НАУЧНЫЙ АСПЕКТ

na-journal.ru

2023

№12

ТОМ 30

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 № 12 2023. – Самара: Изд-во ООО «Аспект», 2023 . – Т30 . – 134 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 17.01.2024

Бумага ксероксная. Печать оперативная. Заказ № .
Формат 60×84 /16. Объем 8,04 п.л. Тираж 100 экз.

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

Содержание

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004

Влияние искусственного интеллекта на рынок труда: способы решения проблем

Чжан Ясюань

студент Университета Шихэцзы (Китай)

***Аннотация**: ИИ стремительно меняет образ жизни и профессиональные привычки, проникая во множество сфер деятельности и рынок труда в целом. В рамках данного исследования будет рассмотрен вопрос о возможном влиянии ИИ на будущие рабочие места и рынок труда. В процессе исследования будут изучены степень интеграции ИИ в разные сферы и возможные результаты такого роста для рынка труда. Кроме того, будут затронуты этические аспекты использования ИИ и его воздействие на трудовые ресурсы. Задача исследования — предложить решения, которые позволят обеспечить плавный переход для сотрудников и бизнеса с учётом интересов всех заинтересованных сторон.*

***Abstract**: AI is rapidly changing lifestyles and professional habits, penetrating many fields of activity and the labor market in general. This research will examine the possible impact of AI on future jobs and the labor market. The research will examine the extent to which AI is integrating into different fields and the possible results of this growth on the labor market. In addition, the ethical aspects of the use of AI and its impact on the labor force will be touched upon. The aim of the study is to propose solutions that will enable a smooth transition for employees and businesses while taking into account the interests of all stakeholders.*

***Ключевые слова**: искусственный интеллект (ИИ), рынок труда, автоматизация, перспективы, этика.*

***Keywords**: artificial intelligence (AI), labor market, automation, prospects, ethics.*

Искусственный интеллект (ИИ) — быстро развивающаяся область, которая в последние годы вмешивается в образ жизни людей, в том числе меняет рабочие процессы. Интеграция ИИ в различные отрасли, такие как здравоохранение, финансы и розничная торговля, принесла множе-

ство преимуществ, включая повышение эффективности, точности и производительности. Однако по мере внедрения искусственного интеллекта в мировую экономику возникают опасения по поводу его потенциального воздействия на рынок труда и будущую занятость.

Применение искусственного интеллекта в сфере труда стало предметом многочисленных обсуждений, и эксперты прогнозировали как положительные, так и отрицательные результаты для работников и предприятий. С одной стороны, ИИ обладает потенциалом для автоматизации рутинных задач, позволяя работникам сосредоточиться на творческой деятельности, приносящей пользу [1]. Это может привести к повышению эффективности и производительности, а также к созданию новых рабочих мест в таких областях, как анализ данных и разработка искусственного интеллекта [2].

С другой стороны, искусственный интеллект может вытеснить определенные рабочие места, особенно в таких отраслях, как производство и розничная торговля, где автоматизация уже начала внедряться. Такое развитие событий может создать новые проблемы для работников, особенно с ограниченными профессиональными навыками и образованием, и усугубить существующее неравенство на рынке труда.

Более того, интеграция ИИ в сферу труда поднимает важные этические вопросы, такие как ответственность предприятий и государства за регулирование процесса перехода к использованию соответствующих технологий, потенциальная потеря рабочих мест и доходов, а также влияние на социальное и экономическое неравенство [3].

В свете стремительных изменений на рынке труда в эпоху ИИ важно осознавать проблемы, которые вместе с тем могут возникнуть, и принимать взвешенные политические решения, способные обеспечить плавный переход для сотрудников и бизнеса.

Итак, обозначим потенциальные риски, которые могут возникнуть с распространением ИИ в сферу труда. С экономической точки зрения существует концепция технологической безработицы, которая связана с сокращением работников из-за достижений в области технологий. Эта теория основана на классической теории рынка труда, которая предсказывает, что достижения в области технологий приведут к повышению производительности, но также приведут к безработице [4].

С точки зрения этики, необходимо выделить важность понимания морально-этических последствий внедрения искусственного интеллекта и автоматизации для будущего сферы труда. Это включает в себя обеспечение справедливого отношения к работникам и равного распределения выгод от технологических достижений между всеми заинтересованными сторонами.

Несмотря на то, что внедрение ИИ и автоматизация процессов повышает эффективность труда и производительность, нельзя игнорировать возникающие описанные выше проблемы. Для этого государственному и промышленному секторам следует инвестировать в программы переподготовки для поддержки работников, которые были вытеснены искусственным интеллектом и автоматизацией. Это поможет обеспечить работников навыками, необходимыми для работы в будущем.

Кроме того, работодателям следует уделять приоритетное внимание разработке программ обучения для своих работников, чтобы помочь им идти в ногу с быстрым темпом технологических изменений. Это поможет работникам адаптироваться к новым технологиям и сохранять конкурентоспособность на рынке труда.

В то же время, политическим деятелям следует учитывать этические последствия, которые могут быть вызваны повсеместной интеграцией технологий ИИ и автоматизацией. Им необходимо предпринимать шаги для обеспечения достойного отношения к работникам. Это включает в себя обеспечение справедливого распределения преимуществ технологии между всеми заинтересованными сторонами.

И наконец, необходимо проводить дальнейшие исследования, чтобы лучше понять влияние искусственного интеллекта на конкретные отрасли и профессии. Это поможет государству и работодателям принимать взвешенные решения о том, как лучше всего готовить людей к будущей работе.

Список литературы

1. Bataev A. V., Gorovoy A. A., Mottaeva A. B. Evaluation of the future development of the digital economy in Russia // Proceedings of the 32nd International Business Information Management Association Conference, IBIMA

2018 — Vision 2020: Sustainable Economic Development and Application of Innovation Management from Regional Expansion to Global Growth. 2018.
2. Фрей К., Осборн М. (2018). Будущее занятости: Что ожидает рабочие места в эру автоматизации. Альпина Паблишер.
3. Полосков С. С., Желтенков А. В., Моттаева А. Б Методические основы мониторинга инновационного потенциала высокотехнологичных наукоемких предприятий // Экономика и предпринимательство. 2018. № 4 (93).
4. Брайнджольссон Э., Макафи Э. (2018). Второй век машин: Как технологии преображают бизнес, экономику и нашу жизнь. Манн, Иванов и Фербер.

УДК 004

Этические аспекты применения искусственного интеллекта: обозначение проблемы и примеры в социуме

Чжан Ясюань

студент Университета Шихэцзы (Китай)

***Аннотация**: В последние годы искусственный интеллект продемонстрировал значительный рост и развитие. Применение технологий ИИ неотрывно связано с прогрессом общества, они проникают в производственный процесс и в повседневную жизнь. При этом ИИ, как новая цифровая технология, требует адаптации механизмов контроля и регулирования. Как и любая инновация, технология ИИ подразумевает возникновение рисков, в том числе социальных. Ввиду быстрого развития технологий ИИ для защиты прав людей и обеспечения безопасности необходимо формировать новую государственную политику, а также способствовать установлению этических норм ИИ. В данной статье рассматриваются вопросы этики, такие как: этика прав человека, информационная этика и безопасность в контексте использования ИИ.*

***Abstract**: Artificial intelligence has shown significant growth and development in recent years. The application of AI technologies is inextricably linked to the progress of society; they are penetrating the production process and everyday life. At the same time, AI, as a new digital technology, requires adaptation of control and regulation mechanisms. Like any innovation,*

AI technology implies risks, including social risks. In view of the rapid development of AI technology, new public policies need to be formed to protect people's rights and ensure safety, and to promote the establishment of AI ethics. This article discusses ethical issues such as human rights ethics, information ethics and security in the context of AI utilization.

***Ключевые слова**: искусственный интеллект (ИИ), риски, этические проблемы, права человека.*

***Keywords**: artificial intelligence (AI), risks, ethical issues, human rights.*

В последние годы одной из наиболее обсуждаемых тем является технология искусственно интеллекта (ИИ, AI). Несмотря на это, до сих пор нет устоявшегося определения термина. Однако ИИ можно определить как область науки, которая занимается разработкой интеллектуальных систем с использованием таких дисциплин, как информатика, линейная алгебра, статистика и анализ данных [1]. Она также исследует вопросы, связанные с философскими и этическими аспектами использования таких систем. Системы, работающие на основе технологий ИИ, могут применяться для выполнения различных функций, включая распознавание речи, образов, прогнозирование исходов, контроль процессов и т.д. Тем не менее, наряду с преимуществами ИИ, существуют и определенные риски, связанные с его применением. Это включает потенциальную угрозу безопасности данных, возможность ошибок в принятии решений и прочее. Рассмотрим существенную проблему, связанную с распространением искусственного интеллекта в социум — нарушение морально-этических норм [2].

Существующие проблемы использования ИИ можно рассматривать в широком смысле (в масштабах целого общества, человечества) и в узком (отдельные общности, индивиды). К глобальным проблемам можно отнести внедрение и развитие технологий ИИ в военных целях (создание оружий, военной техники, гонка вооружений) [3]. Если говорить об угрозах, касающихся отдельных групп населения, то необходимо упомянуть проблемы с безопасностью и конфиденциальностью данных. Это тема особенно актуальна для сотрудников крупных корпораций, где искусственный интеллект применяется для сбора и обработки больших данных. Кроме того, существует угроза повышения дискриминационного выбора

или предвзятости. Действительно, ИИ может составить конкуренцию человеку в этом вопросе, так как именно роботы являются запрограммированными на определенные действия. Технология ИИ предполагает внесение некоторой системы ограничений и совершение выбора согласно с внедренным в неё алгоритмом [4]. Так, существует пример компании Amazon, которая однажды ошиблась, используя технологии ИИ для рекрутинга. Сотрудники отдела кадров использовали инструмент для отбора лучших резюме. Однако спустя время, стало ясно, что технология осуществляет выбор не с гендерно-нейтральной позиции. И это было связано с загруженным в неё шаблоном, согласно которому большинство соискателей за предыдущий период были мужчинами [5]. Так искусственный интеллект проявил себя не с лучшей стороны.

Несомненно, в настоящее время ИИ все глубже проникает во все сферы жизнедеятельности человека, оказывая существенное влияние на общество. Для того чтобы влияние технологий оставалось положительным и безопасным, требуется комплексный и разнообразный подход в решении морально-этических вопросов использования искусственного интеллекта. Появляющиеся угрозы должны быть замечены обществом, а государству необходимо тщательно проработать законодательство во избежание нарастания проблем.

Список литературы

1. What is Artificial Intelligence? FAQ от Джона Маккарти, 2007.
2. Минбалеев А. В. Проблемы регулирования искусственного интеллекта // Вестник ЮУрГУ. Серия: Право. 2018. № 4 // Электронный ресурс. URL: https://cyberleninka.ru/article/n/problemy-regulirovaniya-iskusstvennogo-intellekta (дата обращения: 15.12.2023).
3. Симици Э., Стамолампрос П., Даскалакис Г. и Корфиатис Н. (2021). Информационная ценность онлайн-отзывов сотрудников. Европейский журнал операционных исследований.
4. Artificial intelligence and bias: Four key challenges by John Villasenor [Электронный ресурс] // URL: https://www.brookings.edu/articles/artificial-intelligence-and-bias-four-key-challenges/ (дата обращения: 15.12.2023).

5. Insight — Amazon scraps secret AI recruiting tool that showed bias against women By Jeffrey Dastin [Электронный ресурс] // URL: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN-1MK08G/ (дата обращения: 15.12.2023).

УДК 004.382.7

Общее сравнение возможностей смартфонов с возможностями ПК

Музыченко Анна Николаевна

студентка магистратуры Донского государственного технического университета

***Аннотация**: Даны характеристики основным направлениям деятельности, которые можно реализовывать на смартфоне. Рассмотрена проблема внедрения смартфонов в деятельность пользователя. На основе метода анализа иерархий определено, насколько приближены возможности работы и бытовой деятельности Android к возможностям персонального компьютера/ноутбука. Сделаны выводы о возможностях использования смартфонов для разных целей.*

***Abstract**: Characteristics of the main activities that can be realized on a smartphone are given. The problem of implementation of smartphones in user activities is considered. On the basis of the method of hierarchy analysis it is determined how close the possibilities of work and household activities of Android are to the possibilities of personal computer/laptop. Conclusions are drawn about the possibilities of using smartphones for different purposes.*

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

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

Введение

Существует мнение, что для работы и выполнения бытовых задач в электронном виде обязательно нужно использовать ноутбук или персональный компьютер. Но так или иначе смартфоны вписались в жизнь

человека и имеют место быть в ней. Есть множество показателей, по которым смартфоном пользоваться удобнее. Это делает актуальным исследование общего сравнения возможностей смартфона с возможностями ПК.

Сравнение возможностей

Для того, чтобы провести сравнительный анализ, выделим основные направления деятельности пользователей: разработка, программирование, бытовые задачи, досуг. Показатели числа скачиваний, оценки основного программного обеспечения, оценка возможности осуществления той или иной деятельности взяты из источника [1]. Теперь для проведения сравнительного анализа, воспользуемся известным методом анализа иерархий. [2]. Представим задачу в иерархической форме (рисунок 1). На высшем уровне иерархий будет находиться цель "Каким устройством воспользоваться?". Определены критерии, состоящие из бытовых задач и задач программирования/разработки, которые в свою очередь можно поделить на программы и оценку пользователей. На низшем уровне расположены альтернативы — "персональный компьютер/ноутбук" или "смартфон".

Критерии из подгруппы "программы" будут рассмотрены как отдельная система иерархий каждая (рисунок 2) — целью здесь является "направление деятельности N", альтернативами являются также "персональный компьютер/ноутбук" или смартфон.

Результаты исследования по критерию "нуждаемость при решении бытовых задач на устройстве" ко по отдельной иерархической системе взяты из источника [3]. Из источника также взяты функции в Matlab: ierarhii, которая рассчитывает приоритетные значения и оценку согласованности для матрицы парных сравнений, ierarhii_from2, которая рассчитывает приоритетные значения для системы из 2 критериев, proc_to9, которая переводит процентное соотношение в оценку соответственно методу анализа иерархий.

Для основной иерархической формы с целью «каким устройством воспользоваться?», с помощью шкалы, даны оценки с учётов нумерации, соответственно основной форме иерархии, где 1 — написание кода, 19 — нуждаемость в разработке/программировании на устройстве. В каждой

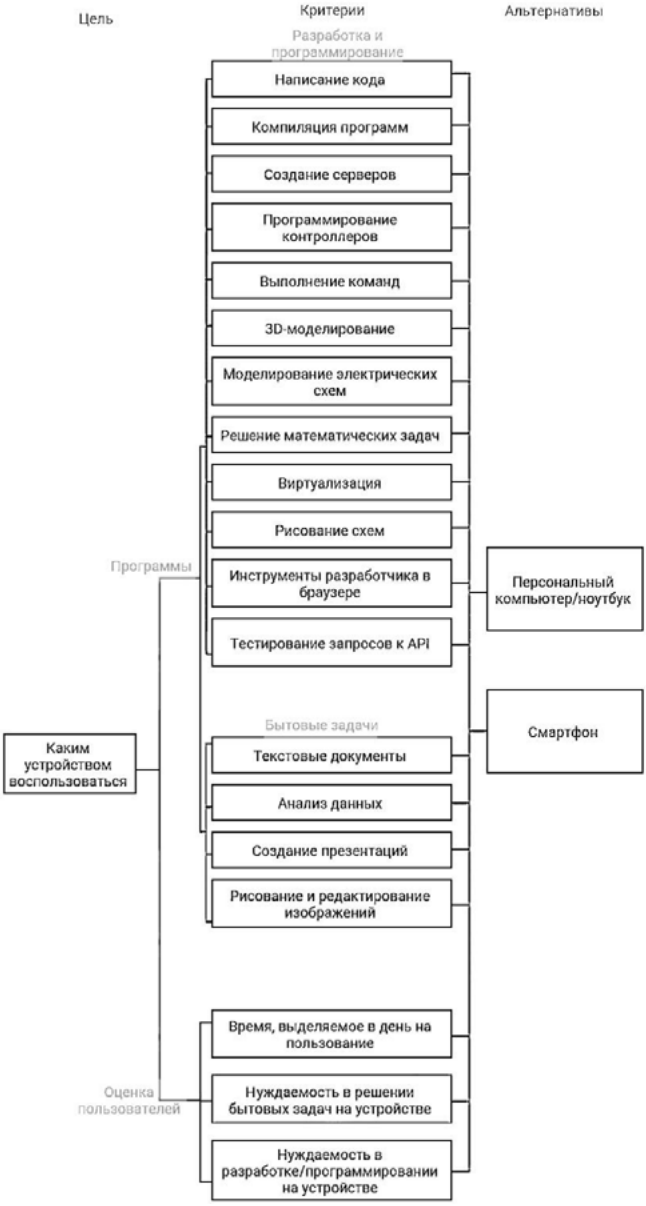

Рисунок 1. **Иерархическая форма задачи выбора устройства**

Рисунок 2. **Иерархическая форма задачи выбора устройства для направления деятельности N**

строке прописывается уровень превосходства критерия из строки над критерием из столбца. Так написание кода равно написанию кода, первый элемент равен 1. Компиляции программ дается настолько сильное превосходство над написанием кода, что оно становится практически значимым, значение 2-го столбца 1-й строки будет 1/7. Опыт и суждения дают сильное превосходство созданию серверов на фоне написания кода, значит значение 3-го столбца 1-й строки будет 1/5 По такому механизму расписана вся таблица, содержащаяся в скрипте на рисунке 3.

Результат выполнения приведён на рисунке 4.

Оценка согласованности меньше 10%, значит оценки согласованы.

На рисунке 5 в виде скрипта расписана матрица парных сравнений для задачи выбора устройства для направления деятельности N, дав критериям субъективные оценки:

Полученные значения приведены на рисунке 6, оценка согласованности меньше 10%, значит оценки согласованы.

```
A = [1  1/7  1/5  1/4  1/3  1/5  1/2  1/5  1/3  1/2  1/3  1   1/2  1/2  1   2   1/3  1/5  1/5 ;
7   1   1   3   2   3   2   2   5   4   7   2   4   2   5   4   7   3   3 ;
5   1   1   2   5   3   7   2   4   7   8   2   7   3   5   6   3   1/2  1/2 ;
4   1/3  1/2  1   1/2  1   1   1/3  2   1/2  8   3   2   1   5   2   1/2  1/4  1/3 ;
3   1/2  1/5  2   1   3   1/2  1/3  2   3   5   2   1   1/2  3   1/2  1/3  1/2  1 ;
5   1/3  1/3  1   1/3  1   3   1/2  5   2   7   2   2   1   4   1   2   1/2  1/4 ;
2   1/2  1/7  1   2   1/3  1   1/8  2   1/2  4   1/2  1/3  1/7  1/2  1   1/4  1/6  1/3 ;
5   1/2  1/2  3   3   2   8   1   8   4   9   6   5   2   5   3   2   1   1/2 ;
3   1/5  1/4  1/2  1/2  1/5  1/2  1/8  1   1/4  1   1/2  1/7  1/9  1/3  1/3  1/5  1/2  1/3 ;
2   1/4  1/7  2   1/3  1/2  2   1/4  4   1   5   4   1   1/3  1   1   1/2  1/3  1/4 ;
3   1/7  1/8  1/8  1/5  1/7  1/4  1/9  1   1/5  1   1/2  1/5  1/8  2   1/4  1/3  1/4  1/5 ;
1   1/2  1/2  1/3  1/2  1/2  2   1/6  2   1/4  2   1   1/2  1/5  1   1/2  1/3  1/3  1/4 ;
2   1/4  1/7  1/2  1   1/2  3   1/5  7   1   5   2   1   1/2  2   2   1   2   1/2 ;
2   1/2  1/3  1   2   1   7   1/2  9   3   8   5   2   1   4   2   2   1   1/2 ;
1   1/5  1/5  1/5  1/3  1/4  2   1/5  3   1   1/2  1   1/2  1/4  1   1/2  1/2  1/3  1/4 ;
1/2  1/4  1/6  1/2  2   1   1   1/3  3   1   4   2   1/2  1/2  2   1   2   1   1/2 ;
3   1/7  1/3  2   3   1/2  4   1/2  5   2   3   3   1   1/2  2   1/2  1   1/2  1/3 ;
5   1/3  2   4   2   2   6   1   2   3   4   3   1/2  1   3   1   2   1   1/2 ;
5   1/3  2   3   1   4   3   2   3   4   5   4   2   2   4   2   3   2   1];

names = ["Написание кода" "Компиляция программ" "Создание серверов"  "Программирование контроллеров" "Выполнение команд" "3D-моделирование"
    "Моделирование электрических схем" "Решение математических задач"  "Виртуализация" "Рисование схем" "Инструменты разработчика в браузере"
    "Тестирование запросов к API"  "Текстовые документы" "Анализ данных"  "Создание презентаций" "Рисование и редактирование фотографий"
    "Время, выделяемое в день на пользование"  "Нуждаемость в решении бытовых задач на устройстве"   "Нуждаемость в разработке/программировании на устройстве"];

r = ierarhii(A,names);
display(r)
```

Рисунок 3. **Скрипт для матрицы парных критериев основной формы**

```
"Значения приоритетов
 Написание кода : 0.016279
 Компиляция программ : 0.126313
 Создание серверов : 0.118812
 Программирование контроллеров : 0.043447
 Выполнение команд : 0.043476
 3D-моделирование : 0.052388
 Моделирование электрических схем : 0.022443
 Решение математических задач : 0.105520
 Виртуализация : 0.014938
 Рисование схем : 0.033177
 Инструменты разработчика в браузере : 0.012466
 Тестирование запросов к API: 0.022684
 Текстовые документы : 0.042558
 Анализ данных: 0.072796
 Создание презентаций : 0.020177
 Рисование и редактирование фотографий : 0.036552
 Время, выделяемое в день на пользование : 0.045945
 Нуждаемость в решении бытовых задач на устройстве: 0.072207
 Нуждаемость в разработке/программировании на устройстве : 0.097821
 Оценка согласованности: 9.480471 "
```

Рисунок 4. **Определение приоритетов для критериев основной таблицы**

```
A = [1 1/6 1/3 1/2 1 1/4;
6 1 5 3 2 1;
3 1/5 1 1 3 1/2;
2 1/3 1 1 4 1/2;
1 1/2 1/3 1/4 1 1/2;
4 1 2 2 2 1];
names = ["Количество скачиваний" "Возможности ПО, наличие нужных функций" "Возможность работы вне дома/офиса"
    "Возможность автономной работы устройства"  "Вес/габариты устройства"
    "Гибкость, возможность переноса работы на другие операционные системы"];
R = ierarhii(A,names);
display(R)

```

Рисунок 5. **Определение приоритетов по направлению деятельности N**

```
"Значения приоритетов
 Количество скачиваний : 0.061081
 Возможности ПО, наличие нужных функций : 0.332285
 Возможность работы вне дома/офиса : 0.137406
 Возможность автономной работы устройства: 0.146708
 Вес/габариты устройства : 0.073354
 Гибкость, возможность переноса работы на другие операционные
системы : 0.249167
 Оценка согласованности: 7.337199 "
```

Рисунок 6. **Приоритеты для направления деятельности N**

На основе данных из источника даны оценки основным критериям каждого направления деятельности: по критерию количества скачиваний — взят процент количества скачиваний на смартфоне от количества скачиваний на компьютере(если не указано, берётся значение 10 млн.) и переведён в девятые; по критерию возможностей ПО — к оценке из таблицы 1 прибавляется 1(чтобы перевести из шкалы 0–8 в шкалу 1–9) и полученная сумма делится на 9; по возможности работать вне дома и офиса, без

```
names = ["Написание кода" "Компиляция программ"  "Создание серверов"
    "Программирование контроллеров"   "Выполнение команд"  "3D-моделирование"
    "Моделирование электрических схем"  "Решение математических задач"
    "Виртуализация"   "Рисование схем"  "Инструменты разработчика в браузере"
    "Тестирование запросов к API"  "Текстовые документы"  "Анализ данных"
    "Создание презентаций"  "Рисование и редактирование фотографий" ];
names2 = ["Количество скачиваний" "Возможности ПО, наличие нужных функций"
    "Возможность работы вне дома/офиса"  "Возможность автономной работы устройства"
    "Вес/габариты устройства"
    "Гибкость, возможность переноса работы на другие операционные системы"];
ves2 = [0.061081 0.332285 0.137406 0.146708 0.073354 0.249167 7.337199];
info1 = [ 28*10^6 10^6 7; 17*10^6 10^5 5; 0.3*10^6 0.1*10^6 8;
    10*10^6 0.1*10^6 6; 0 10*10^6 8; 700*10^6 5*10^6 3; 0 10^6 4;
    63*10^6 10^6 5; 0 0.1*10^6 4; 31*10^6 0.5*10^6 3; 0 0.1*10^6 5;
    20*10^6 0.05*10^6 6; 1.2*10^9 10^9 7; 1.1*10^9 10^9 7; 1.5*10^9 10^9 7;
    0 10*10^6 7];
i=1;
while i<=length(names)
   if info1(i,1) == 0 t1 = 10*10^6; else t1 = info1(i,1); end;
   t2 = info1(i,2);
   k(1,i) = proc_to9(t2/t1*100);
   k(2,i) = proc_to9(info1(i,3)/16*100);
   k(3,i) = 8;
   k(4,i) = 6;
   k(5,i) = 9;
   k(6,i) = 1/6;
   i = i + 1;
end;
A = [1 0; 0 1];
names3 = ["Персональный компьютер/ноутбук", "Смартфон"];

i=1; m = 1;
p(m, 2) = "Критерий"; p(m+1,2)="Вес";
while(i<=length(names2))
    p(m,i+2)=names2(i);
    p(m+1,i+2)=ves2(i);
    i = i + 1;
end;
m = 3;
i = 1;
while i<=length(names)
    j=1;
    p(m,1) = names(i);
    p(m,2) = names3(1);p(m+1,2) = names3(2);
    while(j<=length(names2))
        A(2,1) = k(j,i);
        A(1,2) = 1/k(j,i);
        [r1, r2] = ierarhii_from2(A);
        p(m,j+2)=string(r1);
        p(m+1,j+2)=string(r2);
        j = j + 1;
    end;
    m=m+2;
    i = i + 1;
end;
t = array2table(p);
writetable(t, "data.xls");
```

Рисунок 7. **Скрипт расчёта приоритетов по всем направлениям деятельности с записью в таблицу**

Таблица 1. **Приоритетные значения альтернатив для критериев второго уровня для всех направлений деятельности**

	Критерий	Количество скачиваний	Возможности ПО, наличие нужных функций	Возможность работы вне дома/офиса	Возможность автономной работы устройства	Вес/ габариты устройства	Гибкость, возможность переноса работы на другие операционные системы
	Вес	0,061081	0,33228	0,13741	0,14671	0,073354	0,24917
Написание кода	Персональный компьютер/ ноутбук	0,88889	0,66667	0,11111	0,14286	0,1	0,85714
	Смартфон	0,11111	0,33333	0,88889	0,85714	0,9	0,14286
Компиляция программ	Персональный компьютер/ ноутбук	0,9	0,8	0,11111	0,14286	0,1	0,85714
	Смартфон	0,1	0,2	0,88889	0,85714	0,9	0,14286
Создание серверов	Персональный компьютер/ ноутбук	0,8	0,5	0,11111	0,14286	0,1	0,85714
	Смартфон	0,2	0,5	0,88889	0,85714	0,9	0,14286
Программирование контроллеров	Персональный компьютер/ ноутбук	0,9	0,75	0,11111	0,14286	0,1	0,85714
	Смартфон	0,1	0,25	0,88889	0,85714	0,9	0,14286
Выполнение команд	Персональный компьютер/ ноутбук	0,1	0,5	0,11111	0,14286	0,1	0,85714
	Смартфон	0,9	0,5	0,88889	0,85714	0,9	0,14286
3D-моделирование	Персональный компьютер/ ноутбук	0,9	0,85714	0,11111	0,14286	0,1	0,85714
	Смартфон	0,1	0,14286	0,88889	0,85714	0,9	0,14286
Моделирование электрических схем	Персональный компьютер/ ноутбук	0,875	0,83333	0,11111	0,14286	0,1	0,85714
	Смартфон	0,125	0,16667	0,88889	0,85714	0,9	0,14286
Решение математических задач	Персональный компьютер/ ноутбук	0,9	0,8	0,11111	0,14286	0,1	0,85714
	Смартфон	0,1	0,2	0,88889	0,85714	0,9	0,14286
Виртуализация	Персональный компьютер/ ноутбук	0,9	0,83333	0,11111	0,14286	0,1	0,85714
	Смартфон	0,1	0,16667	0,88889	0,85714	0,9	0,14286
Рисование схем	Персональный компьютер/ ноутбук	0,9	0,85714	0,11111	0,14286	0,1	0,85714
	Смартфон	0,1	0,14286	0,88889	0,85714	0,9	0,14286
Инструменты разработчика в браузере	Персональный компьютер/ ноутбук	0,9	0,8	0,11111	0,14286	0,1	0,85714
	Смартфон	0,1	0,2	0,88889	0,85714	0,9	0,14286
Тестирование запросов к API	Персональный компьютер/ ноутбук	0,9	0,75	0,11111	0,14286	0,1	0,85714
	Смартфон	0,1	0,25	0,88889	0,85714	0,9	0,14286
Текстовые документы	Персональный компьютер/ ноутбук	0,14286	0,66667	0,11111	0,14286	0,1	0,85714
	Смартфон	0,85714	0,33333	0,88889	0,85714	0,9	0,14286
Анализ данных	Персональный компьютер/ ноутбук	0,11111	0,66667	0,11111	0,14286	0,1	0,85714
	Смартфон	0,88889	0,33333	0,88889	0,85714	0,9	0,14286
Создание презентаций	Персональный компьютер/ ноутбук	0,2	0,66667	0,11111	0,14286	0,1	0,85714
	Смартфон	0,8	0,33333	0,88889	0,85714	0,9	0,14286
Рисование и редактирование фотографий	Персональный компьютер/ ноутбук	0,1	0,66667	0,11111	0,14286	0,1	0,85714
	Смартфон	0,9	0,33333	0,88889	0,85714	0,9	0,14286

Таблица 2. **Приоритетные значения альтернатив для направлений деятельности**

	Персональный компьютер/ноутбук	Смартфон
Написание кода	0,532950987	0,467054013
Компиляция программ	0,57793249	0,422072511
Создание серверов	0,47214039	0,527864611
Программирование контроллеров	0,56131849	0,438686511
Выполнение команд	0,42938369	0,570621311
3D-моделирование	0,596918969	0,403086031
Моделирование электрических схем	0,587480357	0,412524643
Решение математических задач	0,57793249	0,422072511
Виртуализация	0,589007382	0,410997618
Рисование схем	0,596918969	0,403086031
Инструменты разработчика в браузере	0,57793249	0,422072511
Тестирование запросов к API	0,56131849	0,438686511
Текстовые документы	0,487382729	0,512622271
Анализ данных	0,485443407	0,514561593
Создание презентаций	0,490872897	0,509132103
Рисование и редактирование фотографий	0,484764797	0,515240203

стола смартфон значительно превосходит персональные компьютеры или ноутбуки — присваивается оценка 8; в ситуации отключения электричества смартфон при наличии современного портативного зарядного устройства может проработать намного дольше, чем ноутбук — поэтому присваивается оценка 6; смартфон однозначно выигрывает у ноутбука/компьютер — поэтому присваивается максимальная оценка 9; смартфон сильно проигрывает компьютеру в возможности разработки под другие операционные системы или в переносе работ на другие операционные системы — поэтому

присваивается оценка 1/6. Указанные коэффициенты помогут составить таблицу иерархий 2-го уровня для направлений деятельности.

На рисунке 7 представлен скрипт на основе алгоритма расстановки оценок, описанного выше, использованы вычисленные ранее весы приоритетов критериев. Скрипт создаёт общую таблицу с приоритетами критериев второго уровня на основе полученных данных для иерархий каждого из направлений.

Полученный результат показан в таблице 1.

Путём перемножения значений критериев второго порядка на вес критериев первого уровня для направлений деятельности получены итоговые приоритетные значения альтернатив для каждого направления деятельности, приведённые в таблице 2.

Таблица 3. **Приоритетные значения для основной иерархии**

	Вес	Персональный компьютер/ноутбук	Смартфон
Написание кода	0,016279	0,532950987	0,467054013
Компиляция программ	0,126313	0,57793249	0,422072511
Создание серверов	0,118812	0,47214039	0,527864611
Программирование контроллеров	0,043447	0,56131849	0,438686511
Выполнение команд	0,043476	0,42938369	0,570621311
3D-моделирование	0,052388	0,596918969	0,403086031
Моделирование электрических схем	0,022443	0,587480357	0,412524643
Решение математических задач	0,10552	0,57793249	0,422072511
Виртуализация	0,014938	0,589007382	0,410997618
Рисование схем	0,033177	0,596918969	0,403086031
Инструменты разработчика в браузере	0,012466	0,57793249	0,422072511
Тестирование запросов к API	0,022684	0,56131849	0,438686511
Текстовые документы	0,042558	0,487382729	0,512622271
Анализ данных	0,072796	0,485443407	0,514561593
Создание презентаций	0,020177	0,490872897	0,509132103
Рисование и редактирование фотографий	0,036552	0,484764797	0,515240203
Время, выделяемое в день на пользование	0,045945	0,5	0,5
Нуждаемость в решении бытовых задач на устройстве	0,072207	0,52776	0,47224
Нуждаемость в разработке/программировании на устройстве	0,097821	0,5	0,5
Приоритетные значения		**0,52850221**	**0,47150071**

С использованием полученных значений, значений из таблицы 2, значений с источника [2] определены итоговые приоритетные значения. Результат приведён в таблице 3.

Заключение

По результатам проведенного исследования можно сделать следующие выводы.

1. Общий приоритет работы на смартфоне составляет примерно 47% от компьютера.
2. По всем направлениям деятельности — как в разработке, так и в бытовых задачах просматривается нуждаемость пользователей в использовании смартфона.
3. По большинству выбранных критериев качества так или иначе просматривается тенденция использования смартфона взамен компьютеру или ноутбуку.

Список литературы

1. Музыченко А. Н. Возможности перехода программирования и разработки в среду Android // Научный аспект. — Самара: Изд-во ООО «Аспект».— 2023.— № 11. — URL: https://na-journal.ru/11–2023-informacionnye-tekhnologii/6737-vozmojnosti-perekhoda-programmirovaniya-i-razrabotki-v-sredu-android.
2. Т. Саати, К. Кернс, перевод с английского Р. Г. Вачнадзе, под редакцией И. А. Ушакова, М.: Радио и связь, 1991.— 224 с.
3. Музыченко А. Н. Исследование внедрения смартфонов в повседневную жизнь человека // Научный аспект. — Самара: Изд-во ООО «Аспект».— 2023.— № 11. — URL: https://na-journal.ru/11–2023-informacionnye-tekhnologii/7037-issledovanie-vnedreniya-smartfonov-v-povsednevnuyu-jizn-cheloveka.
4. Дьяконов В. П. MATLAB. Полный самоучитель; ДМК Пресс — Москва, 2010.— 768 с.

УДК 004.925.83

Создание графиков повышенной точности

Музыченко Анна Николаевна

студентка магистратуры Донского государственного технического университета

***Аннотация**: Рассмотрены проблемы, с которыми можно столкнуться при попытке построения графиков повышенной точности в Matlab. Рассмотрена проблема отсутствия возможности построения графиков повышенной точности. Приведены алгоритм и функция, с помощью которой можно построить график повышенной точности. Показаны результаты выполнения функции.*

***Abstract**: The problems which can be encountered when trying to construct graphs of increased accuracy in Matlab are considered. The problem of lack of possibility to construct graphs of increased accuracy is considered. An algorithm and a function with the help of which it is possible to construct a graph of increased accuracy are given. The results of the function execution are shown.*

***Ключевые слова**: графики, matlab, возможности, точность, повышенная точность, отсутствие возможности.*

***Keywords**: graphs, matlab, capability, precision, accuracy, increased accuracy, no capability.*

Иногда может сложиться такая стуация, что необходимо построить график на точности более, чем 6 знаков после запятой. Это может пригодиться, например, при использовании численных методов, а именно при определении экстремумов при заданной высокой точности. В *Matlab* нет базовых возможностей построить график на высокой точности, могут возникать проблемы — например, график может изображаться в виде прямой линии, расположенной вертикально или горизонтально, а при попытке задать граничные значения по осям *x* и *y* с помощью функций "*xlim*" и "*ylim*" могут возникать ошибки. Поэтому целью будем считать написание функции для построения графиков высокой точности. В качестве функции, которую необходимо изобразить на высокой точности, будем использовать синусоиду. [1]

Построение графика высокой точности можно свести к построению графика стандартной точности, определив значения как части, и воспользовавшись приведённым ниже алгоритмом.

1. Необходимо найти краевые значения x01, x02, y01, y02 по осям x, y.
2. Отнять от основных значений x и y нижние значения (x01 или y01), а затем разделить на длину отрезков по осям (x02-x01 или y02-y01) — таким образом, будут получены вектора значений x2 и y2, обозначающие части от максимальных значений по осяим.
3. Вектор x00 необходимо задать m значениями с вектора x2, находящимися друг от друга на одном и том же расстоянии, где m — количество точек, которые необходимо выделить на графике. Аналогично задаётся вектор y00.
4. Теперь нужно добавить вектор y001, состоящий из сортированных по возрастанию значений вектора y00.
5. Теперь заполнив вектора текстовых подписей xt0 и yt0 по формулам xt0=x01+x00*(x02-x01) и yt0=y01+y001*(y02-y01).
6. После этого можно построить график, образуя линию из значений векторов x2 и y2, отмечая точки из значений векторов x00 и y00, отмечая пунктирными линиями значения с векторов x00 и y001, подписывая эти значения текстом с векторов xt0 и yt0.

Таким образом, можно построить график высокой точности, поменяв его реальные значения на части отрезка, подписав полученные значения как реальные. Код для *Matlab*, написанный по приведённому выше алгоритму приведён на рисунке 1. [2]

Напишем код для построения вершины функции $y=sin(x)$ на точности x — 20 знаков после запятой, как показано на рисунке 2.

Будет получен график, показанный на рисунке 3.

Аналогичным образом можно построить графики функций $y=sin(x*10^{20})$, $y=sin(x*10^{21})$ и $y=sin(x*10^{22})$ как показано на рисунках 4, 5, 6 и 7. [3]

Заметим, что для выше приведённых графиков для корректного отображения необходимо увеличивать изначальное количество точек.

По результатам проведенной работы можно сделать следующие выводы:

1. Написан алгоритм для построения графиков повышенной точности.
2. Создана функция в Matlab, основанная на данном алгоритме.
3. Созданная функция строит график по частям, но правильно отображает значения по осям абсцисс и ординат.

```
function hp_plot(x, y, N, m, info, info2, ttl)
y01=vpa(min(y),N*10); y02=vpa(max(y),N*5);
x01=vpa(min(x),N+1); x02=vpa(max(x),N+1);
x2=double(round((x-x01)./(x02-x01),round(N/2)));
y2=round((y-y01)./(y02-y01),N);
p=size(x2,2);
ns=linspace(1,p,m);
x00=[]; y00=[];
for i=1:size(ns,2)
    x00=[x00; x2(1,round(ns(1,i)))];
    y00=[y00; y2(1,round(ns(1,i)))];
end;
xt0=string(vpa(x01+x00.*(x02-x01),N+1));
y001=double(sort(y00));
yt0=string(vpa(y01+y001.*(y02-y01),N*2+1));
figure(1)
clf
plot(x2,y2,info, x00,y00,info2)
grid on
xlabel("x")
ylabel("y")
xticks(x00)
xticklabels(xt0)
yticks(y001)
yticklabels(yt0)
title(ttl);
end
```

Рисунок 1. **Код функции для создания графика высокой точности**

```
N=20;

clc
digits(N*3); %задаем максимально допустимую точность

P=vpa(10^(-N),N+1); %задаём шаг
p1=5; p2=5;

x=vpa(pi/2-p1*P,N+1):vpa(P/10,N+1):vpa(pi/2+p2*P,N+1);%задаём x
y=vpa(sin(vpa(x,N+1)),N*2+1); %задаём y

hp_plot(x,y,N,p1+p2+1,'-b','.m',"y = sin(x)");
```

Рисунок 2. **Код для построения синусоиды на точности 20 знаков**

4. С помощью созданной функции можно строить графики точности больше, чем 6 знаков после запятой.
5. Построены графики высокой точности в Matlab, в качестве примера рассмотрен график синусоиды.
6. Созданная функция успешно справляется с основной целью — построением графиков высокой точности.

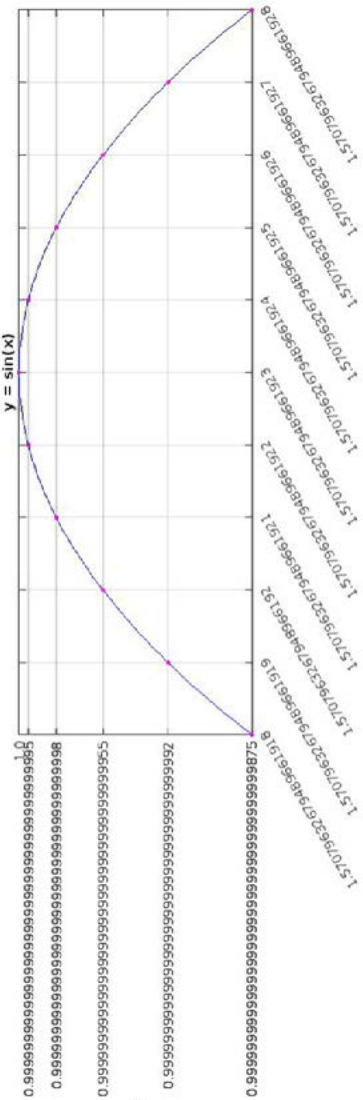

Рисунок 3. **График функции y=sin(x) на точности 20 знаков**

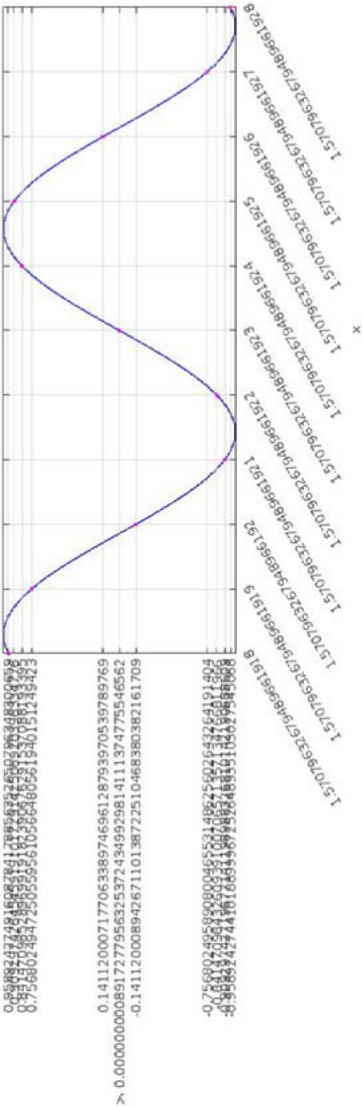

Рисунок 4. **График y=sin(x*10^{20}) на точности 20 знаков**

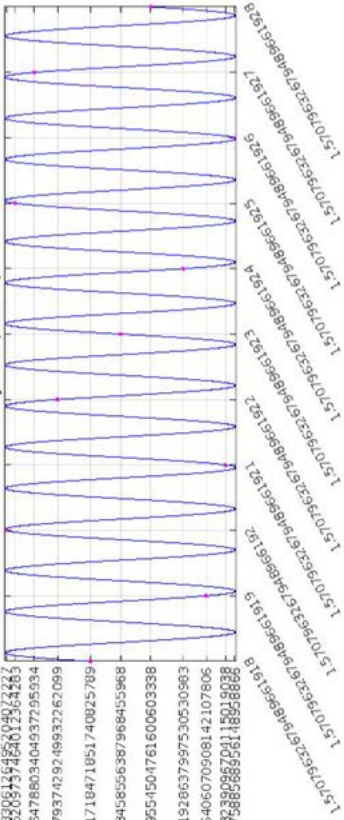

Рисунок 5. **График y=sin(x*10^{21}) на точности 20 знаков**

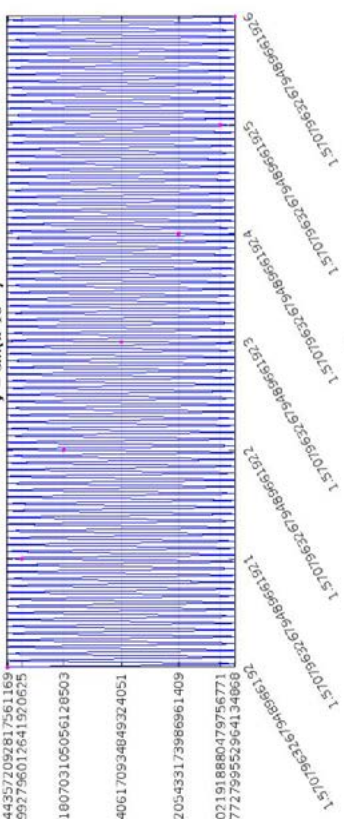

Рисунок 6. **График y=sin(x*10^{22}) на точности 20 знаков**

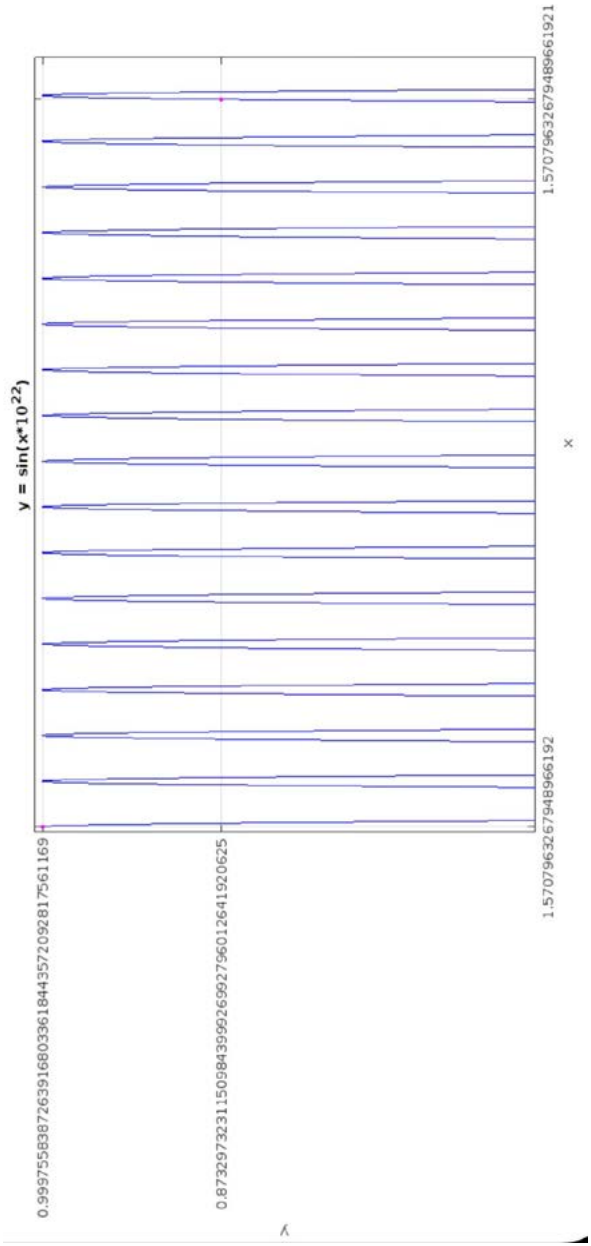

Рисунок 7. **Увеличенный график y=sin(x*10^{22}) на точности 20 знаков**

Список литературы

1. MatLab. Язык технических вычислений. [Электронный ресурс]. — URL: http://www.exponenta.ru/educat/free/matlab/gs.pdf.
2. Дьяконов В. П. MATLAB. Полный самоучитель; ДМК Пресс — Москва, 2010.— 768 с
3. Дьяконов А. Г. Среда для вычислений и визуализации MATLAB. Учебное пособие.

УДК 005

Классификация безопасности Big Data на основе веб-языка онтологий

Голубятников Артем Олегович

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

***Аннотация**: Огромный объем данных (известный как Big Data) теперь может собираться и храниться из различных источников данных, включая журналы событий, Интернет, смартфоны, базы данных, датчики, облачные вычисления и устройства Интернета вещей (IoT). Термин «безопасность Big Data» относится ко всем гарантиям и инструментам, используемым для защиты как данных, так и аналитических процессов от вторжений, краж и других враждебных действий, которые могут поставить их под угрозу или отрицательно повлиять на них. Помимо того, что защита Big Data является ценной и желательной целью, она сталкивается с особыми трудностями. Безопасность Big Data принципиально не отличается от традиционной безопасности данных. Проблемы безопасности Big Data вызваны скорее внешними различиями, чем фундаментальными. В этом исследовании подробно описываются многочисленные трудности безопасности, с которыми сейчас сталкивается аналитика Big Data, и поощряются дополнительные совместные исследования для решения обеих проблем безопасности Big Data с использованием веб-языка Ontology (OWL). Хотя в этом эссе мы фокусируемся на проблемах безопасности Big Data, мы также кратко остановимся на более широких проблемах Big Data. Предлагаемая классификация безопасности Big Data, основанная на онтологическом веб-языке, созданном на основе программного обеспечения-протеже, имеет 32 класса и 45 подклассов.*

***Abstract**: A vast amount of data (known as Big Data) can now be collected and stored from a variety of data sources, including event logs, the Internet, smartphones, databases, sensors, cloud computing, and Internet of Things (IoT) devices. The term "Big Data security" refers to all safeguards and tools used to protect both data and analytical processes from intrusions, theft, and other hostile actions that could jeopardize or adversely affect them. In addition to being a valuable and desirable goal, Big Data security faces special challenges. Big Data security is not fundamentally different from traditional data security. Big Data security challenges are caused by external differences rather than fundamental differences. This study details the many security challenges currently faced by Big Data analytics and encourages additional collaborative research to address both Big Data security challenges using Ontology Web Language (OWL). Although the focus is on Big Data security challenges in this essay, the authors will also briefly discuss the broader Big Data challenges. The proposed Big Data security classification, based on the ontology web language created from protégé software, has 32 classes and 45 subclasses.*

***Ключевые слова**: Big Data, Big Data Security, информационная безопасность, безопасность данных, веб-язык онтологий.*

***Keywords**: Big Data, Big Data Security, information security, data security, ontology web language.*

1. Введение

Возможность собирать и хранить огромные объемы данных (так называемая Big Data) из различных источников данных, включая журналы событий, Интернет, смартфоны, базы данных, датчики, устройства IoT и т. д., стала возможной благодаря технологическим достижениям последних лет. [1]. Эти данные собираются, изучаются и сравниваются друг с другом для получения значимой информации, которая часто используется при принятии решений.

Системы управления реляционными базами данных и настольное/статическое программное обеспечение неэффективны для обработки Big Data; вместо этого необходимо программное обеспечение с массовым параллелизмом, работающее на десятках тысяч или даже миллионах серверов. Огромное внимание, которое уделяется Big Data, в большей степени связано с тем, что анализ только одного большого набора связанных данных может дать гораздо больше информации, чем анализ меньших отдельных наборов с тем же общим объемом данных, что позволяет найти корреляции. Это позволяет вам выявлять тенденции в бизнесе, оценивать

уровень исследований, прогнозировать распространение болезней, предотвращать болезни, бороться с преступностью и многое другое.

Термин «безопасность Big Data» относится ко всем гарантиям и инструментам, используемым для защиты как данных, так и аналитических процессов от вторжений, краж и других враждебных действий, которые могут поставить их под угрозу или отрицательно повлиять на них. Помимо того, что защита Big Data является ценной и желательной целью, она сталкивается с особыми трудностями. Безопасность Big Data по сути не отличается от традиционной безопасности данных. Проблемы безопасности Big Data вызваны скорее внешними различиями, чем фундаментальными.

Типичным определением онтологии является «явная спецификация концепции» [2]. Это указывает на то, что представление спецификации предлагает формальную семантику спецификации и что онтология позволяет определять концепции и взаимодействия между этими концепциями. Из всех распространенных моделей представления знаний онтологии имеют самый высокий уровень семантического богатства [2]. Хотя ни одна из этих моделей не достигает того уровня семантического богатства, который обеспечивают онтологии, они основаны на моделях, которые будут объяснены в последовательности увеличения степени семантического богатства. Из всех перечисленных выше моделей глоссарий обладает наименьшим семантическим богатством. Глоссарий — это список слов в алфавитном порядке с их определениями, но без объяснения того, как эти слова связаны друг с другом. Таксономия — это модель вложенной классификации слов следующего уровня семантического богатства. Для описания отношений между словами используются супер- и суботношения. Эти отношения придают этим понятиям упорядоченность общности. Тезаурус — это расширенная таксономия. Тезаурус объясняет все возможные отношения слов. Модель, которая больше всего напоминает онтологию, — это тематическая карта. Абстрактной моделью и форматом данных для создания структур знаний является тематическая карта. Отношения между различными темами описываются через ассоциации, основанные на тезаурусе. Кроме того, карты тем могут содержать внешние документы, встроенные посредством вхождений [3].

Хотя в этом эссе мы фокусируемся на проблемах безопасности Big Data, мы также быстро рассмотрим общие проблемы, связанные с Big Data.

1.1. Характеристики Big Data

Объем, Разнообразие, Скорость, Достоверность, Ценность, Вариативность, Исчерпывающий, Детализированный и уникально лексический, Реляционный, Экстенсиональный и Масштабируемость — это характеристики, которые лучше всего представляют Big Data, как показано на рисунке 1.

1.2. Технологии Big Data

Существует несколько инструментов для оценки Big Data, включая A/B-тестирование, машинное обучение и обработку естественного языка. Базы данных, облачные вычисления, бизнес-информация и визуальные элементы, такие как графики и диаграммы, как показано на рисунке 2.

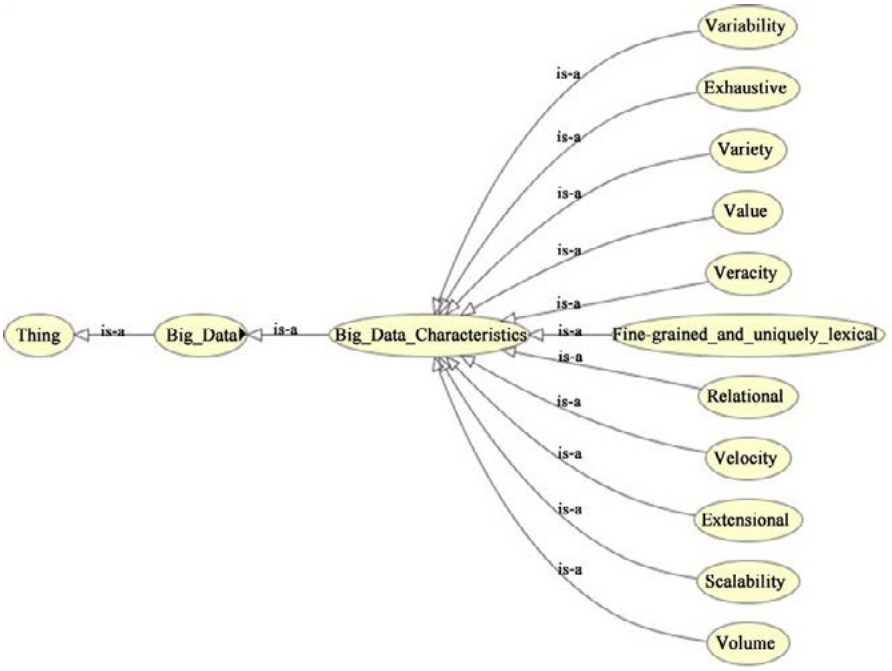

Рисунок 1. **Характеристики Big Data**

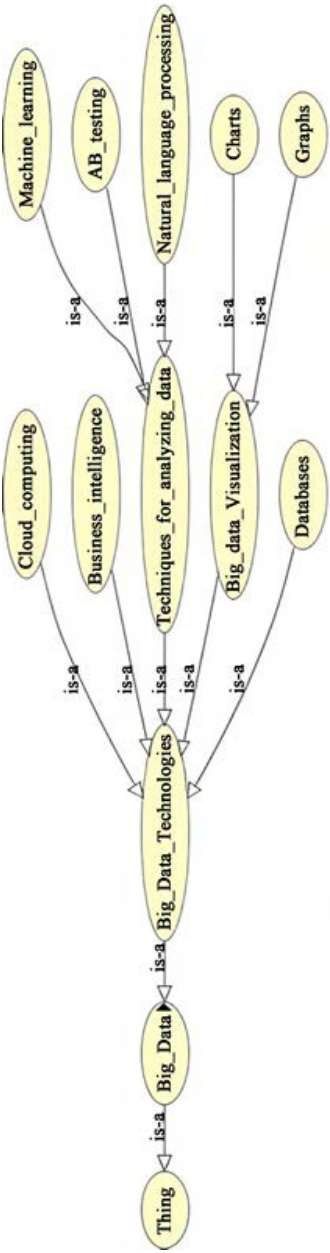

Рисунок 2. **Технологии Big Data**

1.3. Приложения для Big Data

Правительство, международное развитие, здравоохранение, образование, средства массовой информации, страхование, Интернет вещей и информационные технологии — это отрасли, которые больше всего используют Big Data, как показано на рисунке 3.

1.4. Жизненный цикл Big Data

На протяжении жизненного цикла Big Data существуют различные этапы работы с данными. Ниже приведены эти этапы: интеграция данных, хранение и администрирование, обработка и анализ данных, как показано на рисунке 4.

2. Требования к безопасности Big Data

Управление информационной безопасностью при одновременном контроле огромных и быстрых потоков данных — одна из трудностей в сфере Big Data. Поэтому технологии безопасности должны быть адаптируемый и простой в масштабировании, чтобы облегчить интеграцию будущих технологических достижений и корректировку потребностей приложений.

Необходимо найти компромисс между различными требованиями безопасности, обязанностями по конфиденциальности, эффективностью системы и быстрым динамическим анализом различных массивных наборов данных (данные в движении или статические, частные и общедоступные, локальные или общие и т. д.).

3. Проблемы безопасности Big Data

Согласно [3][4], существует два основных компонента безопасности в контексте Big Data: информационная безопасность и безопасность данных, как показано на рисунке 5.

Безопасность Big Data обычно направлена на обеспечение мониторинга в реальном времени для выявления рисков безопасности, уязвимостей

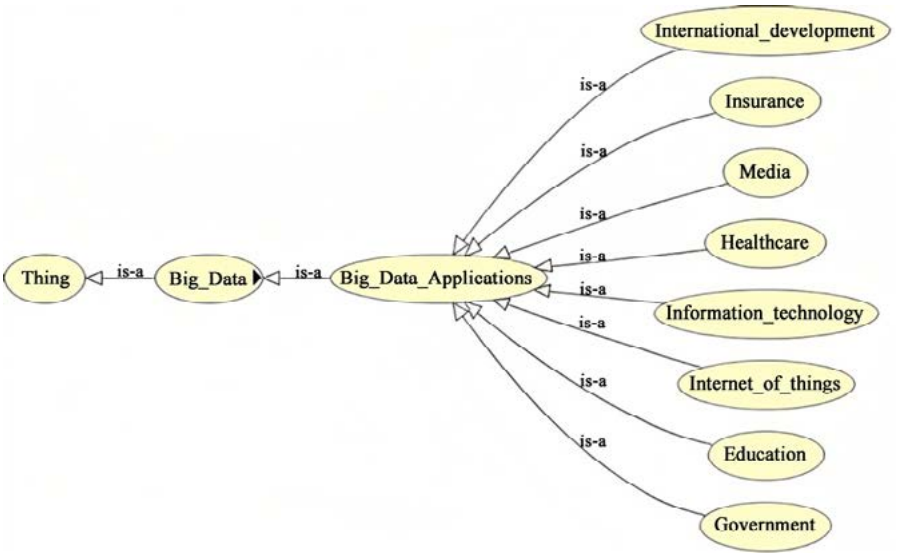

Рисунок 3. **Приложения для Big Data**

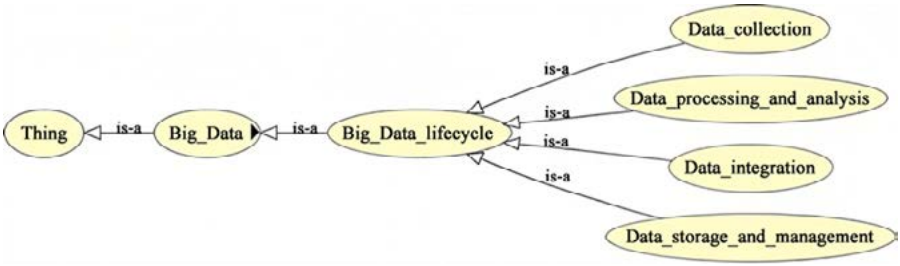

Рисунок 4. **Жизненный цикл Big Data**

и аномального поведения; детальный контроль доступа на основе ролей; надежная защита личной информации; и создание показателей эффективности безопасности. В случае инцидента безопасности это способствует быстрому принятию решений. Трудности в достижении этих целей перечислены и объяснены в следующих разделах.

4. Защита данных Big Data

Организации вынуждены искать инновационные способы производства и доставки ценности клиентам посредством управления цепочками поставок из-за быстрого роста мировой экономики и улучшения использования клиентами информационных технологий [4]. Предприятия будут более успешными, если они будут сотрудничать с другими предприятиями для сокращения затрат, производства высококачественных товаров и максимизации добавленной стоимости от обслуживания своих клиентов. Кроме того, утверждалось, что компания будет более конкурентоспособной, если она передаст часть своего производства компаниям, не связанным с ее основной отраслью.

По мнению Арльбьерна и др., цепочка поставок услуг. [5] — это широкое понятие, включающее компании, которые занимаются поставкой запасных частей, сторонними поставщиками, финансами, страхованием, розничной торговлей и государственными услугами. Определение системы цепочки поставок услуг — это сеть поставщиков, поставщиков услуг, потребителей и других вспомогательных единиц, которые осуществляют транзакции с использованием ресурсов, необходимых для производства услуг, преобразуют эти ресурсы в вспомогательные и основные услуги и предоставляют эти услуги клиентам. [3]. Финансы, телефония, интернет-услуги, мобильные приложения и туризм входят в число секторов сферы услуг, представленных в цепочке поставок услуг [5]. Поставщик услуг должен проявлять творческий подход к разработке предложений, которые отличают его от конкурентов [1]. Сканируя бизнес-среду, корпорация может успешно реализовать цепочку поставок услуг, понимая бизнес-процессы, сети цепочек поставок, а также потребности и желания конечных пользователей.

Рисунок 5. **Проблемы безопасности Big Data**

В свете того факта, что как внутренние, так и внешние элементы оказывают влияние на расходное поведение клиента, [1] определяет сканирование среды как процесс сбора и применения информации о событиях, тенденциях и отношениях во внутренней и внешней среде организации. Статус-кво, образование, занятость и религия — вот несколько примеров внутреннего влияния. Внешние элементы включают экономику, окружающую среду, семью и друзей [2] [3]. Компания должна время от времени оценивать данные о потребителях, которые были разделены на различные сегменты, чтобы включить как текущих, так и потенциальных клиентов. Корпорация должна приложить немало усилий, чтобы точно предсказать желания клиентов, поскольку сегментация рынка часто меняется [2]. Чтобы добиться снижения операционных расходов, работа цепочки поставок услуг должна быть быстрой и адаптируемой в ответ на потребительский спрос [3]. Создание структуры для измерения эффективности цепочки поставок окажет большое влияние на выявление факторов успеха, узких мест, потерь, операционных проблем, потребностей клиентов, которые должны быть удовлетворены, эффективных бизнес-процедур, принятия фактических решений, отслеживания прогресса и внесения предложений по улучшению [4] [5].

Гаванкар *и др.* [5] утверждает, что дальнейшие исследования по-прежнему необходимы для измерения эффективности цепочки поставок, чтобы продвинуться в изучении и применении. В результате, чтобы разделить сегментацию рынка и прогнозирование спроса с помощью инновационных возможностей цепочки поставок, управление цепочкой поставок услуг требует надежных технологий для анализа данных [1]. Сервисные компании используют аналитику Big Data на основе структурированных и неструктурированных данных, чтобы повысить эффективность цепочки поставок услуг и повысить эффективность работы компаний для оптимизации бизнеса за счет инноваций. Таким образом, технология Big Data стала важным компонентом корпоративных операций и стратегии, чтобы предвидеть и удовлетворять потребности современных клиентов.

Повышенная гибкость, оперативность, обслуживание клиентов и надежность — это лишь некоторые из преимуществ, которые аналитика Big Data предлагает поставщикам услуг [2]. Внедрение аналитики Big Data

имеет решающее значение для логистики и операций цепочки поставок, поскольку повышение эффективности цепочки поставок зависит от своевременного и точного выбора цепочки поставок. Эффект кнута в цепочке поставок, который приводит к неэффективности каналов сбыта, можно устранить с помощью анализа Big Data. [3] утверждает, что, поскольку возможности прогнозной аналитики Big Data четко не определены, ее потенциальное влияние на производительность цепочки поставок может быть ограничено.

Существует потребность в эмпирических публикациях, посвященных анализу Big Data, который снижает стандартные отклонения (дисперсию спроса) и добавляет сигнальный аспект в прогнозирование [1]. Тем не менее, ученые и бизнес начали обращать внимание на то, как предприятия используют анализ Big Data, особенно когда возникли опасения по поводу безопасности и конфиденциальности данных. Поставщики услуг собирают информацию в виде видеофайлов, обновлений статуса, лайков, репостов, подписок, ретвитов и комментариев из каналов социальных сетей, которые являются открытыми источниками.

Кроме того, анализ Big Data может использовать информацию из систем управления взаимоотношениями с клиентами и систем планирования ресурсов предприятия. Значительный объем данных, полученных из многих источников, сопряжен с угрозами конфиденциальности и безопасности из-за доступности данных как в структурированных, так и в неструктурированных форматах. Большинство предприятий имеют ограничения на систематические подходы к обеспечению соответствующих механизмов доступа к данным, а существующие решения по обеспечению безопасности, не связанные с Big Data, часто не предназначены для обработки масштаба, скорости, разнообразия и сложности Big Data [2]. В результате сервисным компаниям не хватает аналитических инструментов и методов для получения полезной информации из данных для разработки стратегии и улучшения качества обслуживания и эффективности бизнеса [5].

Несмотря на то, что аналитика Big Data может помочь в процессах принятия решений и управления цепочками поставок, многие предприятия столкнулись с трудностями при внедрении этой технологии. Для этого существуют различные причины. Одной из причин, по которой предприя-

тия не решаются использовать Big Data, является нехватка сотрудников, обладающих необходимым опытом для проведения анализа. Во-вторых, не проводилось большого количества исследований того, как приложения Big Data могут повлиять на цепочки поставок (Уоллер и Фосетт [4]). Доступная в настоящее время литература по этой теме несколько недооценена [3], несмотря на то, что аналитика Big Data полезна для поддержки сервисных организаций в создании новых продуктов и услуг.

5. Информация о безопасности Big Data

В эпоху Big Data читатели сегодня предпочитают электронные литературные ресурсы бумажным. Национальная библиотека Китая сообщает, что к ее электронным литературным ресурсам обращаются более 7 миллионов раз в год, тогда как ее печатные ресурсы берут только от 200 000 до 80 000 человек [4]. Приложения Big Data в библиотеках сталкиваются со сложной проблемой: как управлять и использовать литературные ресурсы.

Интеграция имеет решающее значение для литературных источников, используемых в статьях. Чтобы интегрировать и расположить эти ресурсы бумажной литературы в месте, которое читателям будет легко найти, библиотеки могут использовать данные датчиков для прогнозирования того, какие ресурсы бумажной литературы будут наиболее популярны среди читателей. Другие бумажные литературные ресурсы можно убрать из книжных шкафов или компактно сложить [4]. Библиотеки также могут рассчитать коэффициент использования на основе коэффициента заимствования, чтобы включить ресурс бумажной литературы. Для удовлетворения потребностей читателей интегрированы бумажные литературные ресурсы. Оцифровка имеет решающее значение для ресурсов электронной литературы. Помимо объединения физических и цифровых библиотек, печатных и электронных литературных ресурсов, а также бумажных и электронных литературных ресурсов, оцифровка литературных ресурсов должна стимулировать совместное использование таких ресурсов.

Многие отрасли, включая страхование, телекоммуникации, социальные сообщества и другие, рассмотрели проблему оттока сотрудников. На

сегодняшний день предложено множество методов решения проблемы прогнозирования оттока клиентов. Основные методы включают деревья решений 5, логистическую регрессию 3 и машины опорных векторов (SVM) 4. Чтобы спрогнозировать отток клиентов в предоплаченной мобильной телефонии, Archaux *et al*. [1] использовали SVM, а также оценивали эффективность SVM и ANN (искусственных нейронных сетей)6. Чтобы решить проблему прогнозирования оттока сотрудников, Ауэт предложил систему интеллектуального анализа данных, основанную на эволюционном обучении. Чтобы предсказать отток операторов связи, Идрис *и др*. [2] использовали случайный лес, ротационный лес, RotBoost и ансамбли украшения.

В своем исследовании трех методов интеллектуального анализа данных для прогнозирования оттока газетных служб Куссемент и ван ден Поел обнаружили, что метод случайного леса превзошел по эффективности логистическую регрессию и SVM. Все эти исследования посвящены использованию методов интеллектуального анализа данных для повышения точности моделей прогнозирования, но ни одно из них не учитывает, как социальные факторы влияют на текучесть пользователей.

Другой метод прогнозирования оттока пользователей — анализ социальных сетей (SNA). 7. Анализ социальных сетей может помочь улучшить текущие модели оттока пользователей, изучая модели общения пользователей. В качестве иллюстрации Нгонманг создал надежную статистическую модель для расчета вероятности того, что пользователь покинет социальную сеть, на основе свойств графа. Чтобы спрогнозировать возможные оттоки, Dasgupta *et al*. [3] оценили вероятность оттока пользователей на основе соседей, которые уже покинули систему. Одной из форм CHC, которую также можно рассмотреть, является распространение информации.

Чтобы улучшить эффективность прогнозирования оттока клиентов, Фадке и Чжан *и др*. [4] приняли модель распространения, ориентированную на получателя, и модель распространения, ориентированную на отправителя, соответственно. Однако Кусума продемонстрировал, что метод SNA обычно не применим и что прогнозирование оттока европейских пользователей предоплаты не может быть эффективно улучшено. Кроме

того, в ходе углубленных исследований изучалось влияние и распространение информации. Майерс *и др.* [5] исследовали, как информация достигает узлов социальной сети, и количественно оценили внешние воздействия с течением времени, тогда как Гомес-Родригес сосредоточился на проблеме отслеживания каналов распространения и влияния через сети. В отличие от других исследований, наша работа представляет собой тщательную парадигму анализа оттока, которая учитывает как демографию подписчиков, так и социальное влияние. Наше исследование может не только выявить абонентов с сильными негативными влияниями и важными характеристиками, связанными с текучестью подписчиков, но также может предсказать вероятность оттока подписчиков. Наш анализ основан на реальных Big Data телекоммуникаций, а результаты более тщательны и убедительны.

6. Выводы

Big Data зарекомендовала себя. Правильно анализируя как потоковые, так и массивные массивы статических данных, мы можем добиться прогресса во многих областях науки и медицины и повысить прибыльность многих предприятий. Практически невозможно представить следующее приложение без потребления данных, создания данных и алгоритмов, управляемых данными. Безопасность, контроль доступа, сжатие, шифрование и соответствие требованиям представляют собой проблемы, которые необходимо решать методично, поскольку компьютерные среды становятся более доступными, среды приложений становятся сетевыми, а системные и аналитические среды совместно используются в облаке. Чтобы сделать обработку Big Data и вычислительную инфраструктуру намного безопаснее, в этом исследовании были изложены наиболее актуальные проблемы безопасности Big Data. В предложенной классификации безопасности Big Data, основанной на веб-языке онтологий, созданной программой-протеже, имеется 32 класса и 45 подклассов. Этот отчет побудит научно-исследовательское сообщество вместе сосредоточиться на проблемах, препятствующих повышению безопасности на платформах Big Data и предстоящих проектах.

Список литературы

1. Красов А. и соавт. Использование методов математического прогнозирования для оценки нагрузки на вычислительные мощности сети IoT // 4-я Международная конференция по будущим сетям и распределенным системам (ICFNDS).— 2020. — С. 1–6.
2. 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.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 321–326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике //Цифровизация образования: теоретические и прикладные исследования современной науки.— 2021. — С. 33–37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 526–530.

УДК 004: 343.9

Криминалистика: сбор убедительных цифровых доказательств

Голубятников Артем Олегович

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

***Аннотация**: В данной статье будет обсуждаться концепция судебно-медицинской экспертизы и методы сбора доказательств. Особое внимание будет уделено методам, используемым для сбора криминалистически обоснованных цифровых доказательств с целью ознакомления с цифровой криминалистикой. Результатом этого обсуждения*

будут выявление и классификация различных типов цифровых криминалистических доказательств, а также четкая процедура сбора криминалистически обоснованных цифровых доказательств. В этом документе будет дополнительно обсуждаться повышение осведомленности и продвигаться идея о том, что компетентная практика сбора данных компьютерной криминалистики важна для приемлемости в суде.

***Abstract**: This paper will discuss the concept of forensic investigation and evidence collection techniques. Emphasis will be placed on the methods used to collect forensically sound digital evidence in order to introduce digital forensics. This discussion will result in the identification and categorization of different types of digital forensic evidence as well as in creation of clear procedure for collecting forensically sound digital evidence. This paper will further discuss raising awareness and promote the idea that competent practice in collecting computer forensic evidence is important for admissibility in court.*

***Ключевые слова**: эталонная модель, электронное обнаружение, Национальный институт стандартов и технологий, алгоритм дайджеста сообщений, алгоритм безопасного хеширования, криминалистически обоснованные цифровые доказательства.*

***Keywords**: Electronic Discovery Reference Model, National Institute of Standards and Technology (NIST), Message-Digest Algorithm, Secure Hash Algorithm, Forensically Sound Digital Evidence*

1. Введение

Компьютерные технологии стали неотъемлемой частью жизни каждого человека и являются одной из наиболее быстро развивающихся областей. Следует отметить, что компьютерные системы хранят ценную информацию о компании и личную информацию (PII), тогда как компьютерная сетевая система предоставляет соответствующие средства доступа или поиска и обработки услуг. В результате они стали основной мишенью для злоумышленников, что приводит к увеличению компьютерных преступлений, о чем далее говорится в этой статье.

Чтобы обеспечить возможность проведения и завершения соответствующих расследований преступлений, используется судебно-медицинская экспертиза. Однако в этой статье мы будем придерживаться цифровой криминалистики, которая является частью криминалистики. Это применение науки для идентификации, сбора, изучения и анализа данных, сохраняя при этом их целостность и поддерживая цепочку хранения данных [1].

Цифровая криминалистика используется для выявления и сохранения цифровых доказательств в их наиболее чистой форме.

Цифровая криминалистика — это область криминалистики, которая занимается поиском, хранением и анализом электронных данных, которые могут быть полезны в уголовных расследованиях [2]. Сюда может входить информация с телефонов, планшетов, компьютеров, жестких дисков, дисков памяти, SD-карт и других устройств хранения данных. С помощью цифровой криминалистики следователь может узнать, кто, что и когда сделал в данной системе.

По словам Дютелла [3] «Цифровые доказательства — это информация и данные, имеющие значение для расследования, которые хранятся, получаются или передаются с помощью электронного устройства».

Для любого успешного и значимого криминалистического расследования или восстановления системы после повреждения жизненно важен сбор достаточных, значимых и криминалистически обоснованных данных. Криминалистическая обоснованность означает, что с момента получения цифровых доказательств и на протяжении всего расследования доказательства должны оставаться в своем первоначальном состоянии [4]. Игнорирование рекомендуемых методов цифровой криминалистики может привести к уничтожению доказательств. Если доказательства повреждены, вероятность того, что они будут отклонены в суде, возрастает.

2. Категории цифровой преступности

Цифровая преступность принимает множество различных форм, и они могут совершаться с использованием различных типов цифровых устройств, таких как сетевые журналы, ячейки памяти компьютера, электронная почта, веб-сайты, периферийные устройства, принтеры и т. д. Основные преступления описаны ниже. Существует три основные категории цифровых преступлений: преступления против людей, преступления против собственности и преступления против общества [5].

Преступления против людей в основном носят личный характер. Это преступления, которые происходят с использованием различных цифровых технологий и направлены против лиц, использующих Интернет и ци-

фровые платформы. Некоторые из них включают в себя кражу личных данных, преступления на почве ненависти с использованием социальных сетей, клевету посредством электронной почты или сообщений, шантаж, эксплуатацию детей, киберпреследование с использованием поддельных личных данных и другие.

Преступления против собственности направлены против собственности отдельных лиц или групп. Преступники ищут интеллектуальную собственность, патенты, деньги и даже кражу имущества. Эти преступления не заботятся ни о каком разрешении авторов или владельцев. Некоторые из отмеченных нарушений связаны с пиратством цифровых носителей, таких как фильмы, песни, программное обеспечение и программы.

Некоторые киберпреступления совершаются против общественных интересов. Киберпреступления против общества включают торговлю от небольших до крупных партий, отмывание денег, преступления против правительства и терроризм, направленный против правительства и общественности.

Все эти преступления зависят от цифровых технологий, таких как мобильные телефоны, компьютеры и небольшие электронные устройства, включая Интернет вещей, которые ведут журналы, которые при необходимости можно проанализировать. Потому что именно эти устройства и сети используются для совершения преступлений.

Примеры подходящих источников данных для киберпреступлений включают файлы журналов, накопители, журналы брандмауэра и дисковые накопители.

3. Виды цифровой криминалистики

Существуют различные типы цифровой криминалистики, и они подробно обсуждаются ниже.

Криминалистика электронной почты — это один из видов цифровой криминалистики, который состоит из изучения и детального анализа электронных писем и их содержания с целью определения их легитимности приемлемым с криминалистической точки зрения способом.

Мобильная криминалистика включает в себя проверку и анализ мобильных устройств, в ходе которых можно исследовать контакты, журналы вызовов, SMS, видео и изображения.

Криминалистика дисков включает извлечение данных из медиахранилищ, что включает поиск активных, редактируемых или удаленных файлов.

Сетевая криминалистика занимается изучением и анализом сетевого трафика для сбора доказательств.

Криминалистика баз данных включает изучение и проверку базы данных и ее метаданных на предмет возможных доказательств.

Криминалистика беспроводной сети — это сбор и анализ трафика беспроводной сети, а также изучение полезной нагрузки на наличие любого вредоносного кода. Это называется криминалистией вредоносного ПО.

Криминалистика памяти занимается сбором данных из памяти систем. К ним могут относиться реестр и кэшированная память.

4. Пять правил достоверных цифровых доказательств

Цифровые доказательства могут использоваться для доказательства невиновности подозреваемого, и в этом случае они относятся к категории оправдательных доказательств, тогда как, если они приводят к обвинительному заключению по уголовным делам, они называются обвинительными доказательствами [4].

Существует 5 общих правил, которым необходимо следовать, чтобы цифровые доказательства были допустимыми, и они включают в себя:

1. Цифровые доказательства должны быть допустимыми. Сбор и сохранение цифровых доказательств рекомендуемым способом жизненно важны для того, чтобы сделать их приемлемыми для жюри или где-либо еще.
2. Цифровые доказательства являются подлинными. Оно должно соотноситься с инцидентом соответствующим образом, чтобы что-то доказать.
3. Цифровые доказательства должны быть четкими и полными. Оно должно быть хорошо выстроено и связано со всей историей. Не следует предоставлять неполные доказательства, поскольку они могут направить решение в ином направлении.

4. Оно должно быть надежным. Инструменты и методология, используемые для цифровых доказательств, не должны вызывать сомнений в их точности и подлинности.
5. Цифровые доказательства должны быть полными, надежными, простыми для понимания, правдоподобными и приемлемыми [4]. Судебно-медицинский эксперт должен быть в состоянии объяснить использованную методологию и способы сохранения целостности.

5. Подходы к сбору данных

Следователь должен определить наилучший возможный метод получения доказательств без изменения исходных данных, запись всех действий, связанных с получением и обработкой исходных данных и копий, должна вестись, он не должен выполнять никаких действий, выходящих за рамки возможностей исследователя. следователь, должен учитывать все вопросы безопасности, законные права, а также организационную политику и процедуры [2]. Сбор цифровых данных для каждого устройства может осуществляться в режиме реального времени или в режиме ожидания.

При сборе данных в реальном времени цифровые данные копируются из работающей исследуемой системы в криминалистическую систему с использованием блокировщика записи и программного обеспечения, такого как FTK imager, для копирования операционных систем на криминалистические устройства вместе с проверкой хэш-функции.

При мертвом получении расследуемые цифровые данные копируются в судебно-медицинскую систему, которую также можно назвать доверенным сервером. Расследуемый/подозрительный диск перемещается и подключается к криминалистической системе в доверенной среде и загружается с доверенного загрузочного устройства, которым может быть USB-накопитель, компакт-диск и т. д.

Несмотря на то, что мертвые сборы предпочтительнее живых, существуют ситуации, когда живые сборы являются единственным вариантом в некоторых случаях, когда критически важные службы не могут быть отключены, поскольку отключение предупредит подозреваемого о том,

что его действия были обнаружены, или создаст риск потери данных. при отключении питания системы.

6. Категории цифровых данных

В ходе цифровой криминалистики цифровые данные классифицируются в зависимости от порядка их изменчивости. И исследователь должен подходить к сбору данных, начиная с наиболее изменчивых данных, заканчивая наименее изменчивыми данными и, наконец, энергонезависимыми данными.

Любые данные, которые теряются при выключении системы, называются нестабильными данными. Например, регистры ЦП, кэш, ОЗУ, кэш ARP, таблицы процессов и т. д. — это некоторые из нестабильных данных, и их следует собирать в первую очередь для работающей системы.

Энергонезависимые данные — это данные, которые сохраняются при отключении питания, например, жесткий диск. Некоторые из энергонезависимых данных — это данные на жестком диске, данные, зарегистрированные на удаленном сервере, резервные копии. Успешный сбор данных должен начинаться с наиболее изменчивых данных и, наконец, осуществляться для данных, которые имеют меньшее снижение волатильности или вообще не имеют его.

7. Методы сбора данных

Для копирования данных из подозрительной системы в доверенную можно использовать три основных метода сбора данных:

1. Сеть может использоваться для копирования данных из подозрительной компьютерной системы на назначенный сервер. Это можно использовать как для живых, так и для мертвых приобретений. Для выполнения упражнения можно использовать инструменты сетевой связи, такие как Netcat. В качестве альтернативы можно выполнить монтирование сетевого диска и скопировать данные на сервер. Подключение устройств хранения, таких как общие сетевые ресурсы, приводы компакт-дисков и жесткие диски, делает файлы доступными через файловую систему компьютера.

2. Подозрительное запоминающее устройство, например жесткий диск, можно удалить из подозрительной системы и подключить к доверенному серверу для доступа к данным.
3. В подозрительной системе может быть подключен или установлен новый жесткий диск. Подозрительная система может загрузиться с доверенного USB-накопителя или привода компакт-дисков и, наконец, создать образ подозрительного диска на новом диске.

Во время сбора доказательств с устройства целевая система может включать накопители SATA, SCSI или IDE. К цели также может быть подключено различное периферийное оборудование.

Хорошей практикой является завершение работы исследуемой системы и загрузка ее в доверенную компьютерную систему, которая используется для расследования. Альтернативно, жесткий диск можно снять и подключить к системе, где будет проводиться судебно-медицинская экспертиза.

Однако в некоторых случаях рекомендуется, чтобы исследуемая машина оставалась включенной для сбора всей информации, необходимой для расследования, из активной памяти, поскольку выключение системы может привести к потере всех данных из ячеек памяти.

Ниже приведены рекомендуемые семь шагов, которые необходимо выполнить при выполнении «мертвой» регистрации:

Шаг 1: Здесь подозрительная система отключается, чтобы позволить следователю отметить и записать, что они установили временную метку, после которой в системе не будет происходить никаких других изменений [5].

Шаг 2. Следующим шагом является удаление диска из подозрительной системы, чтобы убедиться, что форма цепочки поставок создана и заполнена. В цепочке хранения учитываются все люди, которые имели дело с доказательствами. Когда, кто, где были получены доказательства, где они хранились и кто контролировал или владел доказательствами в течение периода с момента их получения [3].

Шаг 3. Проверьте наличие других носителей и удалите все оставшиеся носители, например дисковод гибких дисков и дисковод zip. Для каждого устройства должна быть указана цепочка поставок [1].

Шаг 4. Запишите информацию об унифицированном расширяемом интерфейсе прошивки (UEFI) или базовой системе ввода-вывода (BIOS).

На этом этапе систему можно безопасно загрузить, чтобы проверить информацию BIOS или UEFI. Информация об UEFI или BIOS должна быть указана в форме цепочки поставок. Собираемая информация BIOS или UEFI состоит из системного времени и даты. Время BIOS или системы важно, поскольку оно может отличаться от фактического времени и часового пояса, установленного для географической области, в которой вы находитесь [8].

Шаг 5: включает в себя визуализацию драйвера. Это самая рискованная часть процесса сбора доказательств. Необходимо соблюдать осторожность, чтобы избежать записи на исходный носитель при каждом доступе к нему. Прежде чем использовать диск для хранения образа, вы всегда должны использовать какое-нибудь программное обеспечение для очистки диска от любых предыдущих доказательств [3].

Шаг 6. После создания изображений подозрительного носителя вам необходимо записать криптографические хэши, созданные программами создания изображений. Это может быть дайджест сообщения 5 (MD5), SHA256 и т. д. Криптографический хеш обеспечивает целостность данных [5].

Шаг 7: наконец, упакуйте и пометьте доказательства, четко промаркируйте диск, на который был записан судебно-медицинский образ, и храните его в безопасном месте, без доступа посторонних лиц [1].

8. Сбор и расследование удаленных доказательств

В некоторых случаях подозрительная машина может быть производственной машиной или находиться во враждебной среде, что затрудняет ее выключение. В таких случаях сбор данных должен осуществляться удаленно. В большинстве случаев рекомендуется осмотреть машину перед проведением удаленного сбора. Это позволит проверить наличие подозрительных артефактов на удаленном компьютере перед началом сбора данных [3].

Следователю доступны многочисленные инструменты для проведения криминалистического анализа на удаленном компьютере без физического доступа. Необходимо уметь выполнять ключевые задачи криминалисти-

ческого анализа, включая создание изображений, углубленное изучение подписей файлов, хеширование файлов и копирование файлов на рабочую станцию, используемую в криминалистическом расследовании, а также составление отчетов о подозрительной информации.

В ситуациях, когда дело и целевая среда очень чувствительны, например, за границей, решающее значение имеет возможность сохранить расследование в тайне, чтобы субъект не знал, что он/она находится под следствием. Невыполнение этого требования может поставить под угрозу доказательства и иметь непредвиденные последствия.

Следующие действия могут помочь сохранить тайну расследования:

- Минимизируйте количество одновременных операций, чтобы ограничить использование системных ресурсов.
- Назовите программу удаленного расследования системным именем, например lmhosts.exe.
- Брандмауэры должны быть настроены так, чтобы разрешать входящие соединения с компьютера исследователя.
- Убедитесь, что программа, используемая для проведения удаленного расследования, не оставляет следов событий в журналах событий.
- Ищите только те данные, которые имеют отношение к расследованию.
- Расследование следует проводить, когда подозреваемый ожидает большого количества регулярных действий при антивирусном сканировании жесткого диска.

Одна из важнейших проблем при удаленном сборе данных по сети заключается в том, что машина должна быть включена и работать, а данные на ее жестком диске по большей части постоянно меняются [5]. Следовательно, будет сложно полагаться на хэш MD5 для аутентификации полученных данных. В этом случае достоверность данных будет зависеть от того, насколько надежным будет этот процесс. Необходимо следовать четко определенной процедуре.

В ожидании вредоносной деятельности компании должны быть подготовлены к судебно-медицинской экспертизе. Компании должны создать и внедрить адекватные и стандартные механизмы сбора данных с соответствующей политикой.

9. Проблемы

Со временем сбор судебно-медицинских доказательств столкнулся со многими проблемами. Например, сбор полезных доказательств из огромных наборов данных в терабайтах затрудняет поиск именно того, что необходимо.

Правоохранительные органы и суд отметили недостаток обширных знаний и понимания со стороны прокуроров элементов цифровых доказательств [10].

Недавние технологические обновления повлияли на судебно-медицинские решения, поскольку используемые инструменты могут потребовать либо обновления, либо изменения, что делает их дорогостоящими для судебных экспертов.

10. Вывод

Цифровая криминалистика может быть сложной задачей, и ее трудно начать. В статье представлено комплексное руководство, которое охватывает все этапы сбора криминалистически обоснованных цифровых доказательств с использованием различных подходов и методов сбора живых данных, мертвых данных и удаленного сбора данных. Проблемы обсуждаются кратко.

Список литературы

1. Красов А. и соавт. Использование методов математического прогнозирования для оценки нагрузки на вычислительные мощности сети IoT // 4-я Международная конференция по будущим сетям и распределенным системам (ICFNDS).— 2020. — С. 1–6.
2. 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.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020).— 2020. — С. 321–326.

4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике //Цифровизация образования: теоретические и прикладные исследования современной науки.— 2021. — С. 33–37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021).— 2021. — С. 526–530.

УДК 004

Тестирование и отладка программного обеспечения

Саблина Анастасия Андреевна

студент Югорского государственного университета

Научный руководитель **Усманов Руслан Талгатович**

старший преподаватель Югорского государственного университета

***Аннотация**: В современном мире при разработке программного обеспечения важное место занимают процессы тестирования и отладки. В этой статье дается общее представление об этих процессах (на примере структурного программирования). Качество программного продукта напрямую зависит от того, насколько тщательно эти процессы проведены. В данной статье мы рассмотрим основные аспекты тестирования и отладки, их взаимосвязь и значение для разработки программного обеспечения.*

***Abstract**: In the modern world, testing and debugging processes occupy an important place in software development. This paper gives a general idea about these processes (on the example of structural programming). The quality of a software product directly depends on how thoroughly these processes are carried out. In this article the authors will look at the main aspects of testing and debugging, their interrelationship and importance for software development.*

***Ключевые слова**: программное обеспечение, тестирование, функциональное тестирование, тип тестирования.*

***Keywords**: software, testing, functional testing, type of testing.*

Тестирование программного обеспечения — это процесс анализа программного продукта с целью выявления различий между текущим и же-

лаемым состояниями функционирования программы. Тестирование помогает обеспечить, что программа работает корректно и соответствует всем заявленным требованиям и спецификациям.

Этапы тестирования включают:

1. Планирование — определение объема тестирования и инструментов.
2. Разработку тестов — создание тестовых сценариев и случаев.
3. Выполнение тестов — реализация тестов и фиксация результатов.
4. Анализ результатов — оценка результатов тестирования и определение дефектов.
5. Репортинг — составление отчетов о найденных проблемах.

Категории тестирования:

- Модульное тестирование, или юнит-тестирование, проверяет отдельные части программы.
- Интеграционное тестирование оценивает совместную работу нескольких компонентов.
- Системное тестирование проверяет полностью интегрированное приложение.
- Приемочное тестирование осуществляется для подтверждения готовности продукта на стороне пользователя. [3]

Отладка программного обеспечения — это процесс поиска и устранения ошибок или «багов», выявленных в ходе тестирования. Задачей отладки является точное определение причины возникновения дефекта и его устранение.

Процессы отладки включают:

1. Воспроизведение проблемы — выполнение программы в условиях, при которых проявляется ошибка.
2. Локализация проблемы — определение места в коде, где возникает ошибка.
3. Исправление — изменение кода для устранения ошибки.
4. Повторное тестирование — проверка исправлений на отсутствие ошибки и не внесение новых дефектов.

Инструменты отладки включают отладчики, которые позволяют пошагово выполнять программу и просматривать состояние переменных, а также логгеры, которые регистрируют сообщения о ходе выполняемых

операций. Важно отметить, что тестирование и отладка являются взаимосвязанными процессами. [1]

Тестирование идентифицирует наличие проблем, а отладка направлена на их решение. Однако полное избавление от ошибок практически невозможно, поэтому цель этих процессов — минимизировать их количество и влияние на конечного пользователя

Тестирование и отладка программного обеспечения — ключевые элементы разработки, обеспечивающие выпуск надежного и функционального продукта. Регулярное и тщательное тестирование, наряду с качественной отладкой, помогает снизить риски, связанные с выпуском нестабильного или незащищенного программного обеспечения.

Для обеспечения качества комплексных программных систем наиболее эффективными являются следующие методики тестирования:

1. Автоматизированное тестирование: Позволяет автоматизировать рутинные и повторяющиеся тестовые процедуры, повышая тем самым эффективность тестирования и ускоряя процесс разработки. Использование фреймворков для автоматизации позволяет контролировать поведение комплексных систем в разных сценариях работы.[2]
2. Нагрузочное тестирование: Измеряет способность системы справляться с заданными уровнями нагрузки. Это важно для комплексных систем, так как отклонения в производительности могут иметь значительные последствия для бизнеса.
3. Тестирование безопасности: Особенно важно для систем, которые обрабатывают конфиденциальные данные. Проводится для проверки уязвимостей системы в отношении различных видов атак.
4. Интеграционное тестирование: Проверяет, как модули или компоненты системы работают в совместной среде. Это может быть тестирование интерфейсов взаимодействия между модулями или API.
5. Системное тестирование: Охватывает проверку системных интеграций в полной мере с учетом всех аспектов работы программного продукта.
6. Приемочное тестирование: Выполняется с участием пользователей и служит для проверки комплексного решения в реальных условиях эксплуатации и удовлетворения его требованиям конечных пользователей.

7. Тестирование регрессии: После каждого изменения в коде проводят для убеждения, что новые изменения не привели к появлению новых дефектов или не повлияли отрицательно на существующие функции.

Выбор методики тестирования зависит от конкретной ситуации и может изменяться в зависимости от множества факторов, таких как ресурсы, время, требования заказчика и специфические риски, связанные с проектом. Как правило, эффективное обеспечение качества достигается благодаря комбинации разных методик тестирования, адаптированных под конкретную задачу и условия проекта.

Для автоматизации тестирования комплексных программных систем наиболее подходящие инструменты обычно включают в себя программы, предназначенные для широкого спектра тестов — от модульного до приемочного.

Вот несколько из наиболее популярных инструментов:

1. Selenium: Это один из самых популярных инструментов для автоматизации тестирования веб-приложений. Он совместим с множеством браузеров и поддерживает разные языки программирования, такие как Java, C#, Python и Ruby. [4]
2. Jenkins: Хотя это не инструмент тестирования, Jenkins является непревзойденным инструментом непрерывной интеграции, который можно интегрировать с тестовыми фреймворками для автоматического выполнения тестов при каждом коммите кода.
3. Appium: Это открытое программное обеспечение для автоматического тестирования мобильных приложений. Оно работает с нативными, гибридными и веб-мобильными приложениями и совместимо с iOS и Android.
4. TestComplete: Коммерческий инструмент от SmartBear, поддерживающий автоматическое тестирование для настольных, веб- и мобильных приложений. Он предоставляет простой в использовании интерфейс и возможности скриптинга на нескольких языках.
5. LoadRunner: Коммерческий продукт от Micro Focus для нагрузочного тестирования, помогающий определить производительность системы под критическими нагрузками.

6. QTP/UFT (Unified Functional Testing): Также от Micro Focus, этот инструмент ориентирован на функциональное и регрессионное тестирование веб и настольных приложений.
7. Cucumber: Этот инструмент идеально подходит для автоматизации приемочных тестов с использованием BDD (Behavior-Driven Development). Он позволяет создавать тесты на естественном языке, что делает их понятными для не-технических участников проекта. Выбор инструмента автоматизации тестирования зависит от многих факторов, включая технологический стек, опыт команды и специфические требования проекта. В идеале инструмент должен обладать широкой поддержкой платформ, возможностью интеграции с другими системами и предоставлять широкие возможности для создания сценариев тестирования.
8. Robot Framework: Это популярный инструмент с открытым исходным кодом для автоматизации приемочного тестирования и приемочного тест-драйва разработки (ATDD). Он имеет простой синтаксис данных, поддерживаемый на многих языках, и легко интегрируется с другими инструментами.
9. JMeter: От Apache, этот инструмент используется для тестирования производительности и нагрузки как в веб-приложениях, так и в различных других услугах. Он позволяет симулировать большое количество одновременных пользователей и анализировать результаты в удобной форме.
10. Postman: Инструмент, который в основном используют для автоматизации и тестирования API (REST, SOAP, GraphQL). Постман позволяет легко создавать и выполнять различные запросы к API, а также проверять ответы и сценарии использования. [5]
11. SpecFlow: Для пользователей, работающих с.NET, SpecFlow предлагает подход BDD для автоматизации и выполняет сценарии написанные на языке Gherkin. Он тесно интегрируется с Visual Studio и поддерживает NUnit, xUnit и MSTest для выполнения тестов. При выборе инструментов автоматизации тестирования следует учитывать сложность поддержки инструментария, его удобство в использовании командой проекта и возможность масштабирования под растущие нужды проекта. Это особенно важно для комплексных программных систем, для которых внедрение автоматических тестов может быть сложной задачей.[6]

Список литературы

1. Бейзер Б. Тестирование черного ящика. Технологии функционального тестирования программного обеспечения и систем [текст] / Б. Бейзер; — Питер, 2022, 320 с. ISBN 5–94723–698–2.
2. Брауде Э. Д. Технология разработки программного обеспечения [текст] / Э. Д. Брауде; — Питер, 2020, 656 с. ISBN 5–94723–663-X.
3. Винниченко И. В. Автоматизация процессов тестирования [текст] / И. В. Винниченко; — Питер, 2021, 208 с. ISBN 5–469–00798–7.
4. Канер С. Тестирование программного обеспечения. Фундаментальные концепции менеджмента бизнес-приложений [текст] / С. Канер; — ДиаСофт, 2020, 544 с, ISBN 966–7393–87–9.
5. Калбертсон Р. Быстрое тестирование [текст] / Р. Калбертсон, К. Браун, Г. Кобб; — Вильямс, 2022, 384 с. ISBN 5–8459–0336-X.
6. Коликова Т. В. Основы тестирования программного обеспечения. Учебное пособие [текст] / Т. В. Коликова, В. П. Котляров; — Интуит, 2016,— 285 с. ISBN 5–85582–186–2.
7. Касперски К. Техника отладки программ без исходных текстов [текст] / К. Касперски; — БХВ-Петербург, 2022, 832 с. ISBN 5–94157–229–8.

УДК 004

Администрирование операционных систем на базе Linux: методы, инструменты и стратегии

Саблина Анастасия Андреевна

студент Югорского государственного университета

Научный руководитель **Годовников Евгений Александрович**

доцент Югорского государственного университета

***Аннотация**: Статья посвящена вопросам администрирования операционных систем на базе Linux. Описываются основные принципы и практики управления Linux-системами, а также рассматриваются инструменты и стратегии, которые*

администраторы могут использовать для повышения эффективности и безопасности системы.

***Abstract**: The article is devoted to the issues of Linux-based operating systems administration. It describes basic principles and practices of managing Linux systems, and discusses tools and strategies that administrators can use to improve system efficiency and security.*

***Ключевые слова**: командная строка, файловая система, пакетный менеджер, установка ПО, конфигурационные файлы, системный мониторинг, безопасность, разрешения и права доступа, пользователи и группы, сервер, сетевые утилиты, журналирование системы, резервное копирование.*

***Keywords**: command line, file system, package manager, software installation, configuration files, system monitoring, security, permissions and access rights, users and groups, server, network utilities, system logging, backup.*

Linux является одной из самых популярных и гибких операционных систем, используемых в серверных решениях, встроенных системах и как рабочая платформа для разработчиков и исследователей. Открытая архитектура и широкий набор доступных инструментов делают Linux идеальной средой для администрирования. Однако, динамичность современных технологий требует от администратора глубоких знаний и бдительности в постоянном обучении новым методам и подходам. [6]

Стандартный набор инструментов системного администратора Linux включает:

a. Командная строка (Bash, Zsh) и скриптинг.
b. Редакторы (Vim, Nano, Emacs).
c. Средства для работы с файловой системой (ls, cp, mv, mount, fdisk).
d. Инструменты для управления процессами (ps, top, htop, kill).
e. Сетевые утилиты (ip, netstat, ss, tcpdump, nmap).
f. Планировщик задач (cron, at).
g. Менеджеры пакетов (apt, yum, dnf, pacman).

Безопасность:

a. Настройка и использование firewall (iptables, nftables, ufw).
b. Обеспечение безопасности при помощи SELinux или AppArmor.
c. Регулярные обновления и патчи для системы и установленного ПО.
d. Настройка аутентификации и авторизации (PAM, LDAP, Kerberos).

e. Использование зашифрованных протоколов для удаленного доступа (SSH, VPN). [3]

Автоматизация и оркестрация:

a. Системы управления конфигурациями (Ansible, Puppet, Chef).

b. Контейнеризация и виртуализация (Docker, KVM, LXC).

c. Использование CI/CD пайплайнов для автоматизации развертывания (Jenkins, GitLab).

Мониторинг и производительность: a. Настройка и использование систем мониторинга (Nagios, Zabbix, Prometheus). b. Анализ производительности и устранение узких мест (perf, sysstat, vmstat). c. Логирование и централизованный сбор логов (rsyslog, ELK stack).

Резервное копирование и восстановление: a. Решения для резервного копирования (rsync, Bacula, Amanda). b. Стратегии копирования данных и катастрофического восстановления. c. Снапшоты файловых систем и репликации (LVM, ZFS, DRBD).

Администрирование Linux-систем требует не только знаний конкретных инструментов, но и понимания общих принципов работы операционной системы, сетевых технологий и информационной безопасности. Континуальное обучение, развитие навыков и адаптация к изменяющейся технологической среде являются ключевыми факторами, способствующими эффективности системного администратора. [1]

Эффективное администрирование ОС Linux требует от системного администратора понимания того, как максимально использовать возможности системы с учетом требований безопасности, надежности и доступности. Внимание следует уделять не только поддержке текущего функционирования, но и планированию на будущее, включая масштабируемость и устойчивость к сбоям.

Одной из важнейших задач системного администратора является создание проактивной стратегии, которая включает в себя мониторинг системы для предотвращения проблем, а не просто отклик на уже возникшие ситуации. Комбинация надежной автоматизации, четкой документации процессов и проведение частых проверок готовности системы к аварийным сценариям повысит устойчивость инфраструктуры к неожиданным проблемам и сократит время реакции на инциденты. [2]

Кроме того, значимым аспектом в администрировании Linux является сообщество. Обмен знаниями и опытом с другими администраторами и разработчиками является неотъемлемой частью процесса обучения и может существенно улучшить подходы к управлению системами. В заключении, глубокое понимание принципов работы Linux, непрерывное изучение новых технологий, использование проверенных практик и инструментов, а также участие в сообществе позволят системным администраторам поддерживать надежные и эффективные операционные системы, способные стойко переносить вызовы современного технологического ландшафта. [4]

Методы проактивного мониторинга и предотвращения проблем в ОС Linux:

1. Предиктивный анализ: Использование инструментов анализа данных и машинного обучения для распознавания образцов, которые предшествуют возникновению проблем. Такие системы могут автоматически оповещать администраторов о потенциальных угрозах, еще до того, как они станут критическими.
2. Периодические аудиты безопасности: Регулярное сканирование системы на наличие уязвимостей с использованием инструментов типа OpenVAS, Nessus или Lynis. Это помогает выявлять и устранять уязвимости, прежде чем они будут эксплуатироваться в атаках.
3. Автоматизированное тестирование производительности: Проактивное мониторинг нагрузки на системные ресурсы, такие как CPU, память и дисковое пространство, с помощью инструментов типа Stress-ng, чтобы определить потенциальные узкие места до того, как они станут серьезной проблемой.
4. Централизованный сбор логов: Настройка таких систем как ELK Stack или Graylog для агрегации и анализа журналов с нескольких систем и приложений. Это помогает выявлять нестандартные паттерны или подозрительную активность на ранних стадиях.
5. Раннее обнаружение сетевых аномалий: Использование инструментов для мониторинга сети, таких как Nagios, Zabbix или Prometheus, позволяет выявлять необычное сетевое поведение, что может быть индикатором нарушений или неисправностей в работе. [1]

6. Резервное копирование и тестирование процедур восстановления: Регулярное выполнение резервного копирования данных и тестирование процессов восстановления убедит в том, что в случае сбоя системы, данные могут быть восстановлены эффективно и в короткие сроки. 7. Использование configuration drift tools: Инструменты для отслеживания изменений конфигурации, такие как Ansible Tower, помогают контролировать отклонения от эталонных конфигураций и автоматически корректировать их.

Процесс резервного копирования и восстановления может быть интегрирован в систему проактивного мониторинга с помощью следующих шагов: [4]

1. Инструменты для контроля резервного копирования: Использование решений, таких как Bacula, Amanda или Rsync, в сочетании с мониторинговыми системами, чтобы отслеживать статус выполнения резервного копирования и успешное завершение задач.
2. Сообщения и оповещения: Настраивание систем мониторинга, типа Nagios или Zabbix, для отправки алертов системному администратору в случае ошибок в процессе резервного копирования или при выявлении нерегулярностей в доступности бэкапов.
3. Автоматическое триггерное копирование: Настройка скриптов или использование инструментов управления конфигурациями, например Ansible, для автоматического выполнения резервного копирования при определенных условиях, таких как изменение файлов или предупреждения системы мониторинга.
4. Регулярное и случайное тестирование восстановления: Автоматизация процесса восстановления для проверки целостности и доступности резервных копий, а также убедиться в том, что процесс восстановления работает адекватно и в заданные сроки.
5. Интеграция с облачными хранилищами: Внедрение систем, которые автоматически отправляют бэкапы в облачные сервисы типа AWS S3 или Google Cloud Storage, и мониторинг их доступности и целостности. 6. Определение метрик эффективности: Настройка отслеживания таких метрик, как время выполнения бэкапа, скорость восстановления, а также размер и целостность бэкапов. Интеграция данных шагов обес-

печивает не только автоматизацию процесса резервного копирования и восстановления, но и повышает уверенность в возможности быстрого восстановления ИТ-инфраструктуры предприятия после сбоев. [1]

Для проверки и подтверждения целостности резервных копий в автоматизированных системах можно следовать следующим лучшим практикам:

1. Реализация чек-сумм и хэшей: Автоматическое создание чек-сумм (например, MD5 или SHA-256) во время процесса резервного копирования позволяет проверять целостность данных при каждом восстановлении.
2. Тестирование восстановления: Регулярное проведение восстановления на тестовых системах или изолированных средах для проверки целостности данных и работоспособности системы.
3. Включение резервного копирования в состав регламентных работ: Запланированное автоматизированное резервное копирование должно проходить соответствие регламентным процедурам, включая проверку целостности.
4. Журналирование и аудит: Автоматическое ведение логов процесса резервного копирования и восстановления, включая любые ошибки, предупреждения и иные события.
5. Локальное и удаленное хранение копий: Хранение копий данных как в локальных, так и в отдаленных местах повышает шансы на сохранность данных в случае сбоев на местах хранения. [3]
6. Автоматизированные оповещения: Уведомления о любых ошибках или проблемах, возникших при резервном копировании или восстановлении, посылаемые ответственным лицам.
7. Установка пороговых значений и базовых линий: Определение нормальных параметров операции резервного копирования и восстановления для быстрого определения аномалий. [7]
8. Разделение прав и обязанностей: Гарантирование того, что отдельные члены команды обладают необходимыми полномочиями для управления резервным копированием, но при этом поддерживается сегментация обязанностей для предотвращения внутренних угроз.

Применение этих практик может существенно улучшить процесс резервного копирования и восстановления, минимизируя риск потери данных и обеспечивая надежную работу системы. [8]

Список литературы

1. Робачевский А.М., «Операционная система Unix®», СПб. БВХ — Санкт-Петербург, 2020.
2. Армстронг (мл.) Джеймс, «Секреты Unix®»: 2-е изд, М.: Издательский дом «Вильямс», 2021.
3. Паркер Тим, «Linux 5.2. Энциклопедия пользователя», К.: Издательство «ДиаСофт», 2021.
4. Oscar Anderson, Iptables Tutorial,2020.
5. Шевель А, «Linux. Обработка текстов. Специальный справочник», Спб.: Питер, 2022.
6. Системная справочная служба Linux Man,2023.
7. Д. Тейнсли, “Linux и Unix: программирование в shell Руководство разработчика”, К.: Издательская группа BHV, 2022.
8. Справочная система Midnight commander,2020.

УДК 004.056

Разработка DCAP-модуля DLP-системы

Шашин Михаил Антонович

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

***Аннотация**: Статья предоставляет важные сведения о том, какие требования определены для DCAP-системы, требуемый функционал для эффективного обеспечения безопасности файловой системы и защиты конфиденциальных данных от утечек и несанкционированного доступа, а также преимущества использования DCAP-системы с DLP-системой для обеспечения комплексной защиты от утечек данных.*

***Abstract**: The article provides important insights into what requirements are defined for a DCAP system, the required functionality to effectively secure the file system and protect sensitive data from leaks and unauthorized access, and the benefits of using a DCAP system with a DLP system to provide comprehensive protection against data breaches.*

***Ключевые слова**: DCAP-система, DLP-система, аудит файловой системы, групповые политики, права доступа.*

***Keywords**: DCAP-system, DLP-system, file system auditing, group policies, access rights.*

Введение

Системы файлового аудита класса DCAP предназначены для автоматической идентификации и решения проблем, связанных с хранением и использованием данных.

Они структурируют содержимое файлового хранилища, определяют права доступа и выделяют данные, которые не должны быть общедоступными.

Они также могут выполнять удаленный сбор информации, анализировать доступы и классифицировать документы с конфиденциальной информацией.

DCAP также позволяет обнаруживать различные аномалии и мониторить подозрительное поведение без постоянного контроля отдельных пользователей.

DCAP (data-centric audit and protection) — это подход к защите информации, который сосредоточен на данных, а не на пользователях, приложениях или каналах передачи данных. DCAP позволяет определить, какие данные являются конфиденциальными, где они хранятся, кто имеет к ним доступ и какие политики безопасности должны быть применены. Он также включает в себя мониторинг и аудит данных, чтобы обнаружить любые изменения, которые могут указывать на злоумышленную деятельность. DCAP позволяет защитить конкретные данные, а не всю организацию в целом, что делает его масштабируемым и выгодным для бизнеса. DCAP-системы могут помочь компаниям навести порядок в файловых хранилищах, определить права доступа и выделить данные, которые не должны быть общедоступными. Они также могут выполнять удаленный сбор информации, анализировать доступы и классифицировать документы с конфиденциальной информацией.

Перед системами файлового аудита класса DCAP стоит три основных задачи:

1. Обнаружение и классификация данных.
2. Мониторинг пользовательских прав и обращений к данным.

3. Защита данных от нежелательного доступа и использования.

То есть система должна анализировать содержимое файловых хранилищ, выделять в них чувствительную информацию и предотвращать действия пользователей, способные ей навредить.

Логика работы DCAP

Чтобы защитить данные в покое, службе ИБ нужно последовательно пройти несколько этапов. Для наглядности рассмотрим их последовательно.

Шаг 1. Определить чувствительную информацию

Перед началом поиска необходимо определить, какие виды документов используются в компании. Это можно сделать, исходя из бизнес-процессов или требований регулятора. В любой компании встречаются кадровые, бухгалтерские документы, финансовая отчетность, приказы начальства, клиентские договоры и базы контактов, и все они требуют контроля. Другой подход — руководствоваться требованиями регулятора. Например, если законом охраняются персональные данные, то необходимо искать номера паспортов, а если техническое описание объекта составляет тайну, то нужно искать в файлах его фрагменты. В DCAP-системе существуют шаблоны правил классификации, включающие универсальные типы данных, такие как ПДн, документы с грифом «коммерческая тайна» и другие. Эти шаблоны позволяют классифицировать данные с помощью нескольких поисковых алгоритмов, таких как поиск по ключевым словам, фразам, регулярным выражениям, атрибутам и другим.

DCAP-система содержит шаблоны правил классификации, которые включают универсальные типы данных, такие как ПДн, документы с грифом «коммерческая тайна», номера телефонов и кредитных карт, а также возможность создания новых категорий. В DCAP-системе можно использовать предустановленные шаблоны для модуля классификации, которые анализируют каждый документ на хранилищах данных. Кроме того, в DCAP-системе можно создавать неограниченное количество новых категорий, что позволяет более точно классифицировать данные.

Чтобы классифицировать данные, DCAP-система ищет внутри файлов признаки, по которым их можно отнести к той или иной категории. Для этого используется несколько поисковых алгоритмов:

- по ключевым словам, фразам и последовательности символов;
- по словарям;
- по регулярным выражениям;
- по степени схожести с заданным образцом;
- по атрибутам;
- по «ручным» меткам.

Все алгоритмы поиска могут быть объединены в сложные запросы, что позволяет, например, искать одновременно по фрагменту текста и атрибуту файла. Поиск будет работать и по документам нетекстовых форматов благодаря OCR-модулю, который позволяет алгоритмам анализировать контент отсканированных и сфотографированных документов.

Когда правила созданы, DCAP-система в соответствии с ними анализирует содержимое всех файлов в системе и автоматически ставит на них метки классификации. Эти метки выполняют сразу две важные функции.

Во-первых, они визуально маркируют нужный контент — при просмотре дерева папок в DCAP-системе у каждого файла, попавшего под правило, будет цветной «флаг» с названием категории. Службе ИБ не придется прочитывать каждый вручную, чтобы понять, что внутри. При этом пользователям такая метка будет не видна.

Во-вторых, метки «резюмируют» всю информацию о файле. Они хранятся в файловой системе и при обращении к файлу выполняют роль «инструкции», как его обрабатывать. Метка характеризует не атрибуты и свойства файла, а его содержимое. Поэтому она не исчезнет, если пользователь переименует или изменит расширение файла, а если скопирует его или пересохранит текст в новом документе — автоматически появится и на нём.

Автоматическую классификацию можно дополнить вручную. «Ручные» метки могут отражать рекомендуемый уровень доступа к файлу, такие как «Общедоступные», «Для служебного пользования» и другие. Название и формат отображения меток можно настроить. Пользователи могут устанавливать эти метки сами, если служба информационной безопасности

предоставит им такое право. Это позволяет авторам документов лучше определить, насколько чувствительная информация содержится в них. Например, главный бухгалтер может установить метку «Для служебного пользования» на финансовый отчет уже при его создании.

Шаг 2. Определить границы поиска

Благодаря автоматической и ручной классификации файлов DCAP-система понимает, какие данные нужно защищать. Следующим этапом является обнаружение файлов, которые попадают в уязвимые категории, в общем массиве данных в компании. Для этого необходимо запустить мониторинг файлового хранилища, чтобы обеспечить возможность самостоятельного отслеживания текущих параметров.

Даже конфиденциальные документы могут быть обнаружены на компьютере обычного пользователя или в общей папке, доступной всей компании. Кроме того, множество конфиденциальных документов могут быть потеряны в множестве пользовательских файлов и папок. Поэтому необходимо контролировать все директории, где могут храниться важные файлы, и составить «карту» таких хранилищ. Если в результате аудита критические документы будут обнаружены в непредназначенных для них местах, необходимо принять меры для устранения этой проблемы. Для этого необходимо запустить мониторинг файлового хранилища, чтобы обеспечить возможность самостоятельного отслеживания текущих параметров.

Файловый аудитор использует агентский и сетевой режимы сканирования при помощи модулей, использующих библиотеку GFAL2 (Grid File Access Library ver.2) на серверной и клиентской части. Первый контролирует ПК и локальные сервера, второй — сетевые хранилища.

При первом сканировании программа вычитывает всю структуру и содержимое файлов в хранилищах. В мониторинг можно включить любое количество компьютеров и серверов, если требуется — сузить его до отдельных машин или даже папок. Кроме того, из сканирования можно исключить файлы и папки по заданным атрибутам. Например, чтобы не тратить ресурсы ПО на анализ системных файлов, можно задать в исклю-

чения соответствующую категорию объекта, его расширение, расположение и др.

DCAP-система проверяет только новые или измененные файлы, запуская проверку при обращении к файлу, например, при его открытии, редактировании, переименовании или перемещении. Это позволяет системе мгновенно обнаруживать появление новых конфиденциальных файлов в компании и немедленно приступать к их защите.

Мониторинг DCAP-системы происходит незаметно для пользователя: сканирование не влияет на производительность ПК и не мешает работе с файлами. Например, система не будет сканировать файл, пока он открыт у сотрудника. Кроме того, специалист по информационной безопасности может настроить проверку по окончании рабочего времени или установить условие: сканирование происходит только при загрузке ЦП менее N% и только в отсутствие активных сессий.

Система визуализирует все контролируемые директории, и для каждого файла в сканируемых папках доступна подробная информация: какие метки на файле установлены вручную и автоматически, кто, когда и как взаимодействовал с файлом в последний раз. Также можно просмотреть содержимое файла и узнать, почему система отнесла его к той или иной категории.

DCAP-система позволяет настраивать выдачу информации с помощью фильтров. Например, можно отображать только файлы на определенных ПК, с определенным названием, созданные или измененные за определенное время. Также можно искать по содержимому документов с метками, например, паспортные данные шефа среди всех файлов из категории «ПДн». Доступна фильтрация по атрибутам, владельцам документов, операциям с ними и системным событиям, таким как изменение прав доступа, прекращение контроля файла и другие.

Шаг 3. Определить, кто и как работает с данными — и кому это можно и нельзя

Для выявления рисков утечки информации необходимо иметь представление о слабых местах в жизненном цикле уязвимых документов. По-

этому специалисту по информационной безопасности необходимо иметь наглядное представление о том, кто, когда и как обращается к файлам. Важно иметь доступ ко всем операциям с файлами и папками с привязкой к конкретному пользователю.

DCAP-система регистрирует все действия пользователей в «умном» журнале. Для каждого документа доступна история обращений, включая информацию о времени создания, изменения, последнем открытии, а также о том, кто совершил эти действия. Также можно осуществлять поиск по отдельным операциям, например, отображать только переименованные документы.

Особого контроля требуют нежелательные действия: например, копирование контента, нерегламентированные правки или удаление содержимого потенциально могут обернуться проблемами для компании.

Для отслеживания подобных инцидентов можно задать политики безопасности, которые уведомят службу информационной безопасности в случае критических событий с файлами. Кроме того, к срабатыванию политики можно привязать запуск внешних скриптов.

Для отслеживания подобных инцидентов можно настроить политики безопасности не только по операциям, но и по системным событиям, например, если файл перестал попадать под правило, а также по изменению прав пользователей.

Мониторинг пользовательских привилегий — важнейшая задача DCAP. Система должна определять, какие документы нуждаются в дополнительной защите, и выявлять избыточные доступы.

DCAP-система осуществляет анализ прав доступа пользователей к файловой системе, что позволяет службе информационной безопасности видеть, какие сотрудники имеют доступ к критической информации. Эта информация представлена в удобном едином представлении, что упрощает процесс отслеживания и аудита. Аудитор видит полный список пользователей, имеющих доступ к файлу, а также операции, доступные им. Например, можно увидеть всех сотрудников, имеющих право на редактирование и удаление файла, или только тех, кому доступ к файлу запрещен. Также возможен поиск файлов, доступных или запрещенных для определенных пользователей.

Также есть возможность получить подробные отчеты о ресурсах. Отчеты «Права доступа к ресурсам» и «Владельцы ресурсов» содержат наиболее полную информацию о пользовательских разрешениях. Отчет «Владельцы ресурсов» помогает безопасно распределить права доступа к новым объектам (документам или папкам), появившимся в файловой системе. Отчет о наследовании прав отображает, как распределены права пользователей на подпапки и файлы внутри крупных директорий, указывает на ошибки наследования и позволяет обратить внимание на объекты, к которым заданы права, не соответствующие правилам доступа к родительским папкам. Эти отчеты позволяют аудитору видеть полный список пользователей, имеющих доступ к файлу, а также операции, доступные им. Например, можно увидеть всех сотрудников, имеющих право на редактирование и удаление файла, или только тех, кому доступ к файлу запрещен. Также возможен поиск файлов, доступных или запрещенных для определенных пользователей.

Чтобы правильно интерпретировать отчеты, полезно свериться с должностными инструкциями: кому из пользователей действительно положен доступ к данным, а кто пользуется им просто так — потому что может. Нужно ли строго следовать букве нормативов, решать вам. Но очевидно, что, например, возможность прочитать проекты приказов руководства до опубликования ни к чему линейному персоналу.

Шаг 4. Настроить защиту

DCAP без проактивной защиты файлов не DCAP. Третья важная функция этого класса решений — превентивная.

Чтобы посторонние не получили доступ к критичной информации, службе ИБ нужно настроить пользовательские права, задать белые/черные списки, запретить потенциально опасные действия: например, возможность прикрепить конфиденциальный документ к письму или сообщению в мессенджере.

Задачу решают **контентные блокировки**. В DCAP-системе для каждой категории документов можно задать ограничения: кому, на каких ПК и в каких приложениях с ними разрешено или запрещено работать. Блокировки применяются по меткам автоматической и ручной классификации.

DCAP-система способна ограничивать доступ к файлам через любые приложения, независимо от их версии, типа или происхождения, включая системные процессы и корпоративное программное обеспечение. Ограничения применяются в файловой системе, где система разрешает или запрещает приложениям доступ к данным. Например, если установлен запрет на чтение файлов с меткой «Финансовая отчетность» в MS Outlook для пользователей, не входящих в группу «Бухгалтерия», приложение не сможет открыть такой документ и, следовательно, не сможет прикрепить его в качестве вложения к письму при отправке.

Файловый аудитор системы может управлять правами пользователей, включая разрешения в операционной системе, непосредственно из своего интерфейса. Это позволяет гибко настраивать разрешения на конкретные операции с файлом (чтение, редактирование, исполнение, перемещение, копирование и т.д.), а также доступ к целым директориям. Эта функция помогает быстро решать проблемы, такие как неправильное назначение прав на файлы, например, когда пользователь получает права на файл, к которому у него нет доступа к родительской папке. Удаление избыточных прав можно осуществить одним нажатием с помощью кнопки в контекстном меню, что более быстро и удобно, чем ручная настройка через интерфейс операционной системы.

Еще одна защитная функция DCAP-системы — **теневое копирование**.

DCAP-система может архивировать и хранить заданное количество версий критичных файлов, что позволяет отслеживать историю изменений и оперативно восстанавливать важную информацию в случае ее кражи, шифрования, искажения или удаления. Эта функция обеспечивает сохранность данных и возможность восстановления информации в случае возникновения проблем с файлами.

DCAP-система может архивировать и хранить заданное количество версий критичных файлов, что позволяет отслеживать историю изменений и оперативно восстанавливать важную информацию в случае ее кражи, шифрования, искажения или удаления. Теневые копии хранятся в зашифрованном виде на сервере, и система сохраняет только те объекты, для которых заданы соответствующие настройки. Кроме того, эти копии формируют индекс, по которому становится доступен полнотекстовый

поиск, что позволяет службе информационной безопасности искать информацию внутри архивированных файлов.

Количество сохраненных версий каждого уникального файла можно определить, чтобы устаревшие копии, с которыми пользователи перестали взаимодействовать, автоматически удалялись из хранилища.

Результаты работы DCAP

Файловый аудитор DCAP-системы помогает службе ИБ понять, как устроен корпоративный документооборот. Это позволяет легче навести порядок в файловых хранилищах и следить за соблюдением порядка, чтобы избежать инцидентов из-за потери, искажения или случайного распространения чувствительных данных. DCAP-система фиксирует все пользовательские операции в «умный» журнал, который позволяет просмотреть историю обращений к каждому документу, а также управлять правами пользователей прямо из своего интерфейса. Кроме того, DCAP-система может блокировать доступ к файлу через любое приложение вне зависимости от его версии, типа, происхождения, а также архивировать и хранить заданное количество версий критичных файлов для отслеживания истории изменений и оперативного восстановления важной информации в случае ее кражи, шифрования, искажения или удаления.

Использование DCAP-системы усиливает эффективность других инструментов информационной безопасности. Например, совместное использование DCAP и DLP систем обеспечивает комплексную защиту от утечек. DCAP ограничит доступ к файлам, а DLP отследит все случаи, когда пользователи попытаются отправить выдержки из них в сообщениях или письмах, или составит контентный маршрут пересылки важного файла между сотрудниками.

Список литературы

1. 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.

2. 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.
3. Гельфанд А. М., Гвоздев Ю. В., Штеренберг С. И. Исследования недостатков языков высокоуровнего программирования для осуществления скрытого вложения в исполнимые файлы // Актуальные проблемы инфотелекоммуникаций в науке и образовании.— 2015. — С. 295–297.
4. Шемякин С. Н. и др. Теоретическая оценка использования математических методов прогнозирования загрузки виртуальной инфраструктуры // Наукоемкие технологии в космических исследованиях Земли.— 2021. — Т. 13.— № . 4. — С. 66–75.
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.

УДК 004.056

Сниффинг пакетов и обнаружение сниффера в сети

Шашин Михаил Антонович

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

***Аннотация**: Сниффинг пакетов — это процесс мониторинга и перехвата всех пакетов данных, проходящих через заданную сеть, с помощью программного приложения или аппаратного устройства. Снифферы могут использоваться для мониторинга всех видов трафика, как защищенного, так и незащищенного. Используя снифферы, злоумышленник может получить информацию, которая может быть полезна для дальнейших атак. В данной статье рассматриваются основы работы сниффера пакетов, сетевые протоколы, уязвимые для сниффера, различное программное обеспечение, которое может быть использовано для сниффера. Также описываются возможные методы защиты от атак сниффера. Наконец, в конце статьи описываются некоторые*

методы обнаружения снифферов. Снифферы не являются инструментами взлома, но они могут помочь хакеру в проведении дальнейших атак, таких как перехват сеанса, DOS-атаки, MITM-атаки и т.д.

***Abstract**: Packet sniffing is the process of monitoring and intercepting all data packets traveling through a given network using a software application or hardware device. Sniffers can be used to monitor all types of traffic, both secure and insecure. Using sniffers, an attacker can obtain information that can be useful for further attacks. This article discusses the basics of packet sniffers, network protocols vulnerable to sniffers, different software that can be used for sniffing. It also describes possible methods of defense against sniffer attacks. Finally, the paper concludes by describing some methods of sniffer detection. Sniffers are not hacking tools, but they can help a hacker to conduct further attacks such as session hijacking, DOS attacks, MITM attacks, etc.*

***Ключевые слова**: сниффер, анализ трафика, MITM-атака, мониторинг сетевого трафика.*

***Keywords**: sniffer, traffic analysis, MITM attack, network traffic monitoring.*

Введение

Сниффер — это программа или устройство, которое подслушивает сетевой трафик, перехватывая информацию, проходящую по сети. По сути, снифферы представляют собой технологию «перехвата данных». Они работают потому, что Ethernet построен по принципу совместного использования. Большинство сетей используют широковещательную технологию, при которой сообщения для одного компьютера могут быть прочитаны другим компьютером в этой сети. На практике все остальные компьютеры, кроме того, которому предназначено сообщение, будут его игнорировать. Однако можно заставить компьютеры принимать сообщения, даже если они не предназначены для них. Это делается с помощью сниффера.

Используя сниффинг, злоумышленник может перехватить такие пакеты, как Syslog-трафик, DNS-трафик, веб-трафик, Email и другие типы трафика данных. Перехватывая эти пакеты, злоумышленник может раскрыть такую информацию, как данные, имя пользователя и пароли от таких протоколов, как HTTP, POP, IMAP, SMTP, FTP и Telnet. Процесс сниффинга осуществляется с использованием портов Promiscuous. В данной статье

рассматриваются основные принципы работы пакетного сниффера, протоколы, уязвимые для сниффинга, различные типы инструментов, используемых для сниффинга, методы защиты от сниффинг- атак и методы обнаружения сниффинга.

В процессе сниффинга злоумышленник подключается к целевой сети для перехвата пакетов. Используя снифферы, которые переводят сетевую карту (NIC) атакующей системы в режим promiscuous, злоумышленник перехватывает пакет. Перехватив пакет, злоумышленник может расшифровать его для извлечения информации. Снифферы могут использоваться для взлома системы или сети.

Протоколы, уязвимые для сниффинга

Следующие сетевые протоколы уязвимы для сниффинга. Основной причиной взлома этих протоколов является получение конфиденциальных данных, например паролей.

Telnet и Rlogin

Telnet — это протокол, используемый для связи с удаленным хостом (через порт 23) в сети с помощью терминала командной строки. Rlogin позволяет злоумышленнику удаленно войти в сетевую машину через TCP-соединение. Оба протокола не обеспечивают шифрования. Поэтому данные, проходящие между клиентами, подключенными по любому из этих протоколов, находятся в открытом виде и уязвимы для перехвата. Злоумышленники могут перехватывать нажатия клавиш, включая имена пользователей и пароли.

HTTP

Из-за уязвимостей в стандартной версии HTTP сайты, использующие HTTP, передают пользовательские данные по сети в виде открытого текста, который злоумышленники могут прочитать и похитить учетные данные пользователя.

SNMP

SNMP — это протокол на базе TCP/IP, используемый для обмена управляющей информацией между устройствами, подключенными к сети. Первая версия SNMP (SNMPv1) не обеспечивает надежной защиты, что приводит к передаче данных в открытом текстовом формате. Злоумышленники используют уязвимости этой версии для получения паролей в открытом виде.

NNTP

Network News Transfer Protocol (NNTP) распространяет, запрашивает, извлекает и размещает новостные статьи, используя надежную потоковую передачу новостей среди сообщества ARPA-Internet. В протоколе отсутствует шифрование данных, что дает злоумышленнику возможность перехватить конфиденциальную информацию.

POP

Протокол Post Office Protocol (POP) позволяет рабочей станции пользователя получать доступ к почте с сервера почтовых ящиков. Пользователь может отправлять почту с рабочей станции на почтовый сервер по протоколу Simple Mail Transfer Protocol (SMTP). Из-за слабой защиты протокола злоумышленники могут легко перехватывать данные, проходящие по сети POP в виде открытого текста.

FTP

Протокол передачи файлов (FTP) позволяет клиентам обмениваться файлами между компьютерами в сети. Этот протокол не обеспечивает шифрования. Поэтому злоумышленники перехватывают данные, а также учетные данные пользователей, используя такие инструменты, как Cain&Abel.

IMAP

Протокол Internet Message Access Protocol (IMAP) позволяет клиенту получать доступ к электронным почтовым сообщениям на сервере и манипулировать ими. Этот протокол не обладает достаточной степенью защиты, что позволяет злоумышленникам получать данные и учетные данные пользователей открытым текстом.

Защита от сниффинга

В этом разделе описаны контрмеры и возможные методы защиты, которые могут быть использованы для защиты целевой сети от атак типа sniffing. Ниже перечислены некоторые контрмеры, которые можно использовать для защиты от сниффинга.

- Ограничьте физический доступ к сетевым носителям, чтобы исключить возможность установки пакетного сниффера.
- Для защиты конфиденциальной информации используйте сквозное шифрование. Постоянно добавлять MAC-адрес шлюза в ARP-кэш.
- Отключите широковещательную передачу идентификации сети и, по возможности, ограничьте доступ к сети авторизованным пользователям, чтобы защитить сеть от обнаружения средствами сниффинга.
- Использование протокола IPv6 вместо протокола IPv4
- Для защиты пользователей беспроводной сети от атак сниффинга используйте зашифрованные сеансы, например SSH вместо Telnet, SecureCopy (SCP) вместо FTP, SSL для подключения к электронной почте и т.д.
- Для защиты имен пользователей и паролей используйте HTTPS вместо HTTP.
- Используйте коммутатор вместо концентратора, поскольку коммутатор доставляет данные только тому, кому они предназначены.
- Для безопасной передачи файлов используйте протокол Secure File Transfer Protocol (SFTP) вместо FTP.
- Используйте PGP и S/MIME, VPN, IPSec, SSL/TLS, SecureShell (SSH) и одноразовые пароли (OTP).

- Всегда шифруйте беспроводной трафик с помощью надежного протокола шифрования, например WPA и WPA2.
- Получение MAC-адреса непосредственно из сетевой карты, а не из ОС; это предотвращает подмену MAC-адреса.
- Используйте концепцию ACL (Access Control List) для разрешения доступа только к фиксированному диапазону доверенных IP-адресов в сети.
- Избегайте широковещательной рассылки SSID (Session Set Identifier).
- Реализуйте на маршрутизаторе механизм фильтрации MAC-адресов.

Методы обнаружения снифферов

Обнаружить сниффер в сети непросто, поскольку он перехватывает и работает только в режиме promiscuous. Промискуитетный режим позволяет сетевому устройству перехватывать и читать каждый поступающий в сеть пакет целиком. Сниффер не оставляет следов, поскольку не передает данные. Чтобы найти снифферы, проверьте системы, работающие в режиме promiscuous mode, который позволяет сетевой карте пропускать все пакеты (трафик) без проверки адреса назначения. Автономные снифферы трудно обнаружить, поскольку они не передают трафик данных. Обнаружить нештатные снифферы можно с помощью метода обратного DNS-поиска. Существует множество инструментов, таких как Nmap, которые можно использовать для обнаружения promiscuous mode. Запустите IDS и обратите внимание, изменился ли MAC-адрес определенных машин (пример: MAC-адрес маршрутизатора). IDS может обнаружить действия по сниффингу в сети. Она уведомляет или предупреждает администратора о подозрительных действиях, таких как сниффинг или подмена MAC-адресов. Сетевые инструменты, такие как Capsa Network Analyzer, отслеживают сеть на предмет странных пакетов, например пакетов с поддельными адресами. Этот инструмент позволяет собирать, консолидировать, централизовать и анализировать данные о трафике различных сетевых ресурсов и технологий.

Ниже перечислены методы обнаружения сниффинга.

Обнаружение при помощи Ping

Для обнаружения сниффера в сети необходимо определить систему в сети, работающую в режиме promiscuous. Метод ping позволяет обнаружить систему, работающую в режиме promiscuous, что, в свою очередь, помогает обнаружить установленные в сети снифферы.

Просто отправьте на подозреваемую машину запрос ping с указанием ее IP-адреса и неправильного MAC-адреса. Адаптер отклонит его, так как MAC-адрес не совпадает, а подозреваемая машина, на которой работает сниффер, ответит на него, так как не отклоняет пакеты с другим MAC-адресом. Таким образом, этот ответ позволит идентифицировать сниффер в сети.

Обнаружение при помощи DNS

Обратный поиск DNS является противоположностью метода поиска DNS. Снифферы, использующие обратный поиск DNS, увеличивают сетевой трафик. Такое увеличение сетевого трафика может свидетельствовать о наличии в сети сниффера.

Пользователи могут выполнять обратный поиск DNS удаленно или локально. Мониторинг DNS- сервера организации для выявления входящих обратных DNS-поисков. Метод отправки ICMP- запросов на несуществующий IP-адрес также позволяет отслеживать обратный поиск DNS. Компьютер, выполняющий обратный поиск DNS, будет отвечать на запрос ping, что позволит определить, что на нем установлен сниффер.

Обнаружение при помощи ARP

Эта техника посылает нешироковещательный ARP всем узлам сети. Узел, работающий в сети в режиме promiscuous, кэширует локальный ARP-адрес. Затем он передаст в сеть сообщение ping с локальным IP-адресом, но другим MAC-адресом. В этом случае на ваш широковещательный запрос ping сможет ответить только тот узел, который имеет MAC-адрес (кэшированный ранее). Машина в режиме promiscuous отвечает на ping-

сообщение, так как имеет в своем кэше корректную информацию об узле, посылающем ping-запрос; остальные машины посылают ARP-зонд для определения источника ping-запроса. Это позволит обнаружить узел, на котором работает сниффер.

Список литературы

1. 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.
2. 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.
3. Гельфанд А. М., Гвоздев Ю. В., Штеренберг С. И. Исследования недостатков языков высокоуровнего программирования для осуществления скрытого вложения в исполнимые файлы // Актуальные проблемы инфотелекоммуникаций в науке и образовании.— 2015. — С. 295–297.
4. Шемякин С. Н. и др. Теоретическая оценка использования математических методов прогнозирования загрузки виртуальной инфраструктуры // Наукоемкие технологии в космических исследованиях Земли.— 2021. — Т. 13.— № . 4. — С. 66–75.
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.

УДК 004.056

Новые тенденции в информационной безопасности и защите данных

Микков Александр Дмитриевич

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

***Аннотация**: Статья описывает основные тенденции в области информационной безопасности в эпоху цифровизации. Речь идет об усилении киберзащиты с помощью искусственного интеллекта и машинного обучения, использовании шифрования для защиты данных, а также новых вызовах безопасности, связанных с Интернетом вещей (IoT).*

***Abstract**: The article describes the main trends in information security in the era of digitalization. It is about strengthening cyber defense with artificial intelligence and machine learning, using encryption to protect data, and new security challenges related to the Internet of Things (IoT).*

***Ключевые слова**: информационная безопасность, усиление кибер защиты, шифрование, IoT устройства и платформы.*

***Keywords**: information security, cyber defence enhancement, encryption, IoT devices and platforms.*

Эпоха цифровизации привнесла в нашу жизнь массу возможностей, но также сопряжена с угрозами в области информационной безопасности и защиты данных. Новые тенденции в этой области продолжают развиваться, чтобы удовлетворить потребности в безопасности в условиях быстро меняющейся технологической среды.

Одной из главных тенденций в информационной безопасности является усиление киберзащиты за счет использования искусственного интеллекта и машинного обучения.

Усиление киберзащиты с использованием искусственного интеллекта и машинного обучения может быть достигнуто через ряд инновационных методов. Некоторые из них включают в себя:

1. Автоматизированное обнаружение угроз: Использование алгоритмов машинного обучения для анализа больших объемов данных и автома-

тического обнаружения аномального поведения, которое может указывать на потенциальные киберугрозы.

2. Прогнозирование угроз: Использование аналитики данных и моделей машинного обучения для прогнозирования вероятности возникновения конкретных кибератак и разработки мер предотвращения.
3. Адаптивная защита: Создание систем, которые используют искусственный интеллект для адаптивной реакции на активные кибератаки, коррекции существующих защитных мер, и быстрой адаптации к новым угрозам.
4. Анализ больших данных в режиме реального времени: Использование технологий машинного обучения для анализа больших объемов данных из сенсоров и журналов событий в режиме реального времени с целью быстрого выявления и реагирования на угрозы.
5. Улучшение системы обучения персонала: Использование технологий машинного обучения для создания персонализированных программ обучения по кибербезопасности, которые могут адаптироваться к индивидуальным потребностям и поведению сотрудников.

Эти технологии позволяют быстро анализировать и обрабатывать большие объемы данных для выявления угроз и предотвращения кибератак. Благодаря автоматизированным системам обнаружения, компании и государственные учреждения могут быстро реагировать на потенциальные угрозы и защищать свои данные.

Другой важной тенденцией является усиление защиты данных благодаря распространению шифрования.

Шифрование позволяет защищать конфиденциальные информации путем преобразования ее в нечитаемый формат, который может быть восстановлен только с использованием специального ключа. Когда шифрование становится широко доступным и используется в различных аспектах передачи и хранения данных, это способствует увеличению уровня безопасности и защиты информации.

Защита данных с помощью распространения шифрования также становится более важной в контексте современных технологических угроз, таких как кибератаки и хищение личных данных. Распространение шифрования обеспечивает защиту как для хранящихся данных, так и для дан-

ных, передаваемых через общедоступные сети, что способствует укреплению общей кибербезопасности.

Также, с развитием Интернета вещей (IoT) появляются новые вызовы в обеспечении безопасности. Устройства, подключенные к сети, могут стать уязвимыми для хакерских атак, поэтому специалисты по информационной безопасности активно разрабатывают методы защиты IoT-устройств и платформ.

Существует несколько методов защиты IoT-устройств и платформ, которые могут помочь повысить безопасность системы. Некоторые из них включают:

1. Шифрование данных: Использование сильного шифрования для защиты передаваемых данных между устройствами и серверами.
2. Аутентификация и авторизация: Требование уникальных идентификаторов и паролей для доступа к устройствам и платформам, а также установка соответствующих уровней доступа.
3. Обновление и управление программным обеспечением: Регулярное обновление программного обеспечения на устройствах IoT для устранения уязвимостей и добавления новых функций безопасности.
4. Мониторинг и обнаружение инцидентов: Реализация системы мониторинга и обнаружения инцидентов, способной оперативно реагировать на потенциальные угрозы безопасности.
5. Физическая защита: Обеспечение физической безопасности устройств IoT, например, через ограниченный доступ к физическим портам и разъемам.
6. Защита сети: Применение мер безопасности на уровне сети, таких как межсетевые экраны, виртуальные частные сети (VPN) и другие технологии защиты сетей.
7. Обучение пользователей: Проведение обучающих программ для пользователей устройств IoT о методах обеспечения безопасности и защите своих устройств.

Эти методы защиты могут быть использованы в комбинации для обеспечения полной защиты IoT-устройств и платформ.

Наконец, в свете ужесточения законодательства в области защиты данных, компании все активнее внедряют методы обеспечения конфиденциальности данных своих клиентов.

Введение новых правил и требований к хранению и обработке персональной информации создает новые вызовы и стимулирует развитие технологий защиты данных.

В заключение, новые тенденции в информационной безопасности и защите данных позволяют компаниям и государственным учреждениям улучшить свои механизмы защиты от киберугроз и обеспечить безопасность конфиденциальных данных. Развитие технологий и изменения в законодательстве создают новые вызовы, но также открывают возможности для инноваций в области информационной безопасности.

Список литературы

1. Алиметов К.С., Цветков А. Ю. Разработка защищенной системы мгновенного обмена сообщениями // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т.. Санкт-Петербург.— 2023. — С. 56–59.
2. Комашинский В.В., Коржик В.И., Молдовян А.А., Молдовян Н.А., Синюк А.Д., Яковлев В. А. Способ формирования ключа шифрования/дешифрования // Патент на изобретение RU 2171012 C1, 20.07.2001. Заявка № 2000108296/09 от 03.04.2000.
3. Яковлев В.А., Скудняков Ю.А., Пачинин В. И. Шифрование данных с применением искусственных нейронных сетей // Технические средства защиты информации. Тезисы докладов XVI Белорусско-российской научно-технической конференции. Редакционная коллегия: Т. В. Борботько, Л. А. Шичко, В. Ф. Голиков, Г. В. Давыдов, В. К. Конопелько, Л. М. Лыньков.— 2018. — С. 105.
4. Сахаров Д.В., Гельфанд А.М., Казанцев А.А., Пестов И. Е. 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.
5. Крылов А.В., Ушаков И. А. Метрика защищенности интернет вещей // Актуальные проблемы инфотелекоммуникаций в науке и образовании

(АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург.— 2022. — С. 622–626.

УДК 004.056

Развитие технологий и угрозы информационной безопасности: что нужно знать бизнесу

Микков Александр Дмитриевич

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

***Аннотация**: В статье обсуждается важность обеспечения информационной безопасности в современном бизнесе. Развитие технологий приводит не только к упрощению рабочих процессов, но и к возникновению новых угроз в виде кибератак, которые могут нанести серьезный ущерб компаниям.*

***Abstract**: The article discusses the importance of information security in modern business. The development of technology leads not only to the simplification of work processes, but also to the emergence of new threats in the form of cyberattacks that can cause serious damage to companies.*

***Ключевые слова**: развитее технологий, информационная безопасность, бизнес, кибератаки, внутренние угрозы, развитие технологий.*

***Keywords**: technology development, information security, business, cyberattacks, insider threats, technology development.*

Современные технологии привнесли в бизнес множество новых возможностей, упрощая процессы и повышая эффективность работы. Однако вместе с этим развитием появились и новые угрозы в области информационной безопасности, которые могут нанести серьезный ущерб компаниям. В связи с этим бизнес-сообщество должно быть внимательно отнестись к вопросам информационной безопасности и принимать соответствующие меры в целях защиты конфиденциальных данных и бизнес-процессов.

Кибератаки представляют серьезную угрозу для всех компаний, независимо от их размера или индустрии. Хакеры постоянно совершенствуют

свои методы, чтобы обойти защитные меры и получить доступ к конфиденциальной информации компании. Они могут использовать фишинговые атаки, вредоносные программы, атаки на слабые места в сетевой инфраструктуре или социальную инженерию, чтобы достичь своих целей.

Когда корпоративные данные попадают в руки злоумышленников, это вызывает крупномасштабные проблемы для компании. Сначала она сталкивается с потерей доверия клиентов, которые могут опасаться использовать услуги или продукцию компании, не имея уверенности в сохранности своих личных данных. В результате этого компания теряет свою репутацию и клиентскую базу, что может привести к значительным финансовым потерям. Кроме того, компания может столкнуться с юридическими последствиями, такими как штрафы за нарушение законодательства о защите данных и потерей доверия со стороны партнеров и инвесторов.

Конечно, даже небольшая утечка конфиденциальных данных может эскалироваться в серьезный инцидент без должного внимания и мер предосторожности. Поэтому компаниям важно иметь надежную киберзащиту, проводить регулярные аудиты безопасности, обучать сотрудников основам кибербезопасности и строго контролировать доступ к чувствительным данным. В мире, где цифровые технологии играют ключевую роль в бизнесе, защита от киберугроз должна быть приоритетом для всех компаний.

Для борьбы с подобными угрозами бизнеса необходимо принимать целый комплекс мер по обеспечению информационной безопасности. Превентивные действия, такие как инвестирование в современные системы защиты данных, позволяют предотвратить возможные кибератаки. Это включает в себя использование фаерволов, антивирусного ПО, систем обнаружения вторжений и других технологий, способных предотвратить несанкционированный доступ к информации.

Кроме того, постоянное обновление технологических решений и программного обеспечения является критически важным для защиты от новых видов угроз, появляющихся на просторах интернета. Это может включать в себя регулярные проверки на предмет уязвимостей, установку обновлений и патчей безопасности, а также использование криптографии для защиты данных.

Обучение персонала современным методам борьбы с киберугрозами имеет особенно важное значение, поскольку в большинстве случаев уязвимости бывают связаны с человеческим фактором. Проведение тренингов и обучающих сессий помогает улучшить осведомленность сотрудников о возможных угрозах и методах защиты.

Внедрение строгих правил использования корпоративных систем и учетных записей также необходимо для обеспечения безопасности. Это может включать в себя установку политик паролей, двухфакторную аутентификацию, ограничение доступа к конфиденциальным данным, а также мониторинг действий пользователей для предотвращения несанкционированного использования информации.

В целом, обеспечение информационной безопасности требует комплексного подхода, включающего технологические, образовательные и организационные меры.

Кроме защиты от внешних угроз, важно также обратить внимание на внутренние угрозы информационной безопасности. Это включает в себя меры по предотвращению несанкционированного доступа к данным со стороны сотрудников или других внутренних лиц. Например, установление строгих политик доступа к конфиденциальным данным, авторизация каждого сотрудника на необходимых уровнях и шифрование чувствительной информации.

Регулярное резервное копирование данных является также важным аспектом информационной безопасности. Это помогает предотвратить потерю данных в случае кибератак, аварий или других чрезвычайных ситуаций. Резервирование данных на надежных устройствах и облачных платформах обеспечивает защиту информации и возможность быстрого восстановления в случае необходимости.

Важным элементом информационной безопасности также является прозрачность в использовании и обработке персональной информации клиентов и партнеров. Это включает в себя соблюдение законодательства по защите данных, предоставление ясной информации о сборе и использовании персональных данных, а также обеспечение механизмов контроля и обеспечения безопасности этой информации. Такие меры помогут укрепить доверие клиентов и партнеров к организации, а также соблюсти правила и стандарты в области защиты данных.

Развитие технологий приводит к постоянному расширению возможностей бизнеса, упрощению процессов и улучшению качества работы. Однако, параллельно с этим развивается и угроза для информационной безопасности. Кибератаки, вирусы, хакерские атаки — все это создает серьезную опасность для компаний, нанося ущерб не только финансового характера, но и их репутации.

Бизнес-сообщество должно осознавать эти риски и проявлять активное внимание к вопросам информационной безопасности. Важно уделять особое внимание предотвращению возможных атак, защите конфиденциальных данных клиентов, обеспечению надежности и безопасности процессов компании. Только тщательный контроль, меры защиты и применение современных технологий безопасности помогут компаниям обеспечить сохранение доверия клиентов и сохранить свою репутацию на рынке.

Эффективные меры защиты информации и процессов работы компании становятся неотъемлемой частью деловой стратегии, позволяя уверенно вести бизнес в условиях стремительно развивающихся технологий и минимизировать возможные риски.

Список литературы

1. 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.
2. 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.
3. 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.
4. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации //Инновационные технологии, экономика и менеджмент в промышленности.— 2021. — С. 203–204.

5. Пестов И. Е. и др. Метод передачи метрик загруженности инстансов облачной инфраструктуры в кластер обработки средствами и методами больших данных для защиты информации и обеспечения информационной безопасности //I-methods.— 2022. — Т. 14.— № . 1. — С. 4.
6. Алехин Р. В. и др. Анализ защищенности облачной инфраструктуры openstack при эмуляции атаки вида DDOS на узлах инфраструктуры // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023).— 2023. — С. 52–55.

УДК 004.056

Применение изолированной программной среды для защиты от целенаправленных атак

Микков Александр Дмитриевич

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

***Аннотация**: Статья представляет собой описание актуальных видов изолированных программных сред для обнаружения и противодействию современным компьютерным вирусам. Принципам работы программ-песочниц, а также в статье рассматриваются преимущества разных реализаций подобных систем.*

***Abstract**: This article presents a description of the current types of sandbox software environments for detecting and counteracting modern computer viruses. The article describes the principles of sandbox programs and discusses the advantages of different implementations of such systems.*

***Ключевые слова**: информационная безопасность, изолированная программная среда, программа-песочница, программное обеспечение, вредоносное программное обеспечение.*

***Keywords**: information security, isolated software environment, sandbox program, software, malware.*

Безопасность внутренней информационной инфраструктуры — одна из важнейших задач компании, поскольку большинство технологических

и бизнес-процессов, эффективность которых повышается при помощи использования компьютерной техники, которая позволяет обрабатывать большие объемы информации, повысить скорость передачи данных, а также повысить удобство доступа сотрудников к информации, требуемой для работы. В связи с глобальной цифровизацией всех производственных процессов — организации стали основной целью для злоумышленников. Для таких атак злоумышленники могут разрабатывать и использовать вредоносное программное обеспечение, например программы-вымогатели, шпионское программное обеспечение, программы для модификации или удаления сведений с устройств компании, а также для выведения из строя компьютеров и серверов и прочей техники организации.

Для защиты от целевых атак стали использовать антивирусное программное обеспечение, однако в настоящее время вредоносные программы научились эффективно действовать против базовых средств защиты — антивирусов, шлюзов безопасности, систем обнаружения вторжений и систем предотвращения вторжений (IDS и IPS).

Для выявления подобных угроз начали разрабатывать отдельный класс решений — изолированные программные среды («песочницы»). Такие решения проверяют все потенциально опасные файлы, попадающие в сеть компании, в изолированной виртуальной среде и анализирует все действия, совершенные файлом в системе, и выводит вердикт о том, безопасен ли этот файл или нет.

Основу современных методов антивирусной защиты составляет установка изолированных программных сред, поскольку эффективность сигнатурного анализа в борьбе против вредоносного ПО не является достаточной.

На данный момент существуют различные способы установки песочниц:

- Локальные песочницы
- Сетевые песочницы

Локальные песочницы предусматривают изоляцию на основе частичной виртуализации файловой системы и реестра. Вместо создания отдельной виртуальной машины для каждого проверяемого процесса, локальная песочница создает дубликаты объектов файловой системы и реестра.

В итоге на пользовательском компьютере формируется безопасная среда-песочница.

Основу механизма защиты составляет использование разграничительной политики доступа потенциально опасных программ к защищаемым системным объектам (файловым и объектам реестра операционной системы Microsoft Windows). Для предотвращения доступа таких программ (любой запрос доступа определяется двумя сущностями: пользователем — учетной записью — и процессом), реализовать песочницу можно, задав соответствующие права доступа к системным объектам либо для пользователей, либо для процессов. Таким образом, можно ассоциировать песочницу с создаваемой для нее учетной записью, под которой должны запускаться потенциально опасные программы. Альтернативой служит разграничение прав доступа к системным объектам для потенциально опасных процессов (песочница при этом ассоциируется с конкретными процессами).

Преимуществом данного метода является его относительная простота в реализации и низкое потребление системных ресурсов. С другой стороны, существует необходимость регулярной очистки контейнеров виртуализации перед запуском каждого проверяемого файла, что является его недостатком. Более того, существуют способы обхода этой реализации песочницы, которые дают возможность злонамеренному коду «убежать» из виртуальной среды в основную систему и активировать свои функции.

Более защищённый вариант — использовать локальную песочницу, создавая отдельную виртуальную машину, которая повторяет рабочую среду. Однако, это требует слишком много системных ресурсов, поэтому предпочтительнее использовать сетевые песочницы. Они могут быть размещены на специальном сервере внутри сети компании (on-premise) или в облачной среде производителя антивирусного решения.

Сетевые песочницы менее ограничены по сравнению с локальными — они не уменьшают эффективность работы компьютера пользователя и могут тестировать потенциальные угрозы в разных операционных системах. Даже если вредоносный код успешно «сбежит» из такой песочницы, это не станет проблемой, так как она полностью отделена от рабочего компьютера пользователя. При необходимости, эти песочницы могут имитировать подключение к интернету и работу с съемными устройствами.

В процессе использования сетевых песочниц на компьютерах пользователей устанавливается агент, служба, которая пересылает подозрительные файлы на анализ в сетевую песочницу. Отправка файлов на проверку в облачной сервис занимает больше времени, по сравнению с взаимодействием с on-premise-сервером внутри сети компании.

Малициозное программное обеспечение, нацеленное на определенную компанию, обычно проверяет окружение, в котором оно работает. Даже если оно не проверяет, работает ли оно в песочнице, несовпадение окружения может привести к тому, что вредоносная нагрузка не активируется во время анализа, и файл будет признан безвредным. Для предотвращения такого сценария, необходимо, чтобы эмулируемое песочницей рабочее окружение максимально точно отражало рабочие станции реальных пользователей.

С облачными песочницами сложнее достичь такого прямого соответствия, тогда как загрузка образа рабочей станции на on-premise сервер не представляет проблем. Основное условие — сервер-песочница должен поддерживать работу с модифицированными образами операционных систем.

Для того чтобы максимально приблизить конфигурацию виртуальных машин в песочнице к реальной рабочей среде, необходима возможность детальной настройки их содержимого: изменение параметров операционных систем, редактирование списка установленных языков, драйверов внешних устройств, установка дополнительного или нестандартного программного обеспечения, а также управление содержимым рабочего стола, так как все это и многие другие факторы могут быть использованы злоумышленниками как условия для активации вредоносных команд.

Применение стандартных образов для создания виртуальных машин в песочнице может быть легко обнаружено, что дает возможность использовать механизмы для обхода обнаружения в песочницах.

Сейчас, с учетом необходимости достижения максимальной эффективности, предпочтение отдается сетевым решениям, которые работают на серверах компании.

Облачные песочницы могут быть рассмотрены как более бюджетный вариант, или если инфраструктура компании распространена географически.

В заключение стоит отметить, что метод использования виртуальных изолированных сред кардинально упрощает проектирование системы защиты информации. За счет введения обоснованных допущений в отношении реализации угроз атак на защищенную информационную систему он позволяет решить две важнейшие задачи проектирования — определить оптимальный набор функций защиты, реализуемых системой защиты информации, и сформировать требования к эксплуатационным параметрам средств защиты, входящих в состав этой системы.

Список литературы

1. Sandbox — выделенная среда для безопасного исполнения программ // CloudNetworks URL: https://cloudnetworks.ru/inf-bezopasnost/anti-apt-sandbox.
2. Какие варианты «песочницы» существуют // Anti-Malware URL: https://www.anti- malware.ru/analytics/Technology_Analysis/What-sandbox-options-exist.

УДК 004

Разработка приложения якутские сказки «ArGys»

Исакова Татьяна Ивановна

студентка Колледжа инфраструктурных технологий
Северо-Восточный федеральный университет имени М. К. Аммосова

Степанова Марианна Евгеньевна

преподаватель Колледжа инфраструктурных технологий
Северо-Восточный федеральный университет имени М. К. Аммосова

***Аннотация**: Разрабатываемое приложение «ArGys» предполагает собою неповторимый источник, предназначенный состоятельному наследству, а также культуре якутского народа. Дополнение дает шанс юзерам окунуться в общество якутских сказок, какие предоставляют устои, благоразумие, а также ситуацию данного на-*

рода. В дополнении составлена обширная подборка якутских сказок, общедоступных с целью чтения а также выслушивания.

***Abstract**: The ArGys application under development is a unique source intended for the wealthy heritage as well as the culture of the Yakut people. The add-on gives a chance to users to plunge into the society of Yakut tales, which provide the foundations, reasonableness and also the situation of this people. The add-on contains an extensive collection of Yakut tales, which are available for reading and listening.*

***Ключевые слова**: мобильное приложение, якутские сказки, культура, традиции, история, чтение.*

***Keywords**: mobile application, Yakut fairy tales, culture, traditions, history, reading.*

Актуальность исследования подвижного дополнения приурочена к хранению, а также популяризации якутской культуры, а также всенародных сказок. Якутская культура обладает состоятельное достояние оригинальных сказок, какие вплоть до этих времен переходят с поколения в происхождение. Но вместе с формированием технологий, а также переменой вида существования, устои, а также культура зачастую становятся позабытыми либо растерянными. Формирование подвижного дополнения даст возможность совершить данные сказки легкодоступными с целью обширной аудитории, а также сберечь их с целью предстоящих поколений.

Основная цель этой работы разработка мобильного приложения «ArGys» при помощи интегрированной среды Android Studio.

Для достижения поставленной цели необходимо выполнить следующие задачи:

- обзор и анализ программного обеспечения, готовых решений;
- формирование требований к проектируемой системе.

Гипотеза исследования заложена в том, что новое приложение поможет детям не только повысить уровень владения якутским языком, но и расширит их знания.

В соответствии с целью и гипотезой исследования, нами поставлены следующие **задачи:**

1. Обследование объектов и описание предметной области;

2. Выбор средств разработки;
3. Постановка задачи;
4. Определение основных возможностей и функций разрабатываемого приложения;
5. Проведение программной реализации.

При разработке приложения использовали следующие программы:

Android Studio — интегрированная среда разработки (IDE) для работы с платформой Android, анонсированная 16 мая 2013 года на конференции Google I/O. В последней версии Android Studio поддерживается Android 4.1 и выше.

Figma — это инструмент для дизайна интерфейсов (UI/UX), который позволяет дизайнерам и командам создавать, прототипировать и сотрудничать над проектами в одной облачной платформе.

Прототип приложения на Figma

Рисунок 1. **Главные страницы**

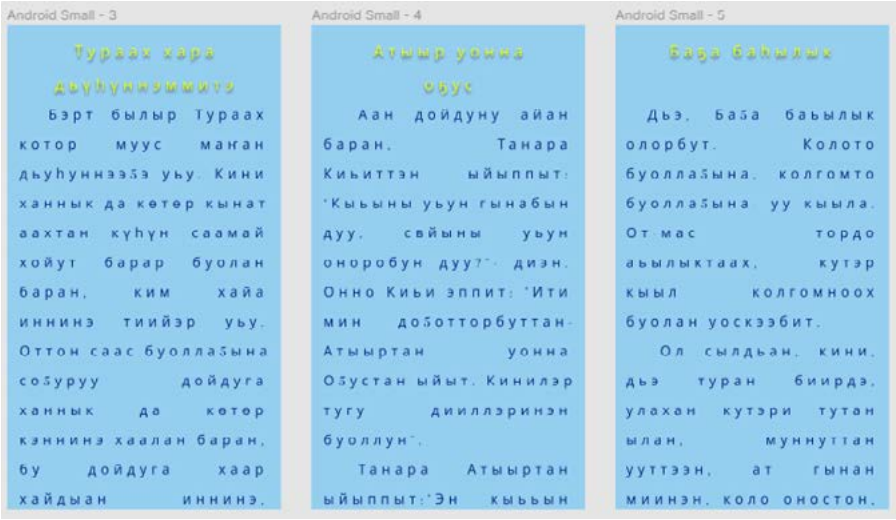

Рисунок 2. **Сказки**

Рисунок 3. **Структура приложения**

Описание технологии создания приложения «ArGys» в среде разработки Android Studio

Рисунок 4. **Заставка**

```
public class MainMenu extends AppCompatActivity {
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main_menu);
    }
```

Рисунок 5. **Код заставки**

Рисунок 6. **Главный экран**

```
public class MainMenu extends AppCompatActivity {
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main_menu);
    }
```

Рисунок 7. **Код главного экрана**

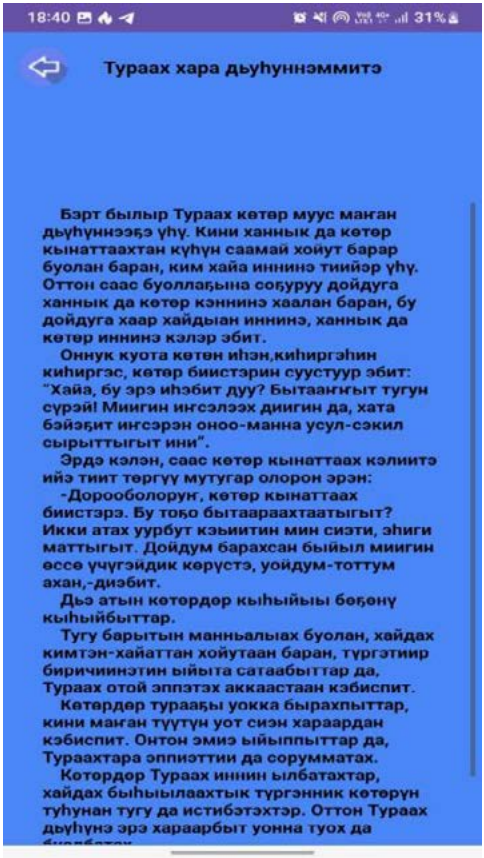

Рисунок 8. **Страница сказки**

```
    public void turaax(View view) {
        String textFromXml =
getResources().getString(R.string.turaah);

        Intent intent = new Intent(this, Histories.class);
        intent.putExtra("nameHistories", "РўСґСЂР°Р°С… С…Р°СЂР°
РґСЊСґһСґРЅСРЅСЌРјРјРёС,СЌ");
        intent.putExtra("histories", textFromXml);
        startActivity(intent);
    }
```

Рисунок 9. **Код сказки**

Заключение

В заключение разработки приложения «ArGys» для курсового проекта можно отметить успешную реализацию поставленных целей и задач. Благодаря учету обратной связи от тестирования и пользователей, удалось значительно улучшить функционал приложения, сделав его более удобным и привлекательным для пользователей.

В целом, разработка приложения «Якутские сказки» была успешной и позволила достичь поставленных целей.

Список литературы

1. Акционерное общество «Национальное издательская компания» «Айар» имени Семена Андреевича Новгородова, 2023.
2. Джава что такое: Что такое Java? — Руководство для начинающих специалистов по работе с Java — AWS (toto-school.ru).
3. Мичил в мире сказок [Электронный ресурс] https://kai0909221208.wix-site.com/my-site-3.
4. Федорова Мария Николаевна, Значение якутских народных сказок в работе с детьми | Материал по теме: | Образовательная социальная сеть (nsportal.ru).
5. Eclipse [Электронный ресурс] https://ru.wikipedia.org/wiki/Eclipse.
6. NetBeans [Электронный ресурс] https://ru.wikipedia.org/wiki/NetBeans.

УДК 004

Разработка приложения для ресто-кафе «Friday»

Винокурова Арина Георгиевна

студент Колледжа инфраструктурных технологий
Северо-Восточный федеральный университет имени М. К. Аммосова

Степанов Александр Александрович

преподаватель кафедры Эксплуатации и обслуживания информационных систем Колледжа инфраструктурных технологий Северо-Восточный федеральный университет имени М. К. Аммосова

***Аннотация**: В данной статье описывается создание приложения для ресто-кафе «Friday», расположенный в г. Якутске. мобильное приложение делает взаимодействие с клиентом более удобным и быстрым. Клиенты могут выбирать еду, напитки и заказывать онлайн без участия менеджера. И это очень важно, так как в наше время люди стараются как можно меньше тратить время и экономить ресурсы.*

***Abstract**: This article describes the creation of an application for the resto-cafe «Friday» located in Yakutsk. The mobile application makes interaction with the client more convenient and faster. Customers can choose food, drinks, and order online without the involvement of a manager. And this is very important, as nowadays people try to waste as little time as possible and save resources.*

***Ключевые слова**: разработка приложения, приложение, анализ, технология, язык программирования.*

***Keywords**: application development, application, analysis, technology, programming language.*

Актуальность: в последние годы сформировался новый тренд: клиенты стали заказывать еду домой и на вынос, а владельцы ресторанов стали активно инвестировать в разработку мобильных приложений, чтобы оптимизировать свои рабочие процессы.

Предмет исследования: технология разработки и формирования приложения.

Методы исследования: анализ, синтез и обобщение при рассмотрении теоретического материала, а также метод сравнения при изучении различных источников.

Цель работы: исследование структуры и разработка мобильного приложения для ресто-кафе «Friday».

«Friday» — это ресто — кафе, расположенный в рабочем центре города Якутска. Уютное место, где вы можете провести время с родными, устроить деловую встречу, посидеть с друзьями или поработать одному. Главным плюсом, конечно, является кухня, которая подойдет для всех: азиатская, паназиатская, европейская кухни, имеется детское меню, а также напитки на любой вкус.

Мобильные приложения помогают ресторанам работать быстрее и эффективнее: связываться с поставщиками, бронировать столики, получать консультации, принимать и доставлять заказы. Приложение этого заведения будет содержать всю необходимую информацию для гостей ресто-кафе: в приложении гости смогут зарегистрироваться и создать личный кабинет или воспользоваться гостевым режимом. В приложении они могут просмотреть новинки, акции и основную информацию о заведении (часы работы, контактные данные, местонахождение и т. д.). Электронное меню с изображениями блюд, стоимостью, составом и граммами, а также условиями доставки.

Для разработки приложения провели анализ существующих приложений для предприятий общественного питания в г. Якутске. На настоящий момент имеется ряд мобильных приложений, решающих поставленную задачу. Каждая из них имеет свои особенности, преимущества и недостатки.

- Мобильное приложение «Traveler's Coffee».
- Мобильное приложение «Хачапури».
- Мобильное приложение «Вышка».

На основе данного сравнения, можно сделать вывод о том, что для приложения, направленного на предприятие общественного питания, важно иметь быстрый доступ к меню, имеющий всю необходимую информацию о блюде, а также простую схему оформления доставки на дом.

Также был проведен сравнительный анализ сред разработки в виде таблицы:

Исходя из приведенного сравнения, более рентабельно использовать платформу Android Studio. В первую очередь, потому что у нее самый удобный пользовательский интерфейс, много доступного материала для обучения, вполне достаточный спектр языков программирования, бесплатность пользования.

Рисунок 1. **Вкладка «Популярные продукты»**

Рисунок 2. **Вкладка «Горячие блюда»**

Таблица 1. **Сравнительный анализ сред разработки**

Среда разработки	**Язык программирования**	**Удобство интерфейса**	**Мобильные платформы для разработки**	**Плата**
Android Studio	Java, C\C++, Delphi	Да	Android	Нет
Intel XDK	HTML5	Да	Все	Да
Intel Beacon Mountain	Java, C, C++	Нет	Android	Нет
«1С: Предприятие 8. Расширение для КПК»	Язык программирования 1С	Да	Windows Mobile, Android	Да
Intel Mobile Development Kit for Android	C, C++, C#, Fortran, Java, ASM	Нет	Android	Да

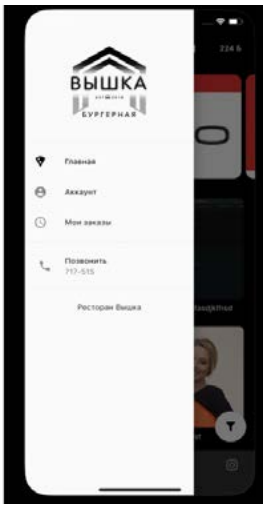

Рисунок 3. **Главная приложения «Вышка»**

Описание технологии создания приложения «FRIDAY» в среде разработки Android Studio:

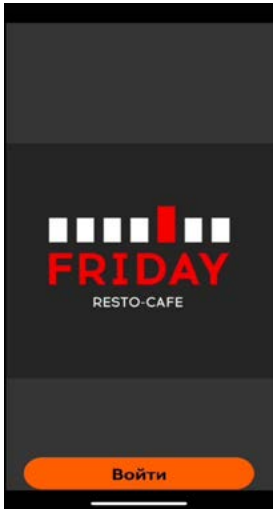

Рисунок 4. **Вход в приложение**

Код:

```
public class IntroActivity extends AppCompatActivity {
    private ConstraintLayout startBtn;
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_intro);

        startBtn = findViewById(R.id.startBtn);
        startBtn.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                startActivity(new
Intent(IntroActivity.this,MainActivity.class));
            }
        });

    }
```

Рисунок 5. **Главный экран**

Код:

```
private void BottomNavigation() {
    FloatingActionButton floatingActionButton = findViewById(R.id.cartBtn);
    LinearLayout homeBtn = findViewById(R.id.home_Btn);

    floatingActionButton.setOnClickListener(new View.OnClickListener() {
        @Override
        public void onClick(View v) {
            startActivity(new Intent(MainActivity.this,
CartListActivity.class));
        }
    });

    homeBtn.setOnClickListener(new View.OnClickListener() {
        @Override
        public void onClick(View v) {
            startActivity(new Intent(MainActivity.this, MainActivity.class));
        }
    });
}
```

Программа выводит выбранные товары, их количество и сумму к оплате для пользователя (Рисунок 6).

Код:

```
private void
CalculateCart() {
    double percentTax = 0.02;
    double delivery = 10;

    tax = Math.round((managementCart.getTotalFee() * percentTax) * 100) /
100;
    double total = Math.round((managementCart.getTotalFee() + tax + delivery)
* 100) / 100;
    double itemTotal = Math.round(managementCart.getTotalFee() * 100) / 100;

    totalFeeTxt.setText("" + itemTotal);
    taxTxt.setText("" + tax);
    deliveryTxt.setText("" + delivery);
    totalTxt.setText("" + total);
```

Рисунок 6. **Раздел «Корзина»**

Пользователь имеет возможность выбора и отмены выбора пункта из распознанного/введенного списка (Рисунок 7).

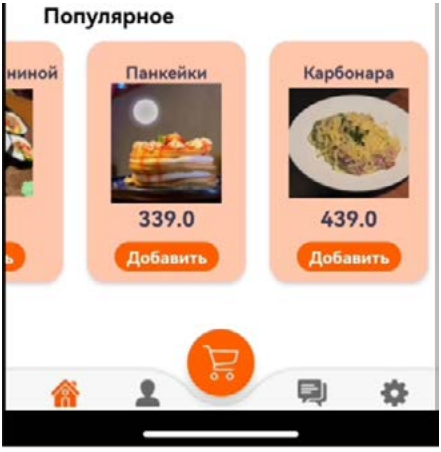

Рисунок 7. **Популярное меню**

Код:

```
private void recyclerViewPopular() {
    LinearLayoutManager linearLayoutManager = new LinearLayoutManager(this, LinearLayoutManager.HORIZONTAL, false);
    RecyclerViewPopularList = findViewById(R.id.recyclerView2);
    RecyclerViewPopularList.setLayoutManager(linearLayoutManager);
    ArrayList<FoodDomain> foodList = new ArrayList<>();
    foodList.add(new FoodDomain("Кимпаб со свининой", "kimpab", "нори, рис, маринованная редька, омлет, жаренаясвинина в корейском соусе", 339.0));
    foodList.add(new FoodDomain("Панкейки", "pankiki", "нежные панкейки со сливочным кремом ", 339.0));
    foodList.add(new FoodDomain("Карбонара", "karbonara", "Карбонара-аппетитная паста с кусочками бекона под сливочным соусом и шапочкой из сыра",439.0));
    foodList.add(new FoodDomain("Картошка Фри", "kart", "хрустящая жареная картошка фри с фаршем, острым перцем халапеньо и тающим во рту сыром моцарелла ", 339.0));
    foodList.add(new FoodDomain("Рис с яйцом", "ric", "питательный рис с яйцом и кусочками овощей, пикантный соус придает блюду азиатский колорит, а чеснок и перец чили приятную остроту ", 249.0));
    foodList.add(new FoodDomain("Спагетти", "spag", "спагетти из твердых сортов пшеницы, паста том ям, куриное филе сливки ", 339.0));
    foodList.add(new FoodDomain("Блинчики", "blin", "блинчики с киви и бананом, политые шоколадныи и клубничными топпинками ", 299.0));
    foodList.add(new FoodDomain("Тори", "tori", "тори горячий запеченный: рис, нори, куриное филе, огурцы, острая сырная шапка, жареная во фритюре ", 339.0));
    adapter2=newPopluarAdaptor(foodList);
    RecyclerViewPopularList.setAdapter(adapter2);
```

Вывод

Таким образом, мы проанализировали и исследовали технологию разработки программы, сделали сравнительный анализ аналоговых программ, на основе которых будет опираться последующая разработка нового приложения. В итоге была разработано мобильное приложение для ресто-кафе «Friday», которое имеет понятный интерфейс с ярким дизайном и простой навигацией.

Список литературы

1. Мобильное приложение [Электронный ресурс]. — URL: https://www.calltouch.ru/blog/glossary/mobilnoe-prilozhenie.
2. Как разработать приложение для ресторана или кафе, зачем это нужно и сколько стоит мобильное приложение [Электронный ресурс]. — URL: https://www.purrweb.com/ru/blog/kak-razrabotat-prilozhenie-dlya-restoranov.
3. Сравнительный анализ программного обеспечения для разработки мобильных приложений [Электронный ресурс]. — URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-programmnogo-obespecheniya-dlya-razrabotki-mobilnyh-prilozheniy.

УДК 004

Приложения для поступления в вуз

Соловьев Вячеслав Петрович

студент Колледжа инфраструктурных технологий
Северо-Восточный федеральный университет имени М. К. Аммосова

Степанов Александр Александрович

преподаватель кафедры Эксплуатации и обслуживания информационных систем Колледжа инфраструктурных технологий Северо-Восточный федеральный университет имени М. К. Аммосова

***Аннотация**: Мобильные приложения для поступления в учебные заведения имеют высокую актуальность в настоящее время и, скорее всего, будут оставаться актуальными. В цифровую эпоху многие аспекты нашей жизни переносятся в онлайн-пространство, и образовательная сфера не исключение. Мобильные приложения позволяют абитуриентам получить доступ к необходимой информации о учебных заведениях, требованиях для поступления, последним новостям и событиям, связанным с поступлением. Это делает процесс поступления более удобным и эффективным. В свете увеличивающегося числа мобильных устройств и роста числа пользователей мобильных приложений, они становятся все более востребованными. Приложения для*

поступления в учебные заведения имеют потенциал улучшить процесс поступления и обеспечить абитуриентам лучший доступ к необходимой информации. Поэтому они остаются актуальными и будут продолжать развиваться.

***Abstract**: Mobile apps for enrollment are highly relevant nowadays and are likely to remain such. In the digital age, many aspects of our lives are moving into the online space, and the educational field is no exception. Mobile apps allow applicants to access essential information about schools, admission requirements, and the latest news and events related to enrollment. This makes the admission process more convenient and efficient. Considering the increasing number of mobile devices and the growing number of mobile app users, they are becoming more and more in demand. Admission apps have the potential to improve the admissions process and provide applicants with better access to the information they need. Therefore, they remain relevant and will continue to evolve.*

***Ключевые слова**: мобильное приложение, абитуриент, вуз.*

***Keywords**: mobile application, applicant, university.*

Цели

Разработка приложения, которое предоставит абитуриентам информацию о различных университетах, специальностях, требованиях для поступления, обучении и стипендиях, чтобы помочь им принять обоснованное решение относительно выбора учебного заведения и специальности.

Методология

Это статья, которая исследует принципы, применяемые в разработке и использовании мобильных приложений, предназначенных для помощи абитуриентам в процессе поступления в высшие учебные заведения. Статья рассматривает основные принципы, на которых основано такое приложение, такие как предоставление информации о университетах, поддержка процесса поступления, помощь в выборе специальности, обмен опытом, поддержка и консультации, и предоставление актуальной информации. В статье также обсуждается значение и выгоды мобильных приложений для абитуриентов и их роль в облегчении и улучшении процесса поступления в университет.

Результаты

Удобство и доступность: Мобильные приложения позволяют абитуриентам получить всю необходимую информацию о поступлении прямо с их мобильных устройств. Поскольку пользователи могут использовать приложение в любое время и в любом месте, что делает процесс подачи документов и подготовки к экзаменам более гибким и доступным.

Выводы

В заключение, разработка приложения для абитуриентов имеет потенциал облегчить процесс выбора учебного заведения и специальности, обеспечивая доступ к информации о различных университетах, специальностях, требованиях для поступления, обучении и стипендиях. Такое приложение может быть основано на психологических принципах принятия решений, информационной архитектуре, удобном интерфейсе пользователя, образовательных педагогических аспектах и технологических новациях. В конечном итоге, цель приложения для абитуриентов — помочь им принять обоснованное и осознанное решение относительно выбора учебного заведения и специальности, что в конечном итоге повысит вероятность успешной учебы и карьерного роста после окончания учебы.

Мобильные приложения для помощи абитуриентам: удобство и информационная поддержка. С каждым годом количество выпускников школ, желающих поступить в высшие учебные заведения, растет, а процесс поступления становится все более конкурентным и сложным. В этой ситуации мобильные приложения выступают важной ролью, предоставляя абитуриентам удобный и информативный инструмент для подготовки и сопровождения процесса поступления. Одним из основных преимуществ мобильных приложений для абитуриентов является доступ к актуальной информации о различных университетах и их программах обучения. Пользователи могут получить подробные данные о требованиях к поступлению, сроках подачи документов, стоимости обучения и многом другом, прямо с своего смартфона. Это позволяет абитуриентам проявить более информированный подход к выбору учебного заве-

дения и специальности. Кроме того, мобильные приложения могут предоставлять поддержку в процессе подготовки к поступлению, предлагая материалы для подготовки к вступительным экзаменам и тестам, а также давая рекомендации по эффективной подготовке. Это особенно важно для абитуриентов, которые живут в удаленных регионах или имеют ограниченный доступ к ресурсам образования. Кроме информационной поддержки, мобильные приложения также могут предоставлять возможность общения и обмена опытом между абитуриентами, что способствует созданию сообщества, где студенты могут обсудить свои вопросы, получить советы или поддержку от тех, кто уже прошел через процесс поступления в университет. Таким образом, мобильные приложения для абитуриентов представляют собой ценный инструмент, обеспечивающий абитуриентов всей необходимой информацией, поддержкой и возможностью общения во время непростого процесса поступления. Они делают этот процесс более доступным, удобным и информативным для всех участников.

Список литературы

1. Самойлова, О.Н. «Мобильные технологии в образовании: проблемы и перспективы.» Москва, Издательство «Педагогика», 2018.
2. Росс, С. «Эффективное использование мобильных технологий в образовании: практические аспекты.» Нью-Йорк, Издательство «Academic Press», 2017.
3. Иванова, Е.А. «Роль мобильных приложений в современном образовании: анализ и перспективы.» Санкт-Петербург, Издательство «Университетская книга», 2019.
4. Березина, Н.Н. «Информационные технологии в образовании: возможности и риски.» Москва, Издательство «Высшая школа», 2018.
5. Джексон, М. «Развитие мобильных технологий в сфере образования: тренды и перспективы.» Бостон, Издательство «Education Press», 2020.
6. Ли, Ч. «Применение мобильных приложений в вузах: педагогические и технические аспекты.» Москва, Издательство «Наука и образование», 2019.

УДК 004

Разработка мобильного приложения «Книга рецептов якутской национальной кухни»

Эверстова Алина Георгиевна

студентка Колледжа инфраструктурных технологий
Северо-Восточный федеральный университет имени М. К. Аммосова

Степанов Александр Александрович

преподаватель кафедры Эксплуатации и обслуживания информационных систем Колледжа инфраструктурных технологий Северо-Восточный федеральный университет имени М. К. Аммосова

***Аннотация**: В данной статье описывается создание приложения для просмотра книги рецептов якутской национальной традиционной кухни при помощи интегрированной системы Android Studio, которым могут пользоваться все желающие.*

***Abstract**: This paper describes the creation of an application to view a recipe book of Yakut national traditional cuisine using the integrated Android Studio system that can be used by everyone.*

***Ключевые слова**: рецепт, якутская кухня, разработка приложения, средства разработки, язык программирования.*

***Keywords**: recipe, Yakut cuisine, application development, development tools, programming language.*

Якутская национальная кухня — это совокупность традиций и рецептов приготовления пищи, обусловленных историческими, географическими, культурными особенностями в условиях Крайнего Севера и вечной мерзлоты.

Актуальность данной работы состоит в том, что сегодня мобильный смартфон становится источником самых разнообразных и необходимых ресурсов для работы, досуга и образования, чему способствует стремительное развитие индустрии мобильных приложений. В Республике Саха (Якутия) растет активность в сфере разработки соответствующего программного обеспечения, но нет приложения книги рецептов якутской национальной кухни. Поэтому разработка этого приложения является несомненно актуальной темой исследования.

Целью работы является создание мобильного приложения «Книга рецептов якутской национальной кухни», как средство для полезного времяпровождения для любителей готовки.

Для достижения данной цели мною поставлены следующие **задачи:**

- изучение процесса разработки мобильных приложений;
- создание прототипа приложения с помощью Figma;
- разработать мобильное приложение с помощью Android Studio.

Объект исследования: процесс разработки мобильного приложения н платформе Android Studio.

Предмет исследования: технология разработки мобильного приложения на Android Studio.

Гипотезой исследования послужило предположение о том, что использование мобильного приложения облегчит процесс готовки если будет отвечать следующим требованиям:

- привлекательный и простой дизайн;
- интуитивно понятный и удобный интерфейс;
- структурированная, достоверная и полная информация;
- технически эффективная и надежная реализация.

Методы исследования: анализ, синтез и обобщение при рассмотрении теоретического материала, а также метод сравнения при изучении различных источников.

Научная **новизна** работы заключается в том, что разработанное приложение будет иметь изображения для освоения теоретического материала.

В современном информационном поле взаимодействие человека и мобильных устройств в различных сферах подтолкнуло нас к созданию разнообразных приложений, которые облегчают нам жизнь. Интернет-сети всё глубже внедряются во все сферы нашей жизни, а в частности и мобильную связь, что позволило сделать большой шаг в направлении развития и оптимизации мобильных приложений для телефонов, а также адаптации многих популярных приложений.

Для создания прототипа приложения использовала Figma. Figma –это графический редактор для создания прототипов сайтов и приложений. Над проектом одновременно могут работать несколько человек, так как можно выдать доступ на редактирование или комментирование любому.

Изюминка мобильного приложения — это современная интерпретация национальных блюд — возрождение старинных рецептов якутских блюд, адаптированных к современным технологиям. Прототип приложения представлен на рисунке 1.

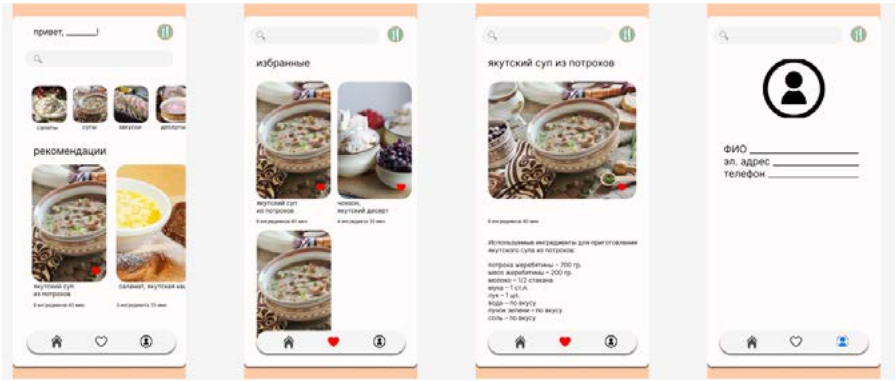

Рисунок 1. **Прототип приложения**

Далее для разработки мобильного приложения я исследовала теоретические основы технологии разработки мобильных приложений на платформе Android Studio.

Android Studio — это стартовая площадка для написания, отладки и сборки кода, а также последующей публикации приложений.

Исследовав различные среды для разработки приложений, проведя сравнительный анализ, пришли к выводу, что для создания простого приложения лучше всего подойдет программа Android Studio, базирующейся на платформе Intellij IDEA компании JetBrains, которая имеет приятный и интуитивно понятный интерфейс, удобный редактор, интеллектуальный анализ кода. Кроме всего, можно проводить интеграцию всех необходимых функций для новых версий Android, т.к. разработчиком является Google. Второстепенные причины: удобный конструктор, приятный дизайн и встроенный SDK, т.е. комплект средств разработки, который позволяет специалистам по программному обеспечению создавать приложения для определённого пакета программ, программного обеспечения базовых средств разработки, аппаратной

платформы, компьютерной системы, игровых консолей, операционных систем и прочих платформ.

Технология разработки создания мобильного приложения состоит из следующих алгоритмов:

Выбор среды программирования — Программирование кодов приложения — Тестирование на эмуляторе созданное приложение — Перенос APK файл в телефон — Установка мобильного приложения — Запуск.

Приложение было разработано по следующему рецепту:

1. В начале разработки приложения выбрать среду программирования (Android Studio);
2. Написать коды приложения;
3. Протестировать созданное приложение;
4. Запустить.

Описание технологии создания приложения «Книга рецептов якутской национальной кухни» в среде разработки Android Studio

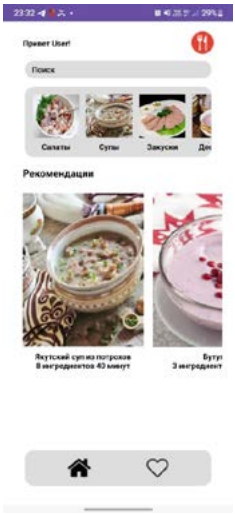

Рисунок 2. **Главное меню и код главного меню**

Рисунок 3. **Страница выбранного блюда**

Рисунок 4. **Раздел «Избраннное».**

Заключение

В данной работе были исследованы языки программирования разных сред, исследована программа Android Studio, а также аналогичные технологии разработки приложения.

Проведенное тестирование программы позволит сделать вывод о работоспособности программы и ее соответствии заданию.

В результате выполнения данного проекта разработано мобильное приложение «Книга рецептов якутской национальной кухни», которая будет полезна для любителей якутской кухни, которым могут пользоваться все желающие.

Список литературы

1. Оконешникова. Н. Якутская национальная кухня. От традиций прошлого до веяний современности, 2021.— 190 с.
2. Павлова. Е. А. Технологии разработки современных информационных систем на платформе Microsoft NET: учебное пособие / Е. А. Павлова.— 3-е изд. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медна, 2020.— 128 с.
3. Разработка мобильного приложения на платформе Android Studio.
4. Тарбахов. И. И. Благословенная пища якутов. Кулинарная книга / И. И. Тарбахов.— 2009.— 220 с.

УДК 004.451.42

Анализ применения технологии Big Data в области предупреждения и борьбы с преступностью

Кирюхин Артем Викторович

адъюнкт факультета подготовки научных и научно-педагогических кадров Академии управления МВД России

***Аннотация**: В статье проведено исследование возрастания роли применения технологии больших данных в сфере предупреждения и борьбы с преступностью. Проанализирован передовой опыт применения технологии больших данных в деятельности правоохранительных органов различных государств в современных условиях цифровой трансформации. Дан прогноз дальнейшего внедрения и развития технологии больших данных в сфере предупреждения и борьбы с преступностью.*

***Abstract**: The article investigates the increasing role of big data technology application in crime prevention and control. The best practices of application of big data technology in the activities of law enforcement agencies of various states in modern conditions of digital transformation are analyzed. The forecast of further implementation and development of big data technology in the field of crime prevention and control is given.*

***Ключевые слова**: большие данные (big data), цифровая трансформация, предупреждение и борьба с преступностью, большие данные и полиция.*

***Keywords**: big data, digital transformation, crime prevention and control, big data and the police.*

Джек Ма, создатель Alibaba, сказал однажды, что данные — это новая нефть. Он олицетворил идею, что данные могут быть такими же ценными ресурсами, как нефть, в мире информационных технологий и бизнеса. Эта аналогия выражает важность и ценность информации в современном мире. Подобно тому, как нефть была ключевым ресурсом для промышленной революции, данные играют фундаментальную роль в цифровой революции. Big Data, как и нефть, проникли во все сферы нашей жизни, становятся её неотъемлемой частью. Современный цифровой мир построен на данных. В последние годы технология больших данных производит революцию во многих областях, например, в розничной торговле, здравоохранении, транспорте, правоохранительной сфере и т.д. Цифровая трансформация правоохранительных органов невыполнима без перехода на новый уровень принятия решений — на основе данных, которые всё больше зависят от обработки и анализа данных для обеспечения предупреждения и борьбы с преступностью.

На сегодняшний день государственные структуры, включая правоохранительные органы, в большинстве стран активно оперируют большим данными. Они придерживаются принципа «чем больше, тем лучше», используя информацию не только из собственных базы данных, но и дополняя информацию из разных источников, таких как интернет, базы данных сторонних организаций, систем видеонаблюдения и т.д. Эта информация имеет большой объем, разнообразна и поступает из различных источников.

Вопрос использования больших данных полицией стал широко обсуждаться с начала текущего десятилетия. Технология больших данных позволяет создавать аналитические модели, использующие большие объемы информации для предсказания возможных преступлений и выявления областей с повышенным риском криминальной активности. Анализ данных помогает полиции оперативно выявлять тенденции, что позволяет более эффективно распределять ресурсы для предотвращения преступлений.

Так же использование больших данных обеспечивает возможность более глубокого анализа различных источников данных, таких как базы данных о преступниках, системы видеонаблюдения и социальные сети и т.д. Это позволяет выявлять связи между преступлениями, идентифицировать шаблоны поведения преступников и, таким образом, увеличивается эффективность расследования преступлений. Анализ больших данных потенциально способен уменьшить необъективность, увеличить результативность и точность прогнозирования [1].

Аналитика данных и прогнозирование не является новым явлением в полиции. Повышение результативности работы правоохранительных органов с помощью анализа данных и статистики началось в XIX веке, когда такие исследователи Кетле и Герри обрабатывали данные с помощью статистических методов для выявления лежащих в основе закономерностей. Последние два десятилетия XX века ознаменовались появлением феномена «актуарного правосудия», при котором методы, заимствованные из сферы страхования, используются в попытке предсказать риск преступного поведения [2].

Еще одним шагом на пути к использованию больших данных стали такие разработки, при которых визуализируются тенденции преступности в определенных областях, чтобы полиция могла лучше предвидеть преступления и беспорядки и эффективнее использовать силы и средства, находящиеся в подчинении. Например в реальном времени определять наиболее опасные районы города. Такая карта используется полицией Лондона, на которой отмечены «горячие точки» [3].

Анализ больших данных также позволяет вовремя определять разнообразные тренды, например тот факт, что в преступной среде оружие и пули являются своего рода валютой. Большую роль в этом в выявлении подобных трендов выполняют социальные сети.

Наиболее известным примером управления большими данными является управление с помощью прогнозирования, целью которого является попытка предсказать вероятность совершения преступлений в определенных районах в определенные периоды времени и последующее использование этих прогнозов для координации развертывания групп.

Так, например, полиция Лос-Анджелеса все больше полагается на технологии, которые не только сообщают патрульным офицерам, где

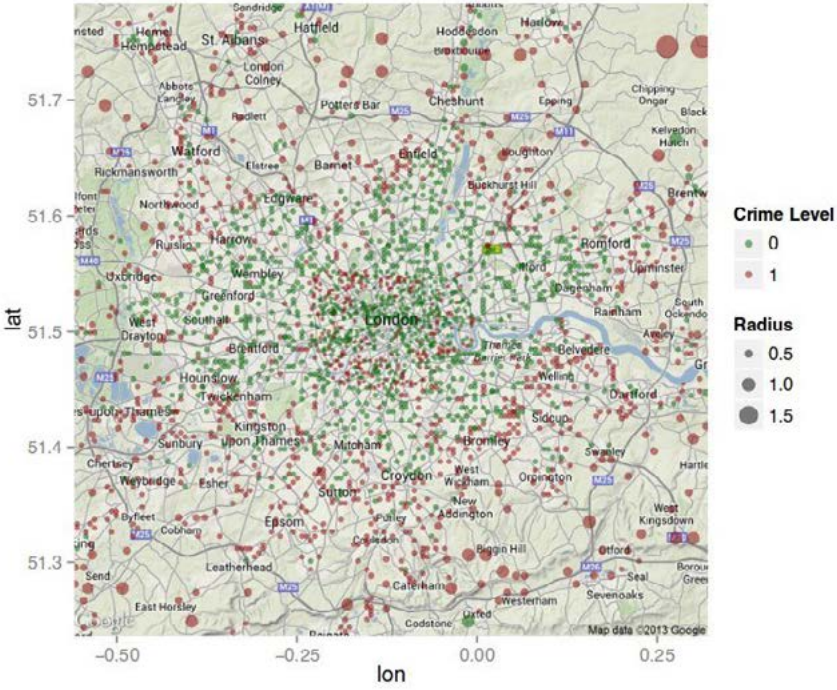

Рисунок 1. **Карта Лондона с «горячими точками»**

с наибольшей вероятностью могут произойти преступления, но также выявляют и отслеживают бывших заключенных и других потенциальных правонарушителей, которые, по их мнению, с наибольшей вероятностью совершат преступление. Полиция заявляет, что эти усилия уже помогли снизить уровень преступности в одном из самых печально известных и исторически бандитских районов города (Вестсайд). Система получила название LASER за её способность выявлять правонарушителей и «горячие точки», это один из многих новых инструментов правоохранительных органов, которые используют, отслеживают и собирают данные, например, сканируют государственные регистрационные номерные знаки автомобилей и биллинг мобильных телефонов, часто без ведома общественности или контроля. Считается, что полиция Лос-Анджелеса является «локомотивом» по анализу данных, что делает ее важным местом для проведения

этого исследования. Таким образом, практика анализа больших данных полицией Лос-Анджелеса может предсказывать более широкие тенденции, которые могут проявиться в других правоохранительных органах в ближайшие годы.

В полиции Нидерландов для прогнозирования используется система под названием «CAS». Система была разработана в 2014 года региональным полицейским подразделением г. Амстердама и после испытательного периода распространена на 160 передовых групп по всей территории Нидерландов. Программное обеспечение рисует на плане города сетку и по каждой секции определяет риск возникновения преступности и нарушений общественного порядка. Это достигается путем использования данных из полицейских систем, включая официальные отчеты и показатели преступности, в сочетании с информацией Статистического управления Нидерландов (автономное учреждение, которое собирает статистическую информацию по различным показателям в Нидерландах) о количестве социальных пособий, выплачиваемых в каждом районе, составе домохозяйств и т.д. Анализ больших данных широко используется сотрудниками правоохранительных органов в повседневной деятельности, речь идет о практических приложениях, ставших возможными благодаря цифровизации. У сотрудника полиции Нидерландов есть специальный смартфон, который представляет собой информационную панель для доступа к различным полицейским системам. Используя эту платформу, они могут на месте проверить, например, было ли у человека в прошлом насилие с применением огнестрельного оружия, или могут обратиться к базе данных разрешений, в которой перечислены все огнестрельное оружие и боеприпасы, зарегистрированные для законного использования. Используя платформу, они могут сканировать государственные регистрационные знаки автомобилей, которые система напрямую преобразует в «полезные» данные. Кроме того, они могут на законных основаниях запрашивать информацию у других государственных органов, например, чтобы проверить, зарегистрировано ли лицо в подразделении финансовой разведки Нидерландов (в Российской Федерации аналог Федеральной службы по финансовому мониторингу) в связи с подозрительными транзакциями или есть ли у него неоплаченные штрафы в Центральном

агентстве судебного взыскания. Сотрудники полиции не только используют функции поиска в приложениях, но и должны записывать свои выводы и действия.

Анализ больших данных используется и международными организациями, такими как Европол и Евроюст. Европол, например, создал информационную систему «Europol», которая содержит данные от полицейских организаций Европейского Союза. Управление большими данными также развивается благодаря сотрудничеству между правительствами разных стран на международном уровне.

Другим примером является система «Prüm». Это общеевропейская сеть, созданная для автоматического обмена отпечатками пальцев, профилями ДНК и информацией о транспортных средствах.

Еще примером является международная группа «Эгмонт». Целью данной группы является создание коллективного механизма для укрепления сотрудничества и обмена информацией, полезной для выявления и пресечения противоборство отмывания полученных преступных путем доходов, финансирования терроризма. В своем распоряжении она имеет разнообразные инструменты, эти инструменты варьируются от автоматизации до анализа больших данных и продвинутой аналитики с использованием искусственного интеллекта. Искусственный интеллект, космические возможности, большие данные и высокопроизводительные вычисления интегрированы в политику безопасности что является эффективным как в борьбе с преступностью, так и в обеспечении основных прав граждан [4–6].

В заключении следует отметить, что дальнейшее внедрение и развитие технологии больших данных в сфере предупреждения и борьбы с преступностью влечет за собой изменения в повседневной деятельности полицейских, технологические возможности, предлагаемые данной «сквозной» технологией, также оказывает влияние на структуру правоохранительных органов и ее сотрудников. Как и любой другой инструмент, большие данные и алгоритмы могут иметь как положительные, так и отрицательные эффекты в зависимости от того, как они используются. Следует ожидать, что в ближайшем будущем для решения задач полиции будут применяться более сложные и полностью самообучающиеся алгоритмы [7].

Список литературы

1. Информационные технологии управления и организация защиты информации / В. В. Баранов, И. В. Горошко, Б. А. Торопов [и др.]. — Москва: Академия управления Министерства внутренних дел Российской Федерации, 2018.— 456 с.
2. Кубасов И. А., Мельников А. В., Мальцев С. А., Нарушев И. Р. Кластеризация объектов со слабо формализуемыми признаками на основе нейронной сети в виде слоя Кохонена // Вестник Воронежского государственного университета инженерных технологий.— 2018. — Т. 80, № 3(77). — С. 86–91. — DOI 10.20914/2310–1202–2018–3–86–91.
3. Иванов А. И., Кубасов И. А., Самокутяев А. М. Тестирование больших нейронных сетей на малых выборках // Надежность и качество сложных систем.— 2020.— № 3(31). — С. 72–79. — DOI 10.21685/2307–4205–2020–3–9.
4. Кубасов И. А., Лекарь Л. А. Внедрение перспективных систем мониторинга и анализа больших данных, полученных в сети Интернет, для обеспечения деятельности оперативных подразделений МВД России // Труды Академии управления МВД России.— 2023.— № 3(67). — С. 154–161. — DOI 10.24412/2072–9391–2023–367–154–161.
5. Hill, D., O'Connor, C. D., and Slane, A. «Police Use of Facial Recognition Technology: The Potential for Engaging the Public through Co-constructed Policy-Making» //International Journal of Police Science & Management. –2022. –№ 24(3): С. 325–335.

УДК 004

Голос будущего здравоохранения: искусственный интеллект в распознавании речи, технологии, вызовы и перспективы в медицине

Нуреев Айдар Разилевич

магистрант, инженер-электроник Акционерного общества «ТАНЕКО» (г. Нижнекамск)

***Аннотация**: В статье проанализированы преимущества современных технологий в оптимизации процессов документации и взаимодействия с пациентами. Выявлены вызовы, связанные с точностью распознавания речи в реальных условиях, представлен анализ технологий для повышения надежности в различных клинических сценариях. Изучены методы интеграции технологий с электронными медицинскими записями для обеспечения непрерывного потока данных и улучшения доступности информации для медицинского персонала. Поднят вопрос о соблюдении стандартов конфиденциальности данных при внедрении технологий ИИ в медицину. 5. Обсуждаются потенциальные улучшения в точности диагностики, образовании медицинского персонала и персонализированных методах лечения.*

Результаты исследования свидетельствуют о значительном потенциале технологий распознавания речи в трансформации медицинской практики. Однако для успешного внедрения необходимо внимательное рассмотрение вызовов, та ких как точность и конфиденциальность данных. Решение этих проблем может максимально реализовать потенциал искусственного интеллекта в повышении эффективности здравоохранения.

***Abstract**: The article analyzed the advantages of modern technologies in optimizing the processes of documentation and interaction with patients. Challenges related to speech recognition accuracy in real-world settings are identified, and an analysis of technologies to improve reliability in various clinical scenarios is presented. Techniques for integrating technology with electronic medical records to ensure continuous data flow and improve accessibility of information to medical staff are explored. The issue of adhering to data privacy standards when implementing AI technologies in medicine is raised. 5. Potential improvements in diagnostic accuracy, medical staff education, and personalized treatments are discussed.*

The results of the study indicate the significant potential of speech recognition technologies in transforming medical practice. However, successful implementation requires careful consideration of challenges such as accuracy and data privacy. Addressing these challenges can maximize the potential of artificial intelligence in improving healthcare efficiency.

***Ключевые слова**: искусственный интеллект, распознавание речи, медицина, технологии здравоохранения, электронные медицинские записи, вызовы искусственного интеллекта, перспективы в медицине, точность диагностики, оптимизация медицинских процессов.*

***Keywords**: artificial intelligence, speech recognition, medicine, healthcare technologies, electronic medical records, challenges of artificial intelligence, prospects in medicine, diagnostic accuracy, optimization of medical processes.*

Введение

С внедрением искусственного интеллекта (ИИ) в различные сферы общества, медицинская индустрия не остается в стороне от инновационных технологических изменений. Одним из фундаментальных направлений этой эволюции становится использование ИИ в области распознавания речи. Эта передовая технология обещает преобразовать способы взаимодействия медицинского персонала с электронными медицинскими записями, диагностическими процедурами и общением с пациентами.

В современном здравоохранении, где эффективность, точность и скорость играют решающую роль, системы распознавания речи, основанные на ИИ, предоставляют медицинским профессионалам мощный инструмент. На фоне растущей потребности в повышении эффективности здравоохранения и сокращении бюрократических задач, эта технология представляет собой перспективный путь к оптимизации процессов и улучшению качества медицинской помощи.

В данной статье мы рассмотрим ключевые аспекты применения ИИ в системах распознавания речи в медицинской практике. Особое внимание будет уделено решениям, которые предоставляют медицинскому персоналу инструменты для более эффективной документации, диагностики и взаимодействия с пациентами. В процессе изучения этих инноваций мы также рассмотрим вызовы, с которыми сталкиваются разработчики и врачи, и потенциальные перспективы внедрения этой технологии для улучшения качества медицинской помощи в будущем.

Цель

Исследование направлено на анализ применения искусственного интеллекта в распознавании речи в медицине с целью понимания технологий, вызовов и перспектив в этой области.

Методы

Оценка существующих источников для анализа современных технологий распознавания речи в медицине, исследование преимуществ и ограничений различных систем искусственного интеллекта в медицинской практике, предоставление полного обзора вызовов, с которыми сталкиваются разработчики и врачи при внедрении технологий распознавания речи, рассмотрение практических примеров успешного внедрения систем распознавания речи в реальной медицинской среде. Ключевым методом является системный анализ технологий распознавания речи, предоставляя читателям глубокое понимание того, как эти методы могут преобразовать современные подходы к здравоохранению.

Роль ИИ

Искусственный интеллект (ИИ) в сфере распознавания речи стал неотъемлемой частью медицинской практики, преобразуя способы взаимодействия медицинского персонала с информацией, пациентами и документацией. Вот несколько ключевых ролей, которые ИИ играет в распознавании речи в медицинской области:

1. Оптимизация электронных медицинских записей (ЭМР)

Точность и эффективность: ИИ в распознавании речи позволяет создавать и обновлять ЭМР с высокой степенью точности. Врачи могут диктовать заметки, диагнозы и планы лечения, и системы ИИ преобразуют речь в текст, что экономит время и уменьшает вероятность ошибок.

2. Диагностика и анализ изображений

Радиология и изображения: Использование ИИ в анализе медицинских изображений, таких как рентгеновские снимки и МРТ, позволяет автоматизировать процессы диагностики. Системы распознавания речи могут дополнить этот процесс, добавляя контекст и комментарии, улучшая взаимодействие врачей с изображениями.

3. Обучение и медицинское образование

Интерактивные обучающие платформы: ИИ в распознавании речи может быть включен в медицинские образовательные платформы. Это упрощает доступ к медицинской информации, обучению и подготовке медицинского персонала.

4. Пациентская связь и общение

Интерактивные ассистенты и боты: Использование ИИ в распознавании речи позволяет создавать интеллектуальных ассистентов, которые могут отвечать на вопросы пациентов, предоставлять информацию о заболеваниях, назначениях и поддерживать общение с пациентами.

5. Персонализированное лечение и прогнозирование

Анализ данных и прогнозирование: ИИ способен анализировать большие объемы данных пациента, включая текстовую информацию из медицинских записей и результаты анализов. Это позволяет предсказывать вероятность заболеваний, эффективность терапии и предоставлять персонализированные подходы к лечению.

Искусственный интеллект в распознавании речи в медицине не только улучшает эффективность работы медицинского персонала, но и повышает качество обслуживания пациентов, делая здравоохранение более доступным, точным и персонализированным.

Технологии и методы

Внедрение искусственного интеллекта (ИИ) в распознавание речи в медицине осуществляется при помощи разнообразных технологий и методов, которые революционизируют процессы документации, диагностики и общения в здравоохранении.

1. Автоматическое распознавание речи (ASR)

Технология ASR: Это ключевая технология, которая позволяет переводить аудио-сигналы, записанные медицинским персоналом или пациентами, в текст. Системы ASR обучаются на больших объемах аудио-данных для повышения точности распознавания.

2. Машинное обучение и нейронные сети

Обучение на Медицинских Данных: Методы машинного обучения, включая глубокие нейронные сети, используются для тренировки систем распознавания речи на медицинских данных. Это позволяет системам учиться от контексте и особенностях медицинской лексики.

3. Обработка естественного языка (NLP)

Понимание Медицинских Текстов: Технологии NLP применяются для более глубокого понимания контекста и смысла медицинских текстов. Это включает в себя разбор специфических терминов, аббревиатур и различных форм изложения медицинской информации.

4. Интерфейсы искусственного интеллекта для медицинского персонала

Голосовые Ассистенты: Разработка голосовых ассистентов, ориентированных на медицинский контекст, позволяет врачам и медсестрам взаимодействовать с медицинскими записями и системами без необходимости использования клавиатуры.

5. Биометрическая идентификация

Идентификация Голоса: Технологии идентификации голоса используются для подтверждения личности медицинского персонала при доступе к чувствительным медицинским данным, что способствует безопасности данных пациентов.

6. Интеграция с электронными медицинскими записями (ЭМР)

API и Системы Интеграции: Технологии, позволяющие интегрировать системы распознавания речи напрямую с ЭМР, обеспечивают бесперебойный обмен информацией и уменьшают время, затрачиваемое на внесение данных.

7. Обучение с учителем и без учителя

Системы обучения с учителем: Используют аннотированные данные для обучения систем точному распознаванию медицинской речи.

Системы обучения без учителя: Анализируют данные без предварительной разметки, что особенно полезно для обработки медицинских данных с высокой степенью разнообразия.

Эффективное внедрение этих технологий и методов в медицинскую практику предоставляет новые возможности для повышения производительности, точности и обогащения данных в здравоохранении.

Вызовы и перспективы

Вопреки значительному прогрессу в области распознавания речи с использованием искусственного интеллекта в медицинской практике, существуют вызовы, которые требуют внимания и решения для полноценного внедрения этой технологии. Однако вместе с вызовами предоставляются перспективы, расширяющие горизонты эффективности и точности в предоставлении медицинской помощи.

Вызовы

1. Точность распознавания:
   - Проблема: В неконтролируемых условиях, таких как шумные медицинские палаты, точность распознавания может снижаться, что приводит к потенциальным ошибкам в медицинской документации.
   - Решение: Улучшение алгоритмов и обучение моделей на разнообразных аудио-данных для повышения устойчивости к различным условиям.
2. Конфиденциальность и безопасность:
   - Проблема: Медицинская информация является чрезвычайно чувствительной, и безопасность данных при использовании систем распознавания речи становится вопросом высокой важности.
   - Решение: Применение передовых методов шифрования и обеспечение соблюдения стандартов безопасности в здравоохранении.
3. Интеграция с практическими аспектами:
   - Проблема: Некоторые медицинские процессы могут требовать сложных интеграций, а сопротивление со стороны медицинского персонала может затруднить внедрение новых технологий.
   - Решение: Обучение медицинского персонала и создание более удобных и интуитивных интерфейсов для использования.

Перспективы

1. Улучшение медицинской документации:
   - Перспектива: Распознавание речи может значительно улучшить процессы создания и обновления электронных медицинских записей, уменьшая бремя бумажной работы для врачей.
2. Более точные диагнозы и планы лечения:
   - Перспектива: Использование ИИ в распознавании речи может значительно улучшить точность диагностики и предоставления персонализированных планов лечения на основе анализа больших объемов данных.

3. Обогащение врачебного образования:
   - Перспектива: Интеграция систем распознавания речи в медицинское образование может улучшить процессы обучения и доступа к медицинской информации для будущего медицинского персонала.
4. Снижение расходов и увеличение эффективности:
   - Перспектива: Использование технологий распознавания речи может привести к сокращению времени, затрачиваемого на документацию и обработку данных, что в конечном итоге снизит расходы и повысит эффективность медицинской практики.

Более глубокое понимание и решение вызовов, а также активное внедрение перспективных аспектов, позволит максимально использовать потенциал искусственного интеллекта в распознавании речи в медицине. Решение вызовов, связанных с точностью распознавания, конфиденциальностью данных и интеграцией с медицинскими процессами, требует совместных усилий медицинских профессионалов, разработчиков и технологических специалистов.

Активное внедрение перспективных аспектов, таких как улучшение медицинской документации, точность диагностики, обогащение врачебного образования и снижение расходов, создает обширные возможности для трансформации здравоохранения. Искусственный интеллект в распознавании речи в медицине не только улучшает текущие процессы, но и создает новые перспективы для персонализированного и более эффективного оказания медицинской помощи.

В конечном итоге, при правильном использовании и развитии этих технологий, мы можем ожидать значительного улучшения качества заботы о пациентах, сокращения времени, затрачиваемого на бумажную работу, и повышения общей эффективности медицинской практики.

Список литературы

1. Everett, M., Redner, J., Kalenscher, A., Durso, D. & Nguyen, S. (Fall 2022). “Speech Recognition Technology for Increasing Nursing Documentation Efficiency.” Online Journal of Nursing Informatics (OJNI), 26(2).

2. Hodgson, T., et al. (2018). “Evaluating the Usability of Speech Recognition to Create Clinical Documentation Using a Commercial Electronic Health Record.” International Journal of Medical Informatics.
3. Lee, T. Y., Li, C. C., Chou, K. R., Chung, M. H. (October 2023). “Machine Learning-Based Speech Recognition System for Nursing Documentation — A Pilot Study.” International Journal of Medical Informatics, Volume 178, 105213.
4. Dinari, F., Bahaadinbeigy, K., Bassiri, S., Mashouf, E., Bastaminejad, S., & Moulaei, K. (2023). “Benefits, Barriers, and Facilitators of Using Speech Recognition Technology in Nursing Documentation and Reporting.” Health Sci Rep, 6(6), e1330.
5. Kumah-Crystal, Y. A., Pirtle, C. J., Whyte, H. M., Goode, E. S., Anders, S. H., & Lehmann, C. U. (2018). “Electronic Health Record Interactions through Voice: A Review.” Applied Clinical Informatics, 9(3), 541–552.
6. Chen, H., Chen, S., Zhao, J. (29 March 2022). “Integrated Design of Financial Self-Service Terminal Based on Artificial Intelligence Voice Interaction.” Frontiers in Psychology, Section: Educational Psychology.

Журнал «Научный аспект №12 2023»

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

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