваться либо автономной динамической системой (1), неизменной во времени, либо неавтономной динамической системой (2), изменяющейся во времени:

$$\dot{\xi} = f(\xi), f : R^d \mapsto R^d; \quad (1)$$

$$\dot{\xi} = f(t, \xi), f : R^+ \times R^d \mapsto R^d, \quad (2)$$

где $f(\xi)$ – непрерывная функция, R^d – декартово произведение d копий множества вещественных чисел. Учитывая начальную точку $\{\xi\}_0$, движение робота во времени можно вычислить путем рекурсивного интегрирования $f(\xi)$:

$$\{\xi\} = \{\xi\}_{t-1} + f(\xi)\delta t\,, \tag{3}$$

где δt – шаг интегрирования по времени.

Далее можно вызвать модуляцию нашего общего движения из-за наличия препятствия. Рассмотрим d-мерный гиперсферический объект с центром в точке ξ^o и радиусом r^o. Объект создает модуляцию во всем пространстве состояний робота, которая передается через нелинейную функцию $\phi^s(\xi;\xi^o,r^o): R^d \mapsto R^d$ следующим образом:

$$\phi^s(\xi;\xi^o,r^o) = \left(1 + \frac{(r^o)^2}{(\xi-\xi^o)^T(\xi-\xi^o)}\right)(\xi-\xi^o). \tag{4}$$

Чтобы определить, как ϕ модулирует скорость робота, вычисляется якобиан, который дает:

$$M^s(\xi;\xi^o,r^o) = \nabla\phi^s(\xi;\xi^o,t^o). \tag{5}$$

Для упрощения обозначений выразим модуляцию в системе отсчета с центром в объекте и определим $\tilde{\xi} = \xi - \xi^o$:

$$M^s(\tilde{\xi};r^o) = I + \left(\frac{r^o}{\tilde{\xi}^T\tilde{\xi}}\right)^2\left(\tilde{\xi}^T\tilde{\xi}I - 2\tilde{\xi}\tilde{\xi}^T\right), \tag{6}$$

где I – единичная матрица, M^s – динамическая матрица модуляции.

Окончательную модель уклонения от сферических препятствий в реальном времени можно получить, применив матрицу динамической модуляции к исходной динамической системе, заданной уравнениями (1) и (2):

$$\dot{\xi} = M^s(\tilde{\xi};r^o)f(\xi), \tag{7}$$

где $M^s(\tilde{\xi};r^o)$ – коэффициент модуляции, который локально деформирует исходную динамику f таким образом, что робот не сталкивается с препятствием.

На рисунке 1 показано влияние модуляции, вызванной таким сферическим объектом, на двухмерные и трехмерные представления. Как видно, в обоих случаях траектория отклоняется правильно и проходит препятствие.

Теперь рассмотрим дугообразные препятствия. Предположим, что существует непрерывная функция $\Gamma\left(\tilde{\xi}\right)$, которая выполняет модуляцию системы на основе текущих состояний или параметров, проектирует R^d в R. Функция $\Gamma\left(\tilde{\xi}\right)$ имеет непрерывные частные производные первого порядка и монотонно возрастает с $\left\|\tilde{\xi}\right\|$. Кривые уровня типа $\Gamma\left(\tilde{\xi}\right) = c, \forall c \in R^+$ окружают выпуклую область. По построению на поверхности препятствия выполняется соотношение:

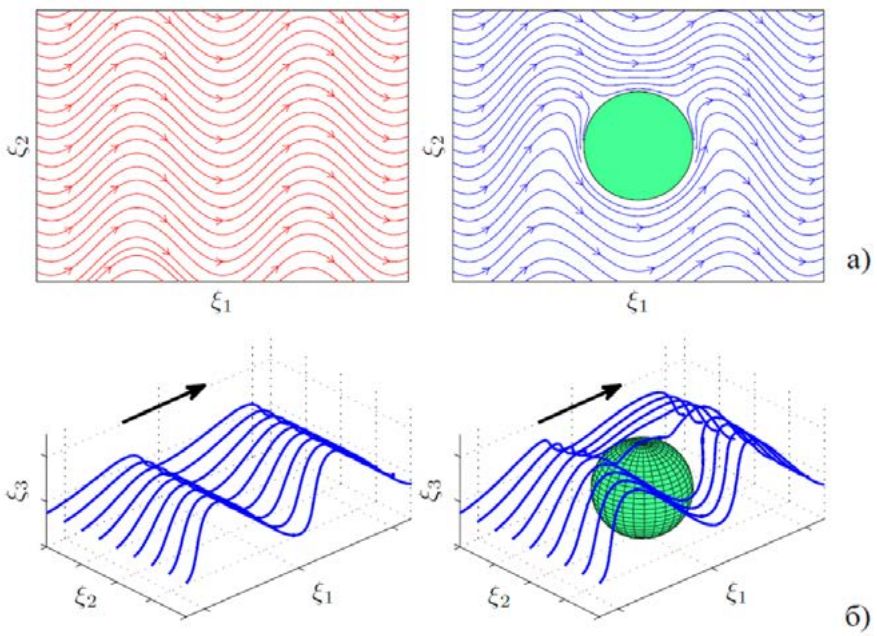

Рисунок 1. **Эффект модуляции, вызванной сферическим препятствием: а) — двумерное представление; б) — трехмерное представление**

$$\Gamma\left(\tilde{\xi}\right)=1. \tag{8}$$

Например, $\Gamma\left(\tilde{\xi}\right):\sum_{i=1}^{d}\left(\tilde{\xi}_i / a_i\right)^2=1$ соответствует d-мерному эллипсоиду с длинами осей a_i. Можно разделить пространство, на три области X^o, X^b, X^f, чтобы различать точки внутри препятствия, на его границе и вне препятствия соответственно:

$$X^o=\left\{\xi\in R^d:\Gamma\left(\tilde{\xi}\right)<1\right\}; \tag{9}$$

$$X^b=\left\{\xi\in R^d:\Gamma\left(\tilde{\xi}\right)=1\right\}; \tag{10}$$

$$X^f=\left\{\xi\in R^d:\Gamma(\tilde{\xi})>1\right\}. \tag{11}$$

В каждой точке $\xi^b\in X^b$, на внешней поверхности препятствия возможно вычислить касательную гиперплоскость, определяемую равенством как его нормальный вектор $n\left(\tilde{\xi}^b\right)$:

$$n\left(\tilde{\xi}^b\right)=\left[\frac{\partial\Gamma\left(\tilde{\xi}^b\right)}{\partial\xi_1^b}\cdots\frac{\partial\Gamma\left(\tilde{\xi}^b\right)}{\partial\xi_d^b}\right]^T. \tag{12}$$

В более широком смысле можно вычислить гиперплоскость отклонения в каждой точке $\xi\in X^f$ вне препятствия с нормалью:

$$n\left(\tilde{\xi}\right)=\left[\frac{\partial\Gamma\left(\tilde{\xi}\right)}{\partial\xi_1}\cdots\frac{\partial\Gamma\left(\tilde{\xi}\right)}{\partial\xi_d}\right]^T. \tag{13}$$

Каждая точка на гиперплоскости отклонения может быть выражена как линейная комбинация набора линейно независимых векторов. Эти векторы составляют основу гиперплоскости отклонения (рис. 2). Для упрощения отображения системы уравнений под набор векторов $e^1,\ldots,e^{d-1}$ определим функцию выбора знака:

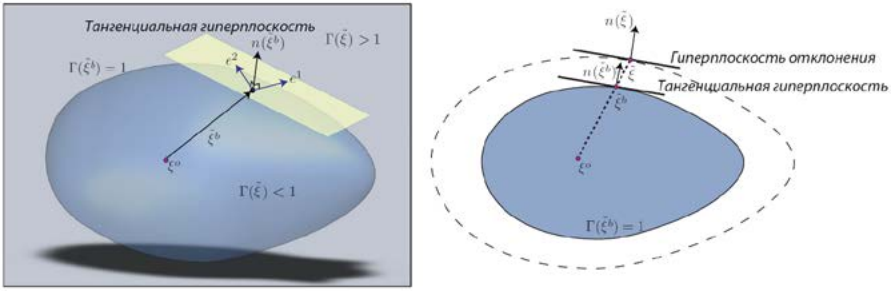

Рисунок 2. **Тангенциальная гипперплоскость и гипперплоскость отклонения**

$$s(a,b,c)=\begin{cases}-1\\ 1\\ 0\end{cases}, \tag{14}$$

где значения -1, 1 и 0 соответствуют условиям $j=1$, $j=i\neq 1$ и $j\neq i\neq 1$.

Тогда один конкретный набор таких векторов $e^1,\ldots,e^{d-1}$ будет равен:

$$e_j^i\left(\tilde{\xi}\right)=s(a,b,c)\frac{\partial\Gamma\left(\tilde{\xi}\right)}{\partial\xi_1}, \tag{15}$$

где e_j^i соответствует j-й компоненте i-го базисного вектора, при условии $i\in 1..d-1$, $j\in 1..d$.

Как и в случае сферического объекта, матрица модуляции, задается выражением:

$$M\left(\tilde{\xi}\right)=E\left(\tilde{\xi}\right)D\left(\tilde{\xi}\right)E\left(\tilde{\xi}\right)^{(-1)}. \tag{16}$$

Матрица динамической модуляции $M\left(\tilde{\xi}\right)$ распространяет влияние препятствия на траекторию движения. Форма уравнения (16) инвариантна к выбору базиса $e^1,\ldots,e^{d-1}$. Кроме того, матрица базисного вектора обратима в $R^d\setminus\xi^o$. В опорной точке препятствия ξ^o гиперплоскость

отклонения не определена, однако это не вызывает никаких проблем, так как ξ^o – это точка внутри препятствия. Кроме того, поскольку $\Gamma\left(\tilde{\xi}\right)$ монотонно возрастает с $\left\|\tilde{\xi}\right\|$, матрица собственных значений и, как следствие, матрица динамической модуляции сходятся к единичной матрице по мере увеличения расстояния до препятствия. Следовательно, влияние матрицы динамической модуляции максимально на границах препятствия и исчезает в точках, удаленных от него.

Подобно уклонению от препятствий гиперсферы, заданному уравнением 7, можно применить модуляцию, заданную уравнением 16 на первоначальную траекторию движения *f*, которая дает:

$$\dot{\tilde{\xi}} = M\left(\tilde{\xi}\right) f\left(\xi\right). \tag{17}$$

На рисунке 3 показано влияние модуляции на поле движения при наличии различных препятствий.

Анализ дискретного движения робота

В предыдущем разделе было показано, как матрица динамической модуляции $M\left(\tilde{\xi}\right)$ может использоваться для изменения движения робота таким образом, чтобы он не сталкивался с препятствием. Однако во многих экспериментах с роботами, он должен не только избежать всех препятствий, но и достичь цели, которая далее обозначается ξ^*. Необходимо, чтобы измененное движение сохраняло свойство сходимости исходной динамики, но при этом гарантировало, что движение не проходит сквозь объект.

Предположим, что *d*-мерная глобально асимптотически устойчивая автономная или неавтономная ДС определяется уравнением 1 или уравнением 2. Глобальная устойчивость *f* требует, чтобы скорость обращалась в ноль только в целевой точке ξ^*, т.е. $f\left(\xi^*\right) = 0$ для автономных ДС и $\lim_{t\to\infty} f\left(t, \xi^*\right) = 0$ для неавтономных ДС. Когда *f*

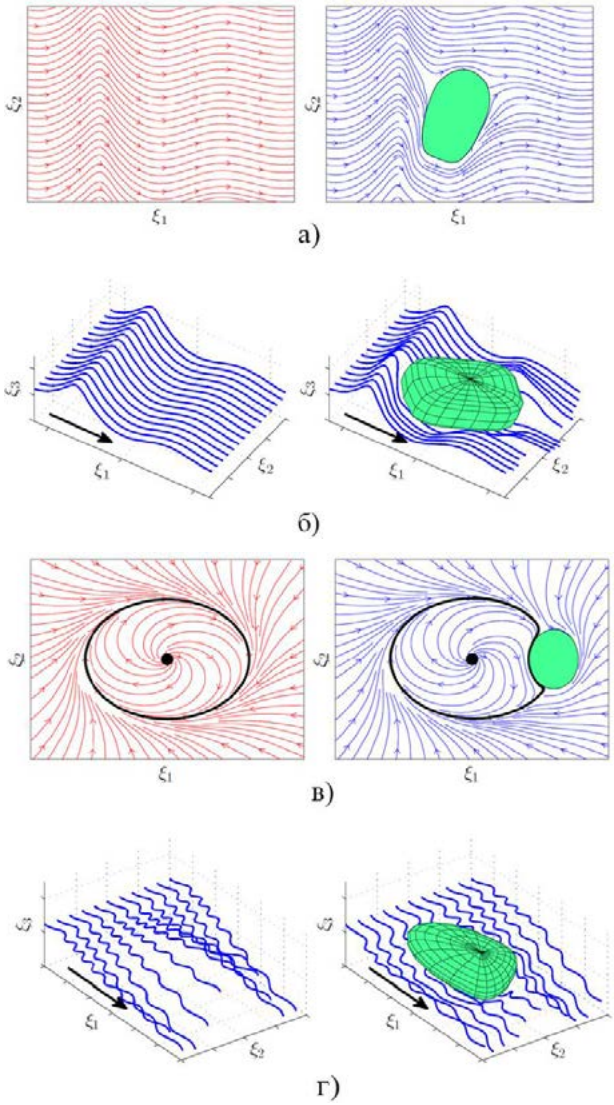

Рисунок 3. **Изменение исходной траектории движения с помощью матрицы модуляции для: а) — двухмерного представления; б) — трехмерного представления; в) — думерного стабильного предельного цикла; г) — трехмерного не автономного представления**

модулируется динамической матрицей $M\left(\tilde{\xi}\right)$, ξ^* остается точкой равновесия, поскольку скорость по-прежнему обращается в ноль в конце маршрута, т.е. $M\left(\xi^*-\xi^o\right)f\left(\xi^*\right)=0$ для автономной динамической системы и $\lim_{t\to\infty} M\left(\xi^*-\xi^o\right)f\left(t,\xi^*\right)=M\left(\xi^*-\xi^o\right)\lim_{t\to\infty} f\left(t,\xi^*\right)$ для не автономных динамических систем.

Однако при наличии препятствия цель может оставаться не единственной точкой равновесия системы. Другие возможные точки равновесия могут быть созданы из-за члена модуляции $M\left(\tilde{\xi}\right)$. Эти точки можно вычислить, взглянув на нулевое пространство $M\left(\tilde{\xi}\right)$. Для всех $\xi\in X^f$, матрица $M\left(\tilde{\xi}\right)$ имеет полный ранг и, следовательно, ξ^* будет единственной точкой равновесия в X^f. Только на границах препятствия, т.е. $\xi^b\in X^b$, $M\left(\tilde{\xi}^b\right)$ теряет один ранг, что дает ряд ложных точек равновесия. На самом деле эти ложные точки равновесия $\xi^s\in X^b$ генерируются, когда существует коллинеарность между скоростью и вектором нормали в граничных точках:

$$n\left(\xi^s\right)^T\frac{f\left(\xi\right)}{\left\|f\left(\xi\right)\right\|}=\pm 1; \tag{18}$$

$$\Gamma\left(\tilde{\xi}^s\right)=1, \tag{19}$$

где $n\left(\xi^s\right)^T$ – единичный вектор нормали гиперплоскости в точке ξ^s.

В зависимости от функции *f* эти точки равновесия могут быть либо седловыми, либо локальными минимумами.

Вычисление этого набора точек равновесия не всегда возможно. Однако возможно упростить задачу, заметив, что, поскольку все точки равновесия появляются исключительно на границе препятствия, можно избежать столкновения, используя некоторые внешние механизмы. На рисунке 4 показаны два примера, где робот обнаружив, что движение остановилось на внешней поверхности (границе) препятствия (т.е. в

точке равновесия), применяет малое возмущение по любому из базисных векторов $e^1,\ldots,e^{d-1}$. Все эти векторы определяют направления, обеспечивающие удаление направления движения робота от препятствия. Если точка равновесия является седловой, алгоритм завершается за одну итерацию.

Если же это локальный минимум, то препятствие очерчивается вдоль направления базисного вектора e^i, тем самым предусмотривается некоторый запас безопасности вокруг препятствий, чтобы БПЛА оставался на безопасном расстоянии от объекта и с меньшей вероятностью могло произойти столкновение. Это происходит до тех пор, пока препятствие не покинет область притяжения локального минимума. Положительная скалярная величина α управляет амплитудой движения вдоль базисного вектора e^i.

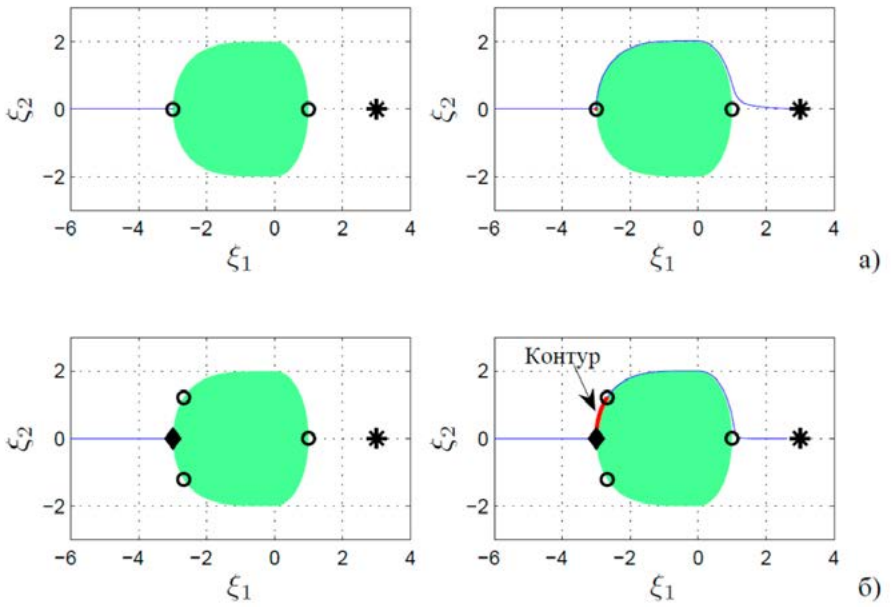

Рисунок 4. **Иллюстрация обхода возможных точек равновесия на границе препятствия: а) — при наличии седловой точки; б) — при наличии локального минимума**

Значение α следует выбирать, находя компромисс между точностью, безопасностью и скоростью движения. При большом шаге интегрирования по времени δt следует использовать малое значение α, чтобы уменьшить ошибку отклонения (из-за интегрирования) от желаемой траектории при оконтуривании препятствия. Кроме того, поскольку контурирование происходит на внешней поверхности препятствия, по соображениям безопасности обычно следует избегать выбора высокого значения для α. Очень маленькое значение α также не рекомендуется, так как оно значительно замедляет скорость контурной обработки.

Заключение

В ходе исследования алгоритма динамической системной модуляции (DSM) были выявлены значительные преимущества его применения в контексте навигации беспилотных летательных аппаратов (БПЛА). Основным достоинством DSM является его способность обеспечивать более гибкое и динамичное управление, что критически важно для эффективного избегания препятствий в сложных и меняющихся условиях.

Более того, этот алгоритм демонстрирует отличную совместимость с алгоритмом 3DVFH+, который уже широко используется для программирования БПЛА. Интеграция DSM с 3DVFH+ обещает значительное улучшение в производительности и надежности систем автоматического уклонения от препятствий.

В следующей статье будет представлен подробный анализ и результаты модификации, объединяющей эти два алгоритма.

Список литературы

1. Еремина В.В., Мокронос К. К. Модернизация типового алгоритма уклонения от препятствий. I // Информатика и системы управления.— 2022.— № 1(71). — С. 27–40.
2. Khansari-Zadeh S.M., Billard A. A dynamical system approach to real-time obstacle avoidance // Autonomous Robots.— 2012. — Vol. 32, № 4. — P. 433–454.

3. Saveriano M, Lee D. Distance based dynamical system modulation for reactive avoidance of moving obstacles. // IEEE international conference on robotics and automation (ICRA).— 2014. — P. 5618–5623.
4. Wang H., Lyu W., Yao P. Three-dimensional path planning for unmanned aerial vehicle based on interfered fluid dynamical system. // Chinese Journal of Aeronautics.— 2015. — Vol. 28, № 1. — P. 229–239.
5. Yao P., Wang H., Su Z. UAV feasible path planning based on disturbed fluid and trajectory propagation // Chinese Journal of Aeronautics.— 2015. — Vol. 28, № 4. — P. 1163–1177.
6. Julier S.J., Uhlmann J. K. Unscented filtering and nonlinear estimation. // Proceedings of the IEEE.— 2004.— № 92(3). — P. 401–422.
7. Wang, N., Dai, F., Liu, F., Zhang, G. Dynamic Obstacle Avoidance Planning Algorithm for UAV Based on Dubins Path. // Algorithms and Architectures for Parallel Processing. ICA3PP 2018. Lecture Notes in Computer Scienceю — 2018 — Vol. 11335.
8. Xu Z., Zhan X., Chen B., Xiu Y., Yang C., Shimada K. A real-time dynamic obstacle tracking and mapping system for UAV navigation and collision avoidance with an RGB-D camera // IEEE International Conference on Robotics and Automation (ICRA) — 2023 — P. 10645–10651.

УДК 004

Анализ моделей и алгоритмов обработки информации для оптимизации трейдинга на электронных биржах

Аверченков Андрей Владимирович

доктор технических наук, профессор кафедры Информационных технологий Брянского государственного инженерно-технологического университета

Пустовой Сергей Ильич

аспирант Брянского государственного инженерно-технологического университета

***Аннотация**: В статье рассказывается про растущий интерес к электронной биржевой торговле из-за технологического прогресса и увеличения доступа к информации,*

про возможности автоматизации торговли и сокращения рисков с помощью искусственного интеллекта как опытным, так и новым трейдерам. Рассмотрены авторефераты диссертаций молодых ученых, связанные с разработкой моделей и алгоритмов, а также другими способами оптимизации торговли на электронных биржах.

***Abstract**: The article tells about the growing interest in electronic exchange trading due to technological progress and increasing access to information, about the possibilities of trade automation and risk reduction with the help of artificial intelligence for both experienced and new traders. Abstracts of dissertations of young scientists related to the development of models and algorithms, as well as other ways to optimize trading on electronic exchanges are considered.*

***Ключевые слова**: искусственный интеллект, трейдинг, электронная биржа, оптимизация, автоматизация.*

***Keywords**: artificial intelligence, trading, electronic exchange, optimization, automation.*

С развитием технологий и увеличением доступности информации, все больше людей обращают внимание на возможности, которые предлагает торговля на электронных биржах. Одной из причин растущего интереса к трейдингу является его доступность. Сегодня, для того чтобы начать торговать на бирже, не нужно иметь большой начальный капитал или специальное образование. Достаточно иметь компьютер или смартфон с доступом в интернет, открыть счет на электронной площадке, и вы можете начать торговлю. Второй причиной является возможность получения высокой доходности. В отличие от традиционных форм инвестирования, таких как банковские депозиты или облигации, трейдинг может принести значительно большую прибыль. Но вместе с возможными высокими доходами идут и высокие риски. Для того чтобы минимизировать риски и оптимизировать процессы торговли трейдеры стали активно внедрять возможности искусственного интеллекта (ИИ) в торговлю на бирже. ИИ может помочь в управлении рисками, анализируя различные сценарии и предсказывая возможные потери. Это помогает трейдерам управлять своими инвестициями более эффективно.

Искусственный интеллект предлагает мощные методы и алгоритмы обработки информации, которые могут быть использованы для автоматизации биржевого трейдинга. Под ИИ понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека

и при выполнении конкретных задач получать результаты, сопоставимые с результатами его интеллектуальной деятельности. На сегодняшний день ИИ уже широко используется участниками российского финансового рынка в различных бизнес-процессах: для взаимодействия с клиентами, управления рисками, аналитики, мониторинга и совершения операций и так далее. При этом потенциал дальнейшего расширения использования ИИ финансовыми организациями представляется значительным. ИИ может повышать эффективность финансовых организаций, а также частных трейдеров. По оценкам экспертов, мировой финансовый сектор находится в числе отраслей, которые наиболее активно внедряют технологии ИИ.

Подавляющее большинство трейдеров теряют все свои средства на рынках из-за их психологической неподготовленности и малого опыта. Многие не готовы посвящать все своё время трейдингу и переживать убытки, но ищут дополнительный доход в этой сфере и хотели бы пользоваться услугами грамотного управляющего или использовать надёжные советы. Развитие автоматизированной торговли открывает новые возможности для научных исследований. Это включает в себя разработку новых алгоритмов и моделей машинного обучения, изучение влияния автоматизации на рынок, а также применение этих технологий в управлении инвестициями и рисками.

Автоматизация торговли позволяет ускорить процесс принятия решений, что критически важно в условиях быстро меняющегося рынка. Автоматизированные системы способны обрабатывать значительно больше информации, чем человек, и делать это более эффективно, может помочь снизить эмоциональный фактор, который часто мешает трейдерам принимать рациональные решения. В научных исследованиях активно изучаются методы и алгоритмы, позволяющие создавать автоматизированные системы торговли, способные анализировать большие объемы данных, прогнозировать поведение рынка и принимать решения о сделках.

Одна из таких работ представлена Николаевой Юлией Викторовной. В своей диссертационной работе «методы и алгоритмы интеллектуальной системы поддержки принятия решений трейдеров финансовых рынков», она попыталась повысить эффективность принятия управленческих решений участников рынка, за счет применения интеллектуальной системы

поддержки принятия решений (ИСППР) трейдеров финансовых рынков. Юлия Викторовна разработала методики поддержки принятия решений трейдера по направлению сделки с финансовым инструментом, основанные на нейросетевой методологии с применением методов технического, фундаментального анализа, эконометрического моделирования, и алгоритма ее реализации в системе поддержки принятия решений. Идея создания методики поддержки принятия решений трейдера основана на эмуляции анализа трейдером привычных ему данных: значений по техническим индикаторам RSI, MACD, значений по прогнозной модели GARCH, знание о влиянии на волатильность рынка приближающихся экономических событий. По полученным данным трейдер на основе своих знаний и опыта делает вывод о текущей рыночной ситуации, и с учетом ожидаемой прибыли вступает в сделку. ИСППР, аналогично анализирует все полученные данные и выдает рекомендацию по направлению сделки. В качестве классификатора используется многослойный персептрон.

Данная система поддержки принятия решений может использоваться при реальной торговле на финансовых рынках профессиональными трейдерами. Разработанный программный продукт «НейроПрофит» обеспечивает трейдера рекомендацией по покупке-продаже финансовых инструментов с достоверностью в 83%. При использовании ИСППР «НейроПрофит» трейдер может получать до 137% ожидаемой от сделки, открытой по рекомендации системы, прибыли. Очень важно, что система способна ориентироваться на анализ вышедших экономических новостей, волатильность после выхода которых может составлять десятки процентов. Но большинство неопытных трейдеров недавно пришедших на рынки не смогут использовать данную систему в полной мере и вероятнее всего по прежнему будут нести убытки, поскольку система основана на алгоритмах и моделях машинного обучения, они не подвержены эмоциональному воздействию и могут принимать рациональные решения, основанные на данных, которые с большей долей вероятности будут правильными, но так как все основные действия при заключении сделок будут проводиться неопытным трейдером использующий данную ИСППР, то человеческий фактор снова возвращается. Ещё одним минусом является сложность в использовании и настройке она потребует специальных знаний и опыта.

Ещё одна диссертационная работа, затрагивающая обсуждаемые вопросы — «математический метод и алгоритмы фрактального анализа динамики финансовых рынков». В ней автор, Неганова Елена Вячеславовна, предлагает использовать фрактальные свойства рынка, методы реконструкции временных рядов и анализ долговременной памяти для прогнозирования поведения цен на различные активы. Это позволяет учитывать нелинейные и непрерывные изменения цен, которые могут быть упущены эконометрическими моделями. Такой подход может быть особенно полезен в условиях рыночной нестабильности и волатильности, когда традиционные модели могут оказаться недостаточно точными.

Недостатком данной работы может быть сложность применения физических и математических моделей финансового рынка в реальных условиях. Требуется высокий уровень математической подготовки и специализированные знания в области финансов, чтобы правильно применять эти модели для прогнозирования и анализа рыночной динамики. Кроме того, такие модели могут быть менее интерпретируемыми для неспециалистов, что может затруднить их принятие решений на основе прогнозов, полученных с их помощью. Данная работа предлагает новый подход к моделированию финансового рынка, но ее применение может быть вызовом для практиков и требует дополнительного изучения и практического опыта для эффективного использования.

Тема электронной биржевой торговли и применения искусственного интеллекта в этой области остается малоизученной. Дальнейшие исследования и разработки в этом направлении могут привести к новым инновационным методам оптимизации торговли на электронных биржах и улучшению результатов трейдеров.

Список литературы

1. Банк России. Применение искусственного интеллекта на финансовых рынках // Центральный банк РФ, 2023. С. 52.
2. Ассоциация ФинТех (05.10.2023). Искусственный интеллект — основа для создания финансовых услуг нового поколения // Ассоциация ФинТех, 2023. С. 80.

3. Николаева Ю. В. Методы и алгоритмы интеллектуальной системы поддержки принятия решений трейдеров финансовых рынков // Автореферат, Брянск 2018. С. 19.
4. Неганова Е. В. Математический метод и алгоритмы фрактального анализа динамики финансовых рынков // Автореферат, Самара 2012. С. 20.
5. Ассоциация ФинТех (23.08.2023). Искусственный интеллект — основа для создания финансовых услуг нового поколения // Ассоциация ФинТех, 2023.

Журнал «Научный аспект №11 2023»

Эл. почта редакции: public@na-journal.ru

Подробнее на сайте: https://na-journal.ru