ISSN 2518-1092

НАУЧНЫЙ РЕЗУЛЬТАТ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

RESEARCH RESULT. INFORMATION TECHNOLOGY

9(1) 2024

16+

Сайт журнала:
rrinformation.ru
сетевой научный рецензируемый журнал
online scholarly peer-reviewed journal

НАУЧНЫЙ РЕЗУЛЬТАТ
RESEARCH RESULT

НАУЧНЫЙ РЕЗУЛЬТАТ. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
RESEARCH RESULT. INFORMATION TECHNOLOGIES

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
Свидетельство о регистрации средства массовой информации Эл. № ФС77-69101 от 14 марта 2017 г.

The journal has been registered at the Federal service for supervision of communications information technology and mass media (Roskomnadzor)
Mass media registration certificate El. № FS 77-69101 of March 14, 2017

Том 9, № 1. 2024

СЕТЕВОЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
Издается с 2016 г.
ISSN 2518-1092

Volume 9, № 1. 2024

ONLINESCHOLARLYPEER-REVIEWEDJOURNAL
First published online: 2016
ISSN 2518-1092

Учредитель: Федеральное государственное автономное образовательное учреждение высшего образования
«Белгородский государственный национальный исследовательский университет»
Издатель: НИУ «БелГУ». Адрес издателя: 308015 г. Белгород, ул. Победы, 85.
Журнал выходит 4 раза в год

Founder: Federal state autonomous educational establishment of higher education
«Belgorod State National Research University»
Publisher: Belgorod State National Research University
Address of publisher: 85 Pobeda St., Belgorod, 308015, Russia
Publication frequency: 4 /year

СОДЕРЖАНИЕ

CONTENTS

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

INFORMATION SYSTEM AND TECHNOLOGIES

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ

AUTOMATION AND CONTROL

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРИНЯТИЕ РЕШЕНИЙ

ARTIFICIAL INTELLIGENCE AND DECISION MAKING

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
INFORMATION SYSTEM AND TECHNOLOGIES

УДК 004:056 **DOI: 10.18413/2518-1092-2024-9-1-0-1**

Чайка Е.М.
Белов С.П.

ОБЗОР КРИПТОШЛЮЗОВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СЕТЯХ

Белгородский университет кооперации, экономики и права,
ул. Садовая, д. 116а, г. Белгород, 308023, Россия

e-mail: desare48@yandex.ru, belovssergei@gmail.com

Аннотация
В данной статье рассматриваются решения отечественных производителей для организации защищенной корпоративной сети (криптошлюзы, VPN шлюзы), основные принципы работы данного оборудования, сценарии подключения и основные используемые протоколы, проведен анализ доступных для органов государственной и федеральной власти решений, согласно законодательства и требований регуляторов, проведен анализ стадий сертификации компонентов рассматриваемых решений, совместимость с отечественными операционными системами, рассматривается возможность применения комплексных решений в организациях.
Ключевые слова: шифрование; защищенные VPN-шлюзы; корпоративные сети; VipNet; Континент; Dionis
Для цитирования: Чайка Е. М., Белов С.П. Обзор криптошлюзов для защиты информации в корпоративных сетях // Научный результат. Информационные технологии. – Т.9, №1, 2024. – С. 3-9. DOI: 10.18413/2518-1092-2024-9-1-0-1

Chayka E.M.
Belov S.P.

OVERVIEW OF CRYPTOGRAPHIC GATEWAYS FOR PROTECTION INFORMATION IN CORPORATE NETWORKS

Belgorod University of Cooperation, Economics and Law,
116a Sadovaya str., Belgorod, 308023, Russia

e-mail: desare48@yandex.ru, belovssergei@gmail.com

Abstract
This article discusses solutions from domestic manufacturers for the organization of a secure corporate network (cryptoslocks, VPN gateways), the basic principles of operation of this equipment, connection scenarios and the main protocols used, an analysis of solutions available to state and federal authorities, according to legislation and regulatory requirements, an analysis of the stages of certification of components of the solutions in question, compatibility with domestic ones The possibility of using integrated solutions in organizations is being considered.
Keywords: encryption; secure VPN gateways; corporate networks; ViPNet; Continent; Dionis
For citation: Chayka E.M., Belov S.P. Overview of cryptographic gateways for protection information in corporate networks // Research result. Information technologies. – T.9, №1, 2024. – P. 3-9. DOI: 10.18413/2518-1092-2024-9-1-0-1

ВВЕДЕНИЕ

Для осуществления эффективного менеджмента в современных реалиях, защита информации является обязательным условием и необходима на всех этапах развития деятельности организации. Информационная безопасность в организации основывается на комплексном подходе,

использовании как организационных мер, так и мероприятий по технической защите. В рамках данной статьи рассмотрим направление защиты информации непосредственно в корпоративных сетях и сетях Интернет (далее – сети). Но перед этим нужно остановится на основных задачах информационной безопасности. К ним относят: оперативный доступ к информационным услугам и к информации в целом в организации; актуальность и целостность информации, а также конфиденциальность данных.

Специалистами по информационной безопасности отмечается, что наиболее распространёнными угрозами в последнее время на сети организаций являются так называемые кибератаки, но при этом не стоит забывать про фишинг, вирусы и иное вредоносное ПО (программное обеспечение), высокий риск реализации угроз безопасности возможен и с использованием социальной инженерии.

Не стоит соответственно забывать и про технические ошибки, которые в свою очередь приводят к реализации уязвимостей в используемых информационных системах.

Для решения задач по защите сетей применяются такие методы как, внедрение межсетевых экранов, шифрование передаваемой информации, использование средства аутентификации и авторизации, системы регистрации событий безопасности и управление доступом к ресурсам.

Большая часть этого функционала реализована в программно-аппаратных комплексах для криптографической защиты трафика, передаваемого по каналам связи, при помощи так называемых «туннельных соединений» между компьютером пользователя и компьютером-сервером с использованием различных протоколов.

В состав данных комплексов опционально входят средства аутентификации и авторизации, с помощью которых происходит идентификация пользователей системы, определяются их права доступа к ресурсам; средства обнаружения и предотвращения вторжений (IDS/IPS) для обеспечения дополнительного уровня защиты.

Для реализации рассматриваемых «туннельных соединений» в организациях используется специализированное оборудование под названием VPN (Virtual Private Network) (криптографический шлюз, криптошлюз).

В последние годы отечественный рынок крипторешений стремительно активизировался, обосновать данную тенденцию можно несколькими причинами. Во-первых, активная политика регуляторов, нацеленная на защиту каналов связи, стимулирует организации обеспечивать безопасность передаваемых данных. Во-вторых, массовый переход на удаленную работу усилил потребность в реальной, а не только «бумажной» безопасности.

ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ КРИПТОШЛЮЗОВ (СЦЕНАРИИ ПОДКЛЮЧЕНИЯ, ИСПОЛЬЗУЕМЫЕ ПРОТОКОЛЫ), КРИТЕРИИ ВЫБОРА

Для начала рассмотрим понятие VPN (виртуальная частная сеть) более подробно. Виртуальная частная сеть – это комплекс решений, обеспечивающих безопасную и качественную связь между территориально распределенными подсетями и группами пользователей через открытую сеть Интернет. Существуют два типичных сценария использования VPN: "site-to-site" (объединение площадок) и "client-to-site" (удаленный доступ).

Сценарий "site-to-site" – это безопасное соединение двух точек с помощью аппаратных шлюзов, которые обеспечивают высокую скорость соединения. Данные решения часто используются в глобальных сетях для подключения локальных сетей предприятий. Сценарии данного типа позволяют обеспечить шифрование всех пакетов данных при передаче через VPN туннель. Одним из преимуществ данного способа является масштабируемость, достаточно установить и настроить дополнительный VPN-шлюз для ввода в эксплуатацию нового удаленного офиса. При этом не стоит забывать о растущей потребности в создании более производительных каналов связи между центральными офисами организации, в некоторых случаях требуются каналы

с пропускной способностью более 100 ГБ, что требует использования кластера VPN-шлюзов. К рискам данного решения можно отнести уязвимости в аппаратном и программном обеспечении.

Рассмотрим другой сценарий реализации VPN "client-to-site". Он позволяет удаленным пользователям получить доступ к своим ресурсам во время работы из удаленного места, в этом способе реализации туннеля основные проблемой является с масштабируемость, при этом стоимость данного решения гораздо ниже, чем предыдущий рассматриваемый вариант.[10]

Дополнительным различием в построении шифрованных туннелей служит создание соединений используя на основе протокол L2 VPN (Layer 2 Virtual Private Network) и протокол L3 VPN (Layer 3 Virtual Private Network). Рассмотрим основные отличия данных способов создания виртуальных соединений. L2 VPN (VPN на основании канального уровня) – вид соединений работает на канальном уровне OSI.

Передача данных осуществляется при помощи фреймов, а не пакетов. Главным преимуществом этой технологии является виртуальное объединение удаленных локальных сетей в одну единую сеть [11].

При построении сетей VPN на основании L3 (Layer 3 Virtual Private Network) работа происходит на третьем уровне OSI (Open Systems Interconnection). L3 VPN создает сеть на основе IP-адресов, в которой удалённые устройства, так же, как и в L2VPN, обмениваются информацией независимо от расположения. Выбор технологии зависит от конкретных задач организации, если требуется объединить несколько сетей, которые будут работать как одна сетевая структура, то предпочтительно использовать L2 VPN, если нужно получить защищенную, гибкую в настройке систему то L3 VPN.

Современные шлюзы, рассматриваемые в рамках данной статьи, обеспечивает защиту, передаваемых по различным каналам связи как с использованием на канальном уровень OSI (L2 VPN), так и на сетевом уровне (L3 VPN).

VPN-шлюзы являются универсальными решениями, и обладают большим функционалом, при выборе важно основываться на многих параметрах, таких как наличие сертификатов регуляторов в сфере информационной безопасности, ценовая политика производителя оборудования, доступность технической поддержки, технические характеристики: пропускная способность оборудования, поддержка различных операционных систем, возможно запуска в среде виртуализации, дополнительные встроенные решения.

Нужно понимать, что выбор VPN-шлюза должен основываться на анализе требований конкретной организации, а также на обеспечении безопасности и удобства использования для конечных пользователей.

ОБЗОР РЕШЕНИЙ, ПРЕДСТАВЛЕННЫХ НА ОТЕЧЕСТВЕННОМ РЫНКЕ.

По данным интернет-издания www.anti-malware.ru в 2023 год на Российском рынке представлены продукты следующих российских вендоров:

- «Атликс-VPN» («НТЦ Атлас»);
- «ЗАСТАВА» («ЭЛВИС-ПЛЮС»);
- «Континент» («Код Безопасности»);
- «С-Терра Шлюз» («С-Терра СиЭсПи»);
- «ФПСУ-IP» («АМИКОН», «ИнфоКрипт»);
- ALTELL NEO («АльтЭль»);
- Diamond VPN (ТСС);
- Dionis-DPS («Фактор-ТС»);
- NGate («КриптоПро»);
- ViPNet Coordinator HW («ИнфоТеКС»).[7]

Рассмотрим три популярных продукта, применяемых в государственных и федеральных органах Российской Федерации. Технические характеристики были получены с официальных ресурсов производителей рассматриваемого оборудования.

Dionis DPS, производство компании ООО «Фактор-ТС». Это единый центр управления защитой сети, сертифицированный ФСБ и ФСТЭК России. Применяется для защищенной передачи конфиденциальной информации через сети общего пользования в качестве пограничного устройства между защищаемыми локальными сетями и транспортной средой. В ПАК (программно-аппаратный комплекс) Dionis DPS реализованы алгоритмы шифрования в соответствии с государственными стандартами Российской Федерации. Комплекс поддерживает два варианта VPN-туннелей, основное отличие которых состоит в том, что при их построении используются две разные схемы распределения ключей шифрования (симметричная и несимметричная). Программные компоненты комплекса включают в себя «DiSec» (клиент для обеспечения защищенного доступа мобильных абонентов), «DioPost» (защищенный почтовый клиент).

Модельный ряд ориентирован как на небольшие компании, так и на крупные организации с большими центрами обработки данных. Обеспечивается скорость шифрования от 100 Мбит/с до 8000 Мбит/с. Имеется сертификат ФСТЭК России на МЭ типа «А» 2-го класса защиты и на СОВ уровня сети 2-го класса защиты, сертификат ФСБ России для СКЗИ (средства криптографической защиты информации) по классам КС1, КС3 [6].

VipNet Coordinator HW/VA, производство компании АО «ИнфоТеКС».

ПАК VipNet Coordinator HW - ряд криптошлюзов (криптомаршрутизаторов) предназначенных для построения виртуальной сети VipNet и обеспечения безопасной передачи данных между её защищенными сегментами, а также фильтрации IP-трафика.

Благодаря функциям криптографической защиты данных, межсетевого экранирования, а также наличию встроенных сетевых сервисов ПАК VipNet Coordinator HW является оптимальным средством защиты компьютерных сетей организаций от несанкционированного доступа к ее ресурсам при передаче информации по открытым каналам связи. Программный комплект состоит из ViPNet Administrator 4 (программное обеспечение, предназначенное для развертывания и администрирования сети ViPNet корпоративного масштаба), ViPNet Client 4U (программный комплекс ViPNet Client 4U для защиты рабочих мест пользователей и мобильных устройств), ViPNet Деловая почта (программное обеспечение для обмена электронными письмами в защищенной сети ViPNet).

В зависимости от модификации ПАК VipNet Coordinator HW позволяет организовать защищенный доступ как в ЦОДы (центры обработки данных), так и в корпоративную облачную инфраструктуру, может быть использован для защиты филиалов организаций, небольших удаленных офисов, удаленных рабочих мест, а также терминалов и устройств, в том числе обеспечивая безопасное подключение к корпоративной защищенной сети по беспроводным каналам связи. Модельный ряд включает в себя оборудование с широким диапазоном производительности: от 75 Мбит/с до 10 000 Мбит/с. Имеются сертификаты соответствия по требованиям безопасности ФСБ России и ФСТЭК России. Из особенностей также доступно виртуализированное исполнение – VipNet Coordinator VA (СКЗИ класса КС1) для развёртывания на популярных платформах виртуализации [9].

АПКШ «Континент», производство компании ООО «Код Безопасности». Представляет собой централизованный комплекс для защиты сетевой инфраструктуры и создания VPN-сетей с использованием алгоритмов ГОСТ. Модельный ряд позволяет подобрать решение для организации связи с удалёнными подразделениями, филиалами или партнёрами по каналам связи с различной пропускной способностью и возможностью централизованного управления. Производительность L2 VPN варьируется от 120 Мбит/с до 40 000 Мбит/с. При этом на специализированной аппаратной платформе «Континент 3.9 IPC-3000FC-40G» реализован криптоускоритель с производительностью VPN ГОСТ до 40 Гбит/с и задержками обработки трафика около 50 мкс. В наличии сертификаты соответствия по требованиям безопасности ФСТЭК России, ФСБ России, Минкомсвязи и Минобороны России. Программные средства, включенные в комплекс: Континент-АП (для

организации доступа удаленных пользователей по защищенному каналу к ресурсам, защищаемым средствами АПКШ).[8]

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА КРИПТОШЛЮЗОВ

Систематизируем основные характеристики трех рассматриваемых решений, представленных в этой статье:

Согласно требованиям регуляторов ФСБ и ФСТЭК в информационных системах персональных данных, государственных информационных системах, автоматизированных системах управления производственными и технологическими процессами применяются только сертифицированные средства защиты информации. Информация о сертификации криптошлюзов (Таблица 1) и программных компонентов (Таблица 2) представлены ниже [1-5].

Таблица 1

Сертификация криптошлюзов

Table 1

Certification of cryptographic gateways

Наименование решения	Сертификат ФСБ КС1/КС2/КС3	Сертификат ФСТЭК
Дионис DPS/NX	+/-/+	+
Vipnet Coordinator	+/+/+	+
Континент АПКШ	+/+/+	+

Таблица 2

Сертификация программных компонентов

Table 2

Certification of software components

Наименование ПО	Сертификат ФСБ Windows	Сертификат ФСБ Linux	Сертификат ФСТЭК Windows	Сертификат ФСТЭК Linux
Dionis DiSec	+	-	+	-
Dionis DioPost	+	-	+	-
ViPNet Administrator 4	+	-	+	-
ViPNet Client 4U	+	-	+	-
ViPNet Деловая почта	+	-	+	-
Континент-АП	+	+	+	+

Рассматривая результаты сравнения наличия сертификатов видно, что большинство продукции не имеет действующих сертификатов соответствия (многие продукты в настоящий момент проходят сертификацию), следовательно, в одиночном исполнении криптошлюзы (VPN-шлюзы) полностью подходят по требования законодательства, а вот использование прикладного программного обеспечения в органах государственной

и федеральной власти попадает под сомнение. Решение данной проблемы только в одном, это ожидание завершения процедур тестирования и сертификации программного обеспечения.

И все же, представленные комплексные решения получили высокие положительные оценки среди специалистов информационной безопасности на рынке криптомашрутизаторов и VPN-шлюзов.

В настоящее время Vipnet Coordinator применяется в государственных структурах для обеспечения безопасности при построении сети, Dionis DPS широкое применение получил в федеральных органах, Континент-АП – в реализациях государственных информационных систем федерального уровня.

ЗАКЛЮЧЕНИЕ

Мы рассмотрели в данной статье определенный класс устройств, используемые в качестве криптомаршрутизаторов и VPN-шлюзов. Из технических характеристик наблюдается, что рассматриваемые решения выполняют не одну, изначально заложенную, функцию, а являются более универсальными средствами для обеспечения безопасности и конфиденциальности информации при передаче по сети. В функционал, помимо создания шифрованных виртуальных туннелей, входят дополнительные сервисы: DHCP, DNS, Proxy-серверы.

Какое дальнейшее развитие этого класса ждет нас в будущем? Либо это будет «комбайн» функций, либо развитие пойдет по дроблению на отдельные устройства и сервисы, пока ответить однозначно сложно. При этом развитие технологий идет по пути использования универсальных устройств, такой подход позволяет строить систему безопасности из однородных компонентов, что положительно сказывается на возможностях администрирования и обслуживания сетей. Также к преимуществам универсальности подобных устройств можно отнести экономическую выгоду и удобство для организаций.

На отечественном рынке криптошлюзов с каждым годом появляются новые игроки, большую роль в этом развитии имеют регуляторы в области информационной безопасности. Нормативные акты ФСБ и ФСТЭК положительно влияют на развитие рынка отечественных сертифицированных VPN решений. Это позволяет российским производителям участвовать в постепенной замене импортных решений и помогает развивать отечественные аналоги. Но при этом одной из ключевых проблем для рынка криптошлюзов в России остается отсутствие аппаратных платформ для построения полностью импортонезависимого продукта.

Список литературы

1. ФЗ №149 от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации».

2. Постановление правительства №1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. Приказ №17 ФСТЭК от 11.02.2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

4. Приказ №21 ФСТЭК от 18.02.2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

5. Приказ №31 ФСТЭК от 14.03.2014 г. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

6. Возможности Dionis DPS. URL: https://dps.factor-ts.ru/vozmozhnosti, дата обращения: 01.12.2023 [Электронный ресурс].

7. Зензин И. «Обзор криптографических шлюзов российских и зарубежных производителей». URL: https://www.anti-malware.ru/analytics/Market_Analysis/cryptographic-gateways-russian-and-foreign-manufacturers-2017, дата обращения: 01.12.2023 [Электронный ресурс].

8. Комплекс безопасности Континент Версия 4 Руководство администратора Принципы функционирования URL: https://www.securitycode.ru/upload/iblock/a6c/mjqueclwoehg014tilmlinzmbwxfdlc5/Continent-Basics-AdminGuide.pdf, дата обращения: 01.12.2023 [Электронный ресурс].

9. Криптографический шлюз безопасности – Межсетевой экран нового поколения VipNet Coordinator HW 5. URL: https://infotecs.ru/products/vipnet-coordinator-hw-5/, дата обращения: 01.12.2023 [Электронный ресурс].

10. Сарычев Д. «Как выбрать корпоративный VPN-шлюз», URL: https://www.anti-malware.ru/practice/methods/How-to-choose-VPN-gateway#part4, дата обращения: 01.12.2023 [Электронный ресурс].

11. SIM-Networks, Каналы связи L2 и L3 VPN – отличия физических и виртуальных каналов разного уровня. URL: https://www.sim-networks.com/ru/blog/the-difference-between-layer-2-and-layer-3-networks, дата обращения: 01.12.2023 [Электронный ресурс].

References

1. Federal Law No. 149 dated 07/27/2006 "On Information, Information Technologies and Information Protection".

2. Government Resolution No. 1119 dated 11/01/2012 "On approval of requirements for the protection of personal data during their processing in personal data information systems".

3. Order No. 17 of the Federal Customs Service of 11.02.2013 "On approval of requirements for the protection of information that does not constitute a State Secret contained in State information systems."

4. FSTEC Order No. 21 dated 02/18/2013 "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems".

5. FSTEC Order No. 31 dated 03/14/2014 "On Approval of Requirements for Ensuring Information Protection in Automated Control Systems for Production and Technological Processes at Critical Facilities, potentially Dangerous facilities, as well as facilities that pose an increased danger to human life and health and to the environment".

6. Features of Dionis DPS Source: https://dps.factor-ts.ru/vozmozhnosti, date of access: 12/01/2023, electronic text.

7. Zenzin I. "Overview of cryptographic gateways of Russian and foreign manufacturers" Source: https://www.anti-malware.ru/analytics/Market_Analysis/cryptographic-gateways-russian-and-foreign-manufacturers-2017, accessed: 12/01/2023, electronic text.

8. Security Complex Continent Version 4 Administrator's Guide Principles of operation https://www.securitycode.ru/upload/iblock/a6c/mjqueclwoehg014tilmlinzmbwxfdlc5/Continent-Basics-AdminGuide.pdf, accessed: 12/01/2023, electronic text

9. Cryptographic Security Gateway – A new generation Firewall ViPNet Coordinator HW 5 Source: https://infotecs.ru/products/vipnet-coordinator-hw-5 /, date of access: 12/01/2023, electronic text.

10. Sarychev D. "How to choose a corporate VPN gateway", Source: https://www.anti-malware.ru/practice/methods/How-to-choose-VPN-gateway#part4, date of access: 12/01/2023, electronic text.

11. SIM Networks, L2 and L3 VPN communication channels – differences between physical and virtual channels of different levels. Source: https://www.sim-networks.com/ru/blog/the-difference-between-layer-2-and-layer-3-networks, date of access: 12/01/2023, electronic text.

Чайка Евгений Михайлович, магистрант 2 курса кафедры информационная безопасность
Белов Сергей Павлович, доктор технических наук, профессор, профессор кафедры информационной безопасности

Chayka Evgeny Mikhailovich, 2nd year Master's student, Department of Information Security
Sergey Pavlovich Belov, Doctor of Technical Sciences, Professor, Professor of the Department of Information Security

УДК 004.05 **DOI: 10.18413/2518-1092-2024-9-1-0-2**

Кузьминых Е.С.
Ильина С.П.
Маслова М.А.

АНАЛИЗ НЕПРОБИВАЕМЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Севастопольский государственный университет,
ул. Университетская, 33, г. Севастополь, 299053, Россия

e-mail: egor2014ru@mail.ru, sofi.ilina@mail.ru, mashechka-81@mail.ru

Аннотация
В данной статье исследуются непробиваемые алгоритмы шифрования, включая DES, RSA и AES, с установленной целью определения наиболее надежного и безопасного алгоритма шифрования. Статья анализирует характеристики каждого из шифров, такие как длина ключа, стойкость и актуальность, а также оценивает их популярность и применение в современных криптографических реалиях. В результате исследования сделан вывод, что AES является самым превосходным вариантом. Это объясняется тем, что DES и RSA уже были взломаны и имеют известные уязвимости, тогда как AES продолжает быть безопасным и лучшим из представленных шифров. Статья заключается в том, что AES рекомендуется для использования в системах, где требуется надежное и непроницаемое шифрование.
Ключевые слова: информационная безопасность; безопасность; кибербезопасность; непробиваемые алгоритмы шифрования; программирование; криптография; шифрование; RSA; DES; AES; ECB; CBC; взлом шифра; безопасность шифра; квантовые компьютеры; квантовая криптография
Для цитирования: Кузьминых Е.С., Ильина С.П., Маслова М.А. Анализ непробиваемых алгоритмов шифрования // Научный результат. Информационные технологии. – Т.9, №1, 2024. – С. 10-18. DOI: 10.18413/2518-1092-2024-9-1-0-2

Kuzminykh E.S.
Ilina S.P.
Maslova M.A.

ANALYSIS OF IMPENETRABLE ENCRYPTION ALGORITHMS

Sevastopol State University,
33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: egor2014ru@mail.ru, sofi.ilina@mail.ru, mashechka-81@mail.ru

Abstract
This article explores impenetrable ciphers, including DES, RSA and AES, with the stated goal of determining the most reliable and secure encryption algorithm. The article analyzes the characteristics of each of the ciphers, such as key length, durability and relevance, and also evaluates their popularity and application in modern cryptographic realities. As a result of the study, it was concluded that AES is the most excellent option. This is because DES and RSA have already been hacked and have known vulnerabilities, whereas AES continues to be secure and the best of the ciphers presented. The article is that AES is recommended for use in systems where reliable and impenetrable encryption is required.
Keywords: information security; security; cybersecurity; code; programming; cryptography; encryption; RSA; DES; AES; ECB; CBC; cipher hacking; cipher security; quantum computers; quantum cryptography
For citation: Kuzminykh E.S., Ilina S.P., Maslova M.A. Analysis of impenetrable encryption algorithms // Research result. Information technologies. – T. 9, №1, 2024. – P. 10-18. DOI: 10.18413/2518-1092-2024-9-1-0-2

ВВЕДЕНИЕ

Шифрование информации является основополагающим принципом для обеспечения конфиденциальности и безопасности данных в цифровой эпохе. Это процесс преобразования информации в непонятную форму, непроходимую для несанкционированного доступа. На протяжении многих лет, криптографы разработали разнообразные алгоритмы шифрования, чтобы защитить данные от злоумышленников и обеспечить безопасность коммуникации. Однако, современные технологии и вычислительная мощность постоянно развиваются, и то, что ранее считалось непробиваемым, может стать уязвимым. Существуют алгоритмы шифрования, которые не возможно взломать математически, а только с помощью брутфорса – это и есть непробиваемые алгоритмы шифрования. В свете этого возникает важный вопрос: насколько надежны и безопасны существующие алгоритмы шифрования?

Целью данной статьи является анализ непробиваемых алгоритмов шифрования, с целью оценки их надежности и выявления возможных уязвимостей. Будут рассмотрены различные алгоритмы шифрования, такие как DES, RSA и AES, а также проанализированы их фундаментальные принципы и математическая основа.

ОСНОВНАЯ ЧАСТЬ

Рассмотрим один из наиболее известных алгоритмов — DES (Data Encryption Standard). DES был разработан в 1970-х годах и был стандартом шифрования США в течение долгого времени. Хотя с тех пор он был заменен более сильными алгоритмами, изучение DES позволит лучше понять принципы и методы работы современных шифров.

DES представляет собой блочный алгоритм шифрования, который оперирует блоками данных фиксированного размера (обычно 64 бита). Основная идея DES заключается в использовании модифицированной формы перестановки и замены, известной как шифрование Фейстеля. Рассмотрим шаги DES внимательнее.

1. Генерация ключей:
   – Начинается с исходного ключа длиной 64 бита;
   – применяется операция перестановки и выбора для создания двух 28-битных подключей (субключей) — левого и правого;
   – затем выполняется раундовая функция шифрования, в результате которой создается новый набор подключей. Этот процесс повторяется 16 раз для получения 16 подключей.
2. Шифрование:
   – Исходный блок данных размером 64 бита проходит через начальную перестановку;
   – он разделяется на две половины — левую и правую — каждая по 32 бита;
   – затем последовательно выполняются 16 раундовых операций шифрования, каждая из которых включает в себя сеть Фейстеля;
   – правая половина расширяется до 48 битов и применяется побитовая операция XOR с соответствующим раундовым подключом;
   – результат подается на вход подстановочных блоков (S-блоков), которые заменяют каждый 6-битный блок на 4 бита с использованием заранее определенных таблиц замен;
   – результаты S-блоков объединяются в блок размером 32 бита;
   – этот блок проходит через операцию перестановки и выбора;
   – левая половина обменивается с правой, а правая половина дополняется побитовой операцией XOR с результатом раундовой функции;
   – после завершения всех раундовых операций, левая и правая половины обмениваются местами и проходят через конечную перестановку, в результате которой получается зашифрованный блок данных.
3. Расшифрование. Процесс расшифрования DES аналогичен процессу шифрования, но раундовые подключи используются в обратном порядке. Таким образом, зашифрованный блок

данных пропускается через алгоритм DES, начиная с конечной перестановки и заканчивая начальной перестановкой, чтобы получить исходные данные.

Пример использования DES:

Допустим, у нас есть исходный блок данных размером 64 бита: 01101011 11000101 01010100 11110000 00110011 10100110 11001101 00101100.

Применяя алгоритм DES с выбранным ключом и раундовыми подключами, мы получаем зашифрованный блок данных: 11010110 00110111 01101100 11100111 00101101 01010001 11000101 01011000.

Существуют несколько методов взлома DES, которые были разработаны исследователями и специалистами в области криптографии. Однако стоит отметить, что эти методы взлома были разработаны в контролируемых условиях и предназначены для демонстрации уязвимостей DES, но не для реальных атак.

Одним из наиболее известных методов взлома DES является атака методом полного перебора, которая известна как «атака на основе исчисления времени». В этом методе злоумышленник перебирает все возможные ключи DES (2^56 комбинаций) и для каждого ключа выполняет шифрование входных данных. Затем злоумышленник сравнивает время, необходимое для шифрования, со средним временем шифрования при правильном ключе. Ключ, который приводит к наиболее близкому времени шифрования, считается правильным ключом. Однако, этот метод требует огромных вычислительных ресурсов и времени.

Другой вариант атаки на DES — это дифференциальный криптоанализ. Этот метод основан на изучении различий в выходных данных при изменении входных данных и ключа шифрования. Атакующий сравнивает различия в выходных данных из разных пар входных данных и пытается извлечь информацию о ключе шифрования. Этот метод также требует больших объемов данных и вычислительных ресурсов.

Однако, стоит отметить, что DES, разработанный в 1970-х годах, сейчас считается устаревшим и ненадежным с точки зрения безопасности. В 1999 году DES был официально заменен стандартом AES (Advanced Encryption Standard), который обеспечивает значительно более высокий уровень безопасности [1-4].

Следующий метод является одним из крупнейших алгоритмов шифрования RSA, который применяется на смарт-картах, в защищенных телефонах, на сетевых платах Ethernet, активно используется в криптографическом оборудовании Thales. Данный алгоритм является одним из составов основных протоколов для защищенных коммуникаций Internet, в том числе S/MIME, SSL и S/WAN. Так же он применяется в учреждениях, корпорациях, университетах, правительственных службах, государственных органах и лабораториях [5].

Алгоритм RSA (Rivest-Shamir-Adleman) — это криптографический алгоритм. Он используется для шифрования и подписи данных, основан на математической проблеме факторизации больших чисел. Данный алгоритм обеспечивает высокий уровень безопасности.

1. Генерация ключей:

– Шаг 1: Выбор двух простых чисел p и q, которые должны быть достаточно большими и случайными.

– Шаг 2: Вычисление модуля N, рассчитывается следующим образом: N = p * q.

– Шаг 3: Вычисление функции Эйлера от N (формула 1):

$$\varphi(N) = (p - 1) * (q - 1) \quad (1)$$

– Шаг 4: Выбор открытой экспоненты e. На которое накладывается условие: $e < \varphi(N)$ и взаимно простым с $\varphi(N)$.

– Шаг 5: Вычисление закрытой экспоненты d с помощью расширенного алгоритма Евклида. Закрытая экспонента должна удовлетворять условию $(e * d) \bmod \varphi(N) = 1$.

– Шаг 6: Пара ключей сформирована: открытый ключ (N, e) и закрытый ключ (N, d).

2. Шифрование данных:

– Шаг 1: Преобразование сообщения M в числовое представление m.

– Шаг 2: Шифрование числа m с использованием открытого ключа (N, e). Зашифрованное сообщение вычисляется по формуле 2:

$$c = m^e \cdot mod\ N \quad (2)$$

– Шаг 3: Шифрованный текст c — это зашифрованная версия сообщения M.

3. Дешифрование данных:

– Шаг 1: Расшифрование зашифрованного текста c с использованием закрытого ключа (N, d). Расшифрованное сообщение вычисляется по формуле 3:

$$m = c^d \cdot mod\ N \quad (3)$$

– Шаг 2: Число m преобразуется обратно в исходное сообщение M.

Реализация на языке Python:

```
# Функция для проверки простоты числа
def is_prime(num):
    if num < 2:
        return False
    for i in range(2, int(num**0.5) + 1):
        if num % i == 0:
            return False
    return True
# Функция для вычисления наибольшего общего делителя
def gcd(a, b):
    while b:
        a, b = b, a % b
    return a
# Функция для вычисления расширенного алгоритма Евклида
def extended_gcd(a, b):
    if b == 0:
        return a, 1, 0
    gcd, x, y = extended_gcd(b, a % b)
    return gcd, y, x - (a // b) * y
# Функция для генерации ключей RSA
def generate_rsa_keys():
    p = 17
    q = 11
    N = p * q
    phi = (p - 1) * (q - 1)
    e = 7

    # Проверка, что e и phi взаимно просты
    if gcd(e, phi) != 1:
        raise ValueError("Ошибка: e и phi не взаимно просты.")
    _, d, _ = extended_gcd(e, phi)
    # Положительное значение d
    d = d % phi
    public_key = (N, e)
    private_key = (N, d)
    return public_key, private_key
# Функция для шифрования сообщения с помощью открытого ключа
def encrypt(message, public_key):
    N, e = public_key
    ciphertext = pow(message, e, N)
    return ciphertext
# Функция для расшифрования сообщения с помощью закрытого ключа
```

```
        def decrypt(ciphertext, private_key):
            N, d = private_key
            message = pow(ciphertext, d, N)
            return message
        # Пример использования
        message = 721782079
        public_key, private_key = generate_rsa_keys()
        encrypted_message = encrypt(message, public_key)
        decrypted_message = decrypt(encrypted_message, private_key)
        print("Открытый ключ:", public_key)
        print("Закрытый ключ:", private_key)
        print("Зашифрованное сообщение:", encrypted_message)
print("Расшифрованное сообщение:", decrypted_message)
```

Данный пример является базовой реализацией алгоритма RSA, который предназначен для понимания работы алгоритма и не обладает высокой производительностью и степенью защиты. Для улучшения алгоритма используются библиотеки такие как, cryptography или pycryptodome, которые обеспечивают больший функционал.

Учёные считали, что для взлома данного алгоритма потребуется квантовый компьютер с вычислительной мощностью в сотни тысяч кубитов, который появится минимум через 10 лет. В начале 2023 года эксперты из Китая опубликовали статью «Factoring integers with sublinear resources on a superconducting quantum processor» [9], где описали методику взлома RSA-48 при помощи квантового компьютера мощностью 372 кубита, что ставит под сомнение безопасность интернета, банков и других сфер, где используется RSA. В настоящее время существует квантовый компьютер мощностью в 433 кубита и компания IBM обещала уже в этом году сделать доступным для клиентов данный сверхмощный компьютер, что насторожило ИБ-специалистов, ведь RSA попросту не устоит. Способ взлома довольно прост, ученые использовали методику Клауса-Питера Шнорра и оптимизировали алгоритм таким образом, что для дешифровки ключа RSA длиной 48 бит хватило 10-кубитного компьютера. Также учёные рассказали, что по их методике для взлома 2048-битного ключа понадобится всего 372 кубита, а не сотни тысяч, как предполагалось ранее [6, 7, 8]. Чтобы предотвратить возможность данной атаки, необходимо воспользоваться тем же средством, квантовым компьютером и использовать более длинные ключи, основанные на квантовой криптографии, или же другие алгоритмы.

Третьим рассматриваемым алгоритмом шифрования будет AES, данный шифр в настоящее время не был взломан. AES является симметричным блочным алгоритмом шифрования, выбранным в качестве стандарта правительством США. AES обладает высокой стойкостью и безопасностью, и широко применяется в различных приложениях и протоколах. Он поддерживает ключи длиной 128, 192 и 256 битов, что обеспечивает большую стойкость. AES остается крепким и безопасным алгоритмом шифрования на сегодняшний день.

Основные этапы алгоритма AES:

1. Инициализация ключа: вначале определяется ключ шифрования. Длина ключа может быть 128 бит, 192 бита или 256 бит, в зависимости от необходимого уровня безопасности.

2. Добавление паддинга: если длина данных не кратна размеру блока (128 бит), то выполняется добавление паддинга до нужной длины.

3. Шифрование раундами: алгоритм AES состоит из нескольких раундов шифрования, которые применяются последовательно к данным.

– К каждому блоку данных применяется операция подстановки байтов (SubBytes), заменяющая каждый байт на соответствующий байт из заранее заданной таблицы подстановки (S-Box).

– Затем происходит сдвиг строк (ShiftRows), при котором байты в каждой строке блока сдвигаются циклически влево на определенное количество позиций.

– Происходит перемешивание столбцов (MixColumns), при котором каждый столбец блока умножается на определенную матрицу, что вносит нелинейность в шифрование.

– В конце каждого раунда применяется операция добавления ключа (AddRoundKey), при которой блок данных побитово складывается с соответствующим раундовым ключом.

4. Финальный раунд: последний раунд отличается от предыдущих тем, что он не выполняет операцию перемешивания столбцов (MixColumns).

5. Результат: после завершения всех раундов, полученные данные являются зашифрованным сообщением.

Пример реализации алгоритма на Python:

```
        from Crypto.Cipher import AES
        from Crypto.Random import get_random_bytes
        # Генерация случайного 128-битного ключа
        key = get_random_bytes(16)
        # Инициализация шифратора AES с выбранным ключом
        cipher = AES.new(key, AES.MODE_ECB)
        # Зашифрование сообщения
        message = b"Hello, AES!"
        ciphertext = cipher.encrypt(message)
        # Дешифрование зашифрованного сообщения
        decipher = AES.new(key, AES.MODE_ECB)
        decrypted_message = decipher.decrypt(ciphertext)
        print("Зашифрованное сообщение:", ciphertext)
print("Дешифрованное сообщение:", decrypted_message)
```

В этом примере используется режим шифрования ECB (Electronic Codebook), который применяет шифратор к каждому блоку данных в отдельности. Однако, для повышения безопасности обычно рекомендуется использовать режимы, такие как CBC (Cipher Block Chaining), который добавляет вектор инициализации для каждого блока данных. Данный пример является базовым примером работы алгоритма, для его улучшения необходимо использовать те же библиотеки, что и для прошлого алгоритма RSA [10 - 13].

Режимы шифрования ECB (Electronic Codebook) и CBC (Cipher Block Chaining) являются двумя различными методами использования алгоритмов блочного шифрования, таких как AES. Они отличаются в том, как они обрабатывают и шифруют блоки данных, и имеют свои особенности и преимущества.

1. Режим шифрования ECB:

В режиме ECB каждый блок данных одинакового размера шифруется независимо друг от друга.

Каждый блок данных передается в шифратор, который независимо применяет операции шифрования к каждому блоку.

Простой пример: представим, что у нас есть изображение, и мы применяем ECB для его шифрования. Каждый блок пикселей (обычно 8x8 или 16x16) будет обрабатываться независимо от других блоков.

2. Режим шифрования CBC:

В режиме CBC каждый блок данных перед шифрованием комбинируется с предыдущим зашифрованным блоком данных.

Используется дополнительный начальный вектор инициализации (IV), который служит для инициализации первого блока шифрования.

Каждый следующий блок данных перед шифрованием проходит операцию XOR с предыдущим зашифрованным блоком данных.

Простой пример: предположим, что у нас есть текстовое сообщение, разделенное на блоки. Первый блок передается в шифратор, а затем каждый следующий блок передается через операцию XOR с предыдущим зашифрованным блоком.

В отличие от ECB, где каждый блок данных обрабатывается независимо, CBC включает предыдущий зашифрованный блок данных в процесс шифрования следующего блока. Это делает

режим CBC более безопасным, поскольку вносит дополнительные изменения в шифрованные данные, усложняя обнаружение и анализ повторяющихся паттернов. Однако он более чувствителен к ошибкам передачи данных, поскольку изменение одного бита повлияет на расшифровку остальных блоков [14, 15].

На сегодняшний день AES (Advanced Encryption Standard) считается крайне надежным алгоритмом шифрования. Он широко применяется и рекомендован для использования правительством США и другими организациями по всему миру.

На данный момент нет известных методов взлома AES с использованием общедоступных вычислительных ресурсов. Он протестирован и подвергался компьютерным атакам на протяжении многих лет, и до сих пор не было документированных случаев успешного взлома. Такие атаки на AES требуют огромные вычислительные мощности и времени, что делает их практически невозможными для большинства злоумышленников. Конечно, в течение времени могут появиться новые методы или уязвимости, которые могут повлиять на безопасность AES. Поэтому постоянное исследование и анализ алгоритмов шифрования, включая AES, является важной задачей для обеспечения безопасности информации.

ЗАКЛЮЧЕНИЕ

Таким образом, в статье были рассмотрены шифры DES, RSA и AES, оценены их стойкость, безопасность и популярность. Шифр DES, несмотря на свою историческую значимость, потерял актуальность из-за ограничений в длине ключа и слабостей алгоритма. RSA, в свою очередь, является асимметричным алгоритмом, широко используемым для шифрования и подписи, но уязвим к будущим атакам с использованием квантовых компьютеров.

С другой стороны, AES продолжает оставаться самым лучшим алгоритмом шифрования в настоящее время. Он обладает высокой стойкостью, безопасностью и применяется во множестве приложений и протоколов, поддерживает различные длины ключей, что позволяет выбирать уровень безопасности в зависимости от потребностей.

На основании обзора этих алгоритмов, можно сделать вывод, что AES является наиболее предпочтительным выбором для надежного шифрования данных. Он обеспечивает современные стандарты безопасности и безопасное применение в широком спектре сценариев.

Важно отметить, что безопасность шифрования также зависит от правильной реализации, корректного использования криптографических протоколов и хранения ключей секретными. Регулярное обновление системы и следование рекомендациям по безопасности являются также важными факторами для обеспечения надежного шифрования данных [16, 17].

Список литературы

1. Стандарт шифрования данных (DES) [Электронный ресурс]. URL: https://intuit.ru/studies/courses/552/408/lecture/9362?page=3
2. Алгоритм шифрования DES [Электронный ресурс]. URL: https://studme.org/239561/informatika/algoritm_shifrovaniya
3. Создание подключей в алгоритме des [Электронный ресурс]. URL: https://studfile.net/preview/2204125/page:4/
4. Стандарт шифрования данных Data Encryption Standard [Электронный ресурс]. URL: https://protect.htmlweb.ru/des.htm
5. Использование криптосистемы RSA в настоящее время [Электронный ресурс]. URL: https://studfile.net/preview/299352/page:6/
6. Китайские программисты взломали алгоритм RSA. Это угрожает всему интернету [Электронный ресурс]. URL: https://4pda.to/2023/01/08/408266/kitajskie_programmisty_vzlomali_algoritm_rsa_eto_ugrozhaet_vsemu_internetu/
7. Эксперты из Китая взломали RSA-шифрование с помощью квантовых компьютеров [Электронный ресурс]. URL: https://www.anti-malware.ru/news/2023-01-06-1447/40255

8. Китайские исследователи заявили об успешном взломе шифрования RSA [Электронный ресурс]. URL: https://cryptonews.net/ru/news/blockchain/18936323/
9. Factoring integers with sublinear resources on a superconducting quantum processor [Электронный ресурс]. URL: https://arxiv.org/pdf/2212.12372.pdf
10. Как работает AES (Advanced Encryption Standard) [Электронный ресурс]. URL: https://vc.ru/dev/656195-kak-rabotaet-aes-advanced-encryption-standard-obyasnenie-dlya-gumanitariev-tipa-menya
11. Объяснение шифрования AES [Электронный ресурс]. URL: https://blog.kraden.com/ru/aes-256-encryption
12. Advanced Encryption Standard (AES) [Электронный ресурс]. URL: https://www.geeksforgeeks.org/advanced-encryption-standard-aes/
13. What is the Advanced Encryption Standard (AES)? [Электронный ресурс]. URL: https://www.zenarmor.com/docs/network-security-tutorials/what-is-advanced-encryption-standard-aes
14. Несколько режимов работы шифрования AES [Электронный ресурс]. URL: https://russianblogs.com/article/2418837814/
15. How to choose an AES encryption mode (CBC ECB CTR OCB CFB)? [Электронный ресурс]. URL: https://stackoverflow.com/questions/1220751/how-to-choose-an-aes-encryption-mode-cbc-ecb-ctr-ocb-cfb
16. Костиков В.А. Необходимость сжатия зашифрованных данных с помощью алгоритмов кодирования LZW и Хаффмана / В.А. Костиков, М.А. Маслова // Теория и практика проектного образования. – 2021. – № 3(19). – С. 62-64.
17. Реализация ESG-принципов в стратегии устойчивого развития экономики России / Н.Г. Вовченко, Н.Г. Кузнецов, Е.Н. Макаренко [и др.]. – Ростов-на-Дону: Ростовский государственный экономический университет "РИНХ", 2022. – 508 с.

References

1. Data Encryption Standard (DES) [Electronic resource]. URL: https://intuit.ru/studies/courses/552/408/lecture/9362?page=3
2. DES encryption algorithm [Electronic resource]. URL: https://studme.org/239561/informatika/algoritm_shifrovaniya
3. Creation of a plug-in in the des algorithm [Electronic resource]. URL: https://studfile.net/preview/2204125/page:4/
4. Data Encryption Standard Data Encryption Standard [Electronic resource]. URL: https://protect.htmlweb.ru/des.htm
5. The use of the RSA cryptosystem at the present time [Electronic resource]. URL: https://studfile.net/preview/299352/page:6/
6. Chinese programmers hacked the RSA algorithm. This threatens the entire Internet [Electronic resource]. URL: https://4pda.to/2023/01/08/408266/kitajskie_programmisty_vzlomali_algoritm_rsa_eto_ugrozhaet_vsemu_internetu/
7. Experts from China cracked RSA encryption using quantum computers [Electronic resource]. URL: https://www.anti-malware.ru/news/2023-01-06-1447/40255
8. Chinese researchers have announced the successful cracking of RSA encryption [Electronic resource]. URL: https://cryptonews.net/ru/news/blockchain/18936323/
9. Factoring integers with sublinear resources on a superconducting quantum processor [Electronic resource]. URL: https://arxiv.org/pdf/2212.12372.pdf
10. How AES (Advanced Encryption Standard) works [Electronic resource]. URL: https://vc.ru/dev/656195-kak-rabotaet-aes-advanced-encryption-standard-obyasnenie-dlya-gumanitariev-tipa-menya
11. Explanation of AES encryption [Electronic resource]. URL: https://blog.kraden.com/ru/aes-256-encryption
12. Advanced Encryption Standard (AES) [Electronic resource]. URL: https://www.geeksforgeeks.org/advanced-encryption-standard-aes/
13. What is the Advanced Encryption Standard (AES)? [Electronic resource]. URL: https://www.zenarmor.com/docs/network-security-tutorials/what-is-advanced-encryption-standard-aes
14. Multiple AES encryption modes [Electronic resource]. URL: https://russianblogs.com/article/2418837814/

15. How to choose an AES encryption mode (CBC ECB CTR OCB CFB)? [Electronic resource]. URL: https://stackoverflow.com/questions/1220751/how-to-choose-an-aes-encryption-mode-cbc-ecb-ctr-ocb-cfb

16. Kostikov V.A. The need to compress encrypted data using LZW and Huffman coding algorithms / V.A. Kostikov, M.A. Maslova // Theory and practice of project education. – 2021. – No. 3(19). – pp. 62-64.

17. Implementation of ESG principles in the strategy for sustainable development of the Russian economy / N.G. Vovchenko, N.G. Kuznetsov, E.N. Makarenko [at al.]. – Rostov-on-Don: Rostov State Economic University "RINH", 2022. – 508 p.

Кузьминых Егор Сергеевич, студент четвертого курса кафедры «Информационная безопасность»
Ильина София Павловна, студент четвертого курса кафедры «Информационная безопасность»
Маслова Мария Александровна, доцент кафедры «Информационная безопасность»

Kuzminykh Egor Sergeevich, 4th year student of the Department of Information Security
Ilina Sofia Pavlovna, 4th year student of the Department of Information Security
Maslova Maria Aleksandrovna, Associate Professor of the Department of Information Security

УДК 004 **DOI: 10.18413/2518-1092-2024-9-1-0-3**

Федоров А.В.[1]
Жихарев А.Г.[2]
Кальченко Д.М.[1]

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ. ПРОБЛЕМЫ И РЕШЕНИЯ

[1)] Белгородский университет кооперации, экономики и права,
ул. Садовая, 116а, г. Белгород, 308023, Россия
[2)] Белгородский государственный технологический университет им. В.Г. Шухова,
ул. Костюкова, 46, Белгород, 308012, Россия

e-mail: zhikharev@bsu.edu.ru

Аннотация
В статье рассмотрены основные проблемы и соответственно принимаемые меры безопасности органов исполнительной власти, в которых определены цели и задачи, оценка рисков. Рассмотрены основные принципы выбора и внедрении защитных мер, разработки процедур и политик информационной безопасности, предложены основные отечественные системы управления информационной безопасностью, также описаны основные формы обучения сотрудников, мониторинга и принимаемых действий на основе анализа результатов мониторинга. Определены этапы анализа инцидентов в процессе расследования инцидентов, которые позволяют выявить уязвимости и проблемы в системе безопасности и принять меры по их устранению. Обусловлено регулярное обновление и совершенствование системы безопасности обеспечением более надежной защиты от различных видов угроз, приведено несколько рекомендаций для пересмотра и адаптации политик информационной безопасности с целью адаптация к изменяющимся условиям и требованиям. Приведены причины целесообразности внедрение систем управления информационной безопасности.
Ключевые слова: проблемы информационной безопасности; меры обеспечения; оценка рисков; защитные меры; системы управления информационной безопасности; мониторинг и анализ результатов; расследования инцидентов; уязвимости и проблемы; пересмотр и адаптация политик информационной безопасности; целесообразность внедрения систем управления информационной безопасности
Для цитирования: Федоров А.В., Жихарев А.Г., Кальченко Д.М. Обеспечение информационной безопасности в органах исполнительной власти. Проблемы и решения // Научный результат. Информационные технологии. – Т.9, №1, 2024. С. 19-28. DOI: 10.18413/2518-1092-2024-9-1-0-3

Fedorov A.V. [1]
Zhikharev A.G.[2]
Kalchenko D.M.[1]

ENSURING INFORMATION SECURITY IN EXECUTIVE AUTHORITIES. PROBLEMS AND SOLUTIONS

[1)] Belgorod University of Cooperation, Economics and Law,
116a Sadovaya str., Belgorod, 308023, Russia
[2)] Belgorod State Technological University named after V.G. Shukhov,
46 Kostyukova str., Belgorod, 308012, Russia

e-mail: zhikharev@bsu.edu.ru

Abstract
The article discusses the main problems and, accordingly, the security measures taken by executive authorities, which define goals and objectives, risk assessment. The basic principles of the choice and implementation of protective measures, the development of information security procedures and policies are considered, the main domestic information security management systems are proposed, the main forms of employee training, monitoring and actions taken based on the analysis of monitoring results are also described. The stages of incident analysis in the process of incident investigation are defined, which allow identifying vulnerabilities and problems in the security

system and taking measures to eliminate them. The regular updating and improvement of the security system is due to the provision of more reliable protection against various types of threats, several recommendations are given for the revision and adaptation of information security policies in order to adapt to changing conditions and requirements. The reasons for the expediency of implementing information security management systems are given.
Keywords: information security problems; security measures; risk assessment; protective measures; information security management systems; monitoring and analysis of results; investigation of incidents; vulnerabilities and problems; revision and adaptation of information security policies; the feasibility of implementing information security management systems
For citation: Fedorov A.V., Zhikharev A.G., Kalchenko D.M. Ensuring information security in executive authorities. Problems and solutions // Research result. Information technologies. – T.9, №1, 2024. – P. 19-28. DOI: 10.18413/2518-1092-2024-9-1-0-3

ВВЕДЕНИЕ

Обеспечение информационной безопасности (ИБ) является одним из ключевых аспектов современного мира, так как информация играет огромную роль в повседневной жизни людей, а также в деятельности предприятий и организаций. В условиях цифровой трансформации и активного использования информационных технологий, информационная безопасность становится особенно актуальной.

Проблемы ИБ связаны с угрозами нарушения конфиденциальности, целостности и доступности информации. Эти угрозы могут быть вызваны различными факторами, включая хакерские атаки, вирусы, фишинг, сбои в работе оборудования и программного обеспечения, а также человеческий фактор.

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение ИБ в органах исполнительной власти является одной из ключевых задач, так как от этого зависит конфиденциальность, целостность и доступность данных, а также защита от внутренних и внешних угроз. Однако, несмотря на все усилия и внедрение современных технологий, проблемы в области ИБ все еще остаются актуальными.

Проблемы ИБ можно разделить на несколько основных категорий:

- Недостаток квалифицированных специалистов: Проблема нехватки специалистов в области обеспечения ИБ актуальна для многих стран. Это связано с тем, что подготовка специалистов требует значительных временных и финансовых затрат, а также постоянного обновления знаний и навыков.
- Недостаточное финансирование: Недостаток средств на обеспечение ИБ может привести к тому, что меры по защите информации будут недостаточными или устаревшими. Это может привести к утечке конфиденциальной информации, нарушению работы информационных систем и другим негативным последствиям.
- Отсутствие единой стратегии: В разных органах исполнительной власти могут быть разные подходы к обеспечению ИБ, что может привести к несогласованности действий и снижению общего уровня защиты информации.
- Угрозы со стороны внешних источников: К ним относятся хакеры, киберпреступники и другие злоумышленники, которые могут использовать различные методы для получения доступа к конфиденциальной информации.

Одной из основных проблем, с которой сталкиваются органы исполнительной власти, является уязвимость информационных систем. Злоумышленники могут использовать различные методы, чтобы получить доступ к конфиденциальной информации. Это может привести к серьезным последствиям, таким как утечка данных, нарушение работы информационных систем и даже экономический ущерб.

МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для решения этой проблемы необходимо применять комплексные меры по обеспечению ИБ. Это включает в себя использование надежных методов шифрования данных, регулярное обновление программного обеспечения и операционных систем, а также обучение сотрудников правилам работы с конфиденциальной информацией.

К комплексным мерам по обеспечению ИБ относятся:

1. Определение целей и задач ИБ: На этом этапе разрабатывается стратегия по обеспечению ИБ. Определяются основные цели и задачи, такие как защита конфиденциальной информации, обеспечение доступности и целостности данных, предотвращение кибератак и т.д.

Обеспечение ИБ является одним из ключевых аспектов работы любой организации. Для эффективного управления рисками и обеспечения безопасности информации необходимо определить цели и задачи ИБ.

Цели информационной безопасности:

- Защита конфиденциальности: Обеспечение того, чтобы информация была доступна только авторизованным пользователям и не раскрывалась без разрешения.
- Защита целостности: Обеспечение точности, полноты и правильности информации, а также предотвращение ее несанкционированного изменения или уничтожения.
- Защита доступности: Обеспечение своевременного доступа к необходимой информации для авторизованных пользователей.
- Задачи информационной безопасности:
- Разработка и внедрение политики ИБ, которая устанавливает основные принципы и требования к обеспечению безопасности.
- Создание и поддержание системы управления ИБ (СУИБ), включая определение ролей и обязанностей, а также контроль за соблюдением политик ИБ.
- Внедрение мер и процедур для защиты информации от различных угроз, таких как вирусы, хакерские атаки, фишинг и т.д.
- Обучение и информирование сотрудников о мерах безопасности и их ответственности в области ИБ.
- Мониторинг и анализ системы ИБ с целью выявления уязвимостей и принятия мер по их устранению.
- Внедрение механизмов восстановления после инцидентов ИБ для минимизации их последствий.
- Взаимодействие с внешними организациями, такими как регуляторы, поставщики услуг и правоохранительные органы, по вопросам ИБ.
- Постоянное совершенствование системы ИБ и адаптация ее к изменяющимся условиям и угрозам.

2. Оценка рисков: Проводится анализ возможных угроз и уязвимостей, а также оценка рисков для информационных систем. Это помогает определить приоритетность мер безопасности и спланировать ресурсы для их реализации.

Оценка рисков включает в себя следующие этапы:

- Идентификация угроз: Определение возможных угроз для информационной системы, таких как хакерские атаки, вирусы, ошибки персонала и т. д.
- Оценка уязвимостей: Выявление слабых мест в системе, которые могут быть использованы угрозами для нарушения безопасности.
- Анализ рисков: Расчет вероятности реализации угроз и оценка возможных последствий для информационной системы.
- Выбор мер защиты: Определение оптимальных мер и средств защиты информации, направленных на минимизацию рисков.

• Мониторинг и аудит: Контроль за соблюдением мер защиты и анализ эффективности выбранных методов.

Оценка рисков может проводиться как на регулярной основе, так и при возникновении новых угроз или изменении условий работы информационной системы. Важно учитывать, что риски не являются статичными и могут изменяться в зависимости от внешних факторов и действий злоумышленников. Поэтому регулярная оценка и анализ рисков являются неотъемлемой частью обеспечения безопасности информационных систем.

3. **Выбор и внедрение защитных мер:** На основе проведенного анализа рисков выбираются соответствующие меры безопасности. Защитные меры могут включать в себя технические средства защиты, такие как антивирусное программное обеспечение, межсетевые экраны, системы обнаружения вторжений и т.д., а также организационные меры, такие как обучение персонала, контроль доступа к информации, регламентация работы с конфиденциальной информацией и т.п.

При выборе защитных мер необходимо учитывать множество факторов, таких как тип информационной системы, характер обрабатываемой информации, уровень угроз и уязвимостей, а также финансовые и технические возможности организации. Важно также обеспечить своевременное обновление и поддержку используемых защитных мер, чтобы они оставались эффективными и соответствующими современным угрозам.

Внедрение защитных мер должно осуществляться в соответствии с разработанной стратегией информационной безопасности, учетом требований законодательства и регуляторов. Необходимо также контролировать эффективность внедренных мер и при необходимости проводить их адаптацию и модернизацию.

В целом, выбор и внедрение защитных мер требует комплексного, профессионального подхода, чтобы обеспечить надежную защиту информации и минимизировать возможные риски для организации.

4. **Разработка процедур и политик ИБ:** Разрабатываются и документируются процедуры и политики, которые определяют порядок действий в случае инцидентов ИБ, правила работы с конфиденциальными данными, порядок реагирования на кибератаки и другие вопросы.

Процедуры ИБ могут включать в себя инструкции по работе с конфиденциальной информацией, правила использования информационных систем, процедуры реагирования на инциденты безопасности и т.д. Политики ИБ, в свою очередь, устанавливают общие принципы и направления деятельности организации в области информационной безопасности.

Разработка процедур и политик ИБ должна осуществляться с учетом специфики деятельности организации, ее информационных систем и существующих угроз. Важно также регулярно обновлять и актуализировать эти документы, чтобы они соответствовали текущим требованиям и стандартам безопасности.

Кроме того, процедуры и политики ИБ должны быть доступны для всех сотрудников организации и обязательны для исполнения. Это позволит обеспечить единый подход к обеспечению ИБ и снизить вероятность возникновения инцидентов.

5. **Внедрение системы управления ИБ:**

Существует несколько отечественных СУИБ, которые могут быть использованы в разных организациях в зависимости от их потребностей и специфики. Вот некоторые из них:

• АСТРА LINUX SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) – система, которая является частью операционной системы AstraLinux и обеспечивает мониторинг, сбор и анализ событий безопасности, а также обнаружение и предотвращение вторжений.“

• “DallasLock” – еще одна популярная российская СУИБ. Она обеспечивает защиту конфиденциальной информации и персональных данных, а также контроль доступа к информационным системам.

• “SecretNet” – программный комплекс для защиты информации от несанкционированного доступа, который включает в себя средства идентификации и аутентификации пользователей, шифрования данных и контроля целостности.

- "ЕЦУDallasLock" – современное сертифицированное на соответствие требованиям безопасности информации ФСТЭК России решение, которое находится в Едином реестре российских программ для ЭВМ и БД (№11185 от 29.07.2021 г.). Позволяет управлять не только различными СЗИ DallasLock, но также АРМами и серверами СЗИ DallasLock через Агента ЕЦУ для ОС Windows и Linux, позволяет контролировать сетевое оборудование, обеспечивает безопасный доступ к удаленному АРМ за пределами периметра организации. Лицензируется по количеству контролируемых АРМ и количеству сетевых устройств.
- "СЗИ DallasLockLinux" – специальная версия системы "DallasLock", предназначенная для защиты конфиденциальной информации в Linux-системах. (с 01.11.2023 г. прекращены продажи СБ DallasLock 8.0-С и 8.0-К – необходимо заменить на ЕЦУ DallasLock).
- "ParsecNet" – система контроля и управления доступом, которая обеспечивает безопасное удаленное подключение к корпоративным ресурсам.
- "SolarinRights" – решение для управления правами доступа к информационным ресурсам, позволяющее контролировать доступ к файлам, папкам, приложениям и другим объектам.
- "ZecurionDLP" – комплексная DLP-система последнего поколения. Защищает информацию от утечки по локальным и сетевым каналам, выявляет случаи корпоративного мошенничества, помогает расследовать инциденты и оценивать риски информационной безопасности.
- "InfoWatchTrafficMonitor" – программа для анализа и контроля информационных потоков в компании, выявления нарушений и инцидентов ИБ.
- "КриптоПроCSP, JCP, NETи т.д." – средства криптографической защиты информации.

Выбор СУИБ зависит от потребностей и возможностей конкретной организации. Некоторые из этих продуктов могут быть интегрированы друг с другом для обеспечения более комплексной защиты информации.

6. **Обучение и информирование сотрудников:** Сотрудники информируются о новых мерах безопасности и обучаются необходимым навыкам для работы с ними.

Обучение и информирование сотрудников является одним из ключевых аспектов управления персоналом. Оно способствует развитию профессиональных навыков, повышению квалификации, а также позволяет сотрудникам лучше понять цели и задачи компании, что в свою очередь положительно влияет на их мотивацию и лояльность.

Основные формы обучения сотрудников:

- Внутреннее обучение: включает проведение тренингов, семинаров, мастер-классов и других обучающих мероприятий внутри компании. Часто это наиболее экономичный вариант, так как не требует дополнительных затрат на внешние ресурсы.
- Внешнее обучение: предполагает привлечение внешних специалистов или организаций для проведения обучающих программ. Это может быть более дорогостоящим вариантом, но позволяет получить доступ к новым знаниям и технологиям.
- Онлайн-обучение: использование онлайн-платформ для дистанционного обучения, что позволяет сотрудникам обучаться в удобное для них время и месте.
- Наставничество: передача знаний и опыта от более опытных сотрудников к менее опытным, что помогает новичкам быстрее адаптироваться и развиваться в компании.

Информирование сотрудников включает в себя различные способы донесения информации до сотрудников. Это могут быть корпоративные рассылки, доски объявлений, встречи и совещания, а также корпоративная газета или журнал.

7. **Мониторинг и анализ системы безопасности**: Осуществляется постоянный мониторинг и анализ информационных систем на предмет потенциальных угроз и уязвимостей. Результаты мониторинга используются для корректировки и совершенствования системы ИБ.

Мониторинг и анализ систем безопасности является важной частью процесса обеспечения информационной безопасности предприятия. Это включает в себя наблюдение и сбор данных о состоянии безопасности информационных систем, сетей и оборудования, а также анализ этой информации для выявления потенциальных угроз и уязвимостей.

Мониторинг системы безопасности включает в себя:

- Обнаружение и предотвращение вторжений (IDS/IPS) – системы, которые отслеживают и анализируют сетевой трафик на предмет подозрительной активности.
- Системы обнаружения уязвимостей (VDMS) - программное обеспечение, которое сканирует системы на наличие известных уязвимостей и предоставляет отчеты об их состоянии.
- Системы мониторинга событий безопасности (SIEM) – инструменты, которые собирают, коррелируют и анализируют события безопасности из различных источников данных для выявления аномалий.
- Системы управления обновлениями (PatchManagement) – автоматизированные инструменты, которые следят за обновлениями и исправлениями для операционных систем и приложений, уведомляя пользователей о доступных обновлениях и помогая их применять.
- Системы анализа сетевого трафика – программное обеспечение для мониторинга сетевого трафика с целью выявления подозрительной активности или проблем.

Анализ данных мониторинга системы безопасности может включать такие действия, как:

- Идентификация и классификация угроз – выявление потенциальных угроз для информационных систем и определение их уровня риска.
- Определение уязвимостей - анализ данных мониторинга для обнаружения уязвимостей в системах и сетях, которые могут быть использованы злоумышленниками.
- Выработка рекомендаций по улучшению безопасности – на основе анализа данных мониторинга, предоставление рекомендаций по устранению уязвимостей, улучшению процессов безопасности и принятию превентивных мер.
- Управление инцидентами безопасности – обработка и реагирование на инциденты безопасности, включая сбор доказательств, расследование и восстановление после инцидентов.
- Анализ трендов и метрик – использование данных мониторинга для анализа тенденций и метрик, связанных с безопасностью, чтобы определить, какие области требуют улучшения или корректировок.
- Обучение и осведомленность – использование данных мониторинга и анализа для обучения сотрудников и повышения осведомленности о проблемах безопасности.

В целом, мониторинг и анализ системы безопасности является важным процессом, который помогает организациям обнаруживать и предотвращать угрозы, устранять уязвимости и улучшать общую информационную безопасность.

8. Расследование инцидентов ИБ: В случае возникновения инцидентов, проводится расследование для определения причин и принятия мер по их устранению.

В ходе расследования анализируются различные факторы, такие как действия злоумышленников, уязвимости в системе безопасности, ошибки персонала и другие факторы, которые могут привести к инцидентам.

Процесс расследования инцидентов включает в себя следующие этапы:

- Регистрация и классификация инцидентов: На этом этапе необходимо зарегистрировать все инциденты, связанные с информационной безопасностью, и классифицировать их по степени серьезности. Это поможет определить приоритеты и спланировать дальнейшие действия.
- Сбор и анализ информации: После регистрации инцидента необходимо собрать всю доступную информацию о нем, включая данные о злоумышленниках, используемых ими инструментах, методах атаки и других факторах. Анализ этой информации поможет выявить причины инцидента и определить меры, которые необходимо принять для его устранения.
- Определение причин инцидента: На основе собранной информации необходимо определить причины инцидента, включая уязвимости в системах безопасности, ошибки персонала или неправильные настройки. Это позволит принять меры для предотвращения подобных инцидентов в будущем.
- Разработка и реализация мер по устранению причин инцидента: После определения причин инцидента необходимо разработать и реализовать меры по их устранению. Эти меры могут

включать обновление программного обеспечения, изменение настроек системы, обучение персонала и другие действия.

- Мониторинг и контроль: После реализации мер по устранению причин инцидентов необходимо осуществлять мониторинг и контроль за их эффективностью. Это может включать в себя анализ логов системы безопасности, проведение регулярных аудитов и тестов на проникновение, а также оценку эффективности обучения персонала.
- Отчетность и информирование: По результатам расследования инцидентов необходимо подготовить отчет, в котором будут представлены все полученные данные, выводы и рекомендации. Этот отчет должен быть представлен руководству и другим заинтересованным сторонам, а также использован для информирования персонала о выявленных проблемах и мерах по их устранению.

Расследование инцидентов ИБ является важным компонентом системы обеспечения ИБ организации. Оно позволяет выявить уязвимости и проблемы в системе безопасности и принять меры по их устранению, что в свою очередь снижает вероятность возникновения подобных инцидентов в будущем.

9. Регулярное обновление и совершенствование системы безопасности: Система ИБ постоянно совершенствуется и обновляется с учетом новых угроз и технологических изменений. Может включать следующие пункты:

- Анализ уязвимостей: Регулярный анализ уязвимостей позволяет выявить слабые места в системе безопасности и принять меры по их устранению.
- Обновление программного обеспечения: Важно регулярно обновлять программное обеспечение, так как это снижает риск использования злоумышленниками уязвимостей.
- Обучение персонала: Сотрудники должны быть обучены работе с системами безопасности и знать, как правильно реагировать на различные угрозы.
- Внедрение новых технологий: Постоянное внедрение новых технологий может помочь улучшить систему безопасности и сделать ее более эффективной.
- Мониторинг и контроль: Системы мониторинга и контроля должны быть настроены для отслеживания активности пользователей и предотвращения возможных угроз.
- Установка антивирусного ПО: Установка антивирусного программного обеспечения и регулярное обновление его баз данных поможет защитить систему от вредоносных программ.
- Физическая безопасность: Обеспечение физической безопасности, например, установка систем видеонаблюдения, замков и охранных систем, поможет предотвратить несанкционированный доступ к системе.
- Разработка политик безопасности: Разработка и внедрение политик безопасности для всех пользователей системы поможет обеспечить соблюдение стандартов безопасности.
- Оценка рисков: Регулярная оценка рисков поможет определить наиболее уязвимые места и разработать стратегии для их устранения.
- Обратная связь: Получение обратной связи от пользователей и сотрудников позволит улучшить систему безопасности, учитывая их потребности и ожидания.

Регулярное обновление и совершенствование системы безопасности требует постоянных усилий и внимания, но в результате обеспечивает более надежную защиту от различных видов киберугроз и несанкционированного доступа к информации.

10. Пересмотр и адаптация политики ИБ: Периодически проводится анализ политики ИБ и ее адаптация к изменяющимся условиям и требованиям. Вот несколько рекомендаций для пересмотра и адаптации политик ИБ:

- **Регулярно проводите анализ рисков:** Оцените текущие угрозы и уязвимости в вашей организации, чтобы определить, какие изменения в политике ИБ необходимы.
- **Обучайте сотрудников:** Обучите всех сотрудников основам информационной безопасности, чтобы они знали, как правильно обращаться с конфиденциальной информацией и как реагировать на инциденты безопасности.

- **Внедрите новые технологии:** Постоянно следите за новыми технологиями и решениями в области ИБ, чтобы внедрять их в свою организацию.
- **Установите системы мониторинга и контроля:** Используйте системы мониторинга и контроля для отслеживания действий пользователей и обнаружения подозрительной активности.
- **Обновляйте программное обеспечение:** Регулярно обновляйте программное обеспечение на своих устройствах, чтобы устранить уязвимости и предотвратить атаки.
- **Обеспечьте физическую безопасность:** Обеспечьте надежную физическую безопасность, такую как установка систем видеонаблюдения и контроля доступа, чтобы предотвратить несанкционированный доступ в здание.
- **Разработайте политику паролей:** Разработайте и внедрите политику надежных паролей, чтобы предотвратить взлом учетных записей пользователей.

Проектируемая СУИБ должна соответствовать международным и отечественным стандартам ISO/IEC 27001:2022, ISO/IEC 27002:2022, NIST SP 800-53Rev.5, ГОСТ Р ИСО/МЭК 27001-2021, ГОСТ Р ИСО/МЭК 27002-2021, ГОСТ Р 59453.1-2021, ГОСТ Р 59453.2-2021. Одним из наиболее весомых факторов, которые необходимо учесть внес Указ Президента РФ от 01.05.2022 N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации". Он определяет построение СУИБ, а именно с 01.01.2025 г. использование иностранных средств защиты информации будет невозможно.

Внедрение СУИБ является целесообразным по следующим причинам:

- Защита данных: СУИБ обеспечивает защиту конфиденциальных данных от несанкционированного доступа, кражи, потери и других угроз, что позволяет сохранить целостность и доступность информации.
- Соответствие стандартам: Внедрение СУИБ помогает организациям соответствовать требованиям международных стандартов и регулятивных норм, таких как ISO 27001, PCI DSS, GDPR и другие, что снижает риск штрафов и судебных исков.
- Управление рисками: Система управления позволяет идентифицировать, анализировать и оценивать риски информационной безопасности, а также разрабатывать и внедрять соответствующие меры защиты. Это помогает организациям управлять рисками и предотвращать возможные инциденты информационной безопасности.
- Улучшение процессов: Система управления предоставляет инструменты для оптимизации процессов информационной безопасности, например, для определения политик и процедур, обучения персонала, мониторинга и аудита. Это способствует улучшению общего управления и контроля над информационной безопасностью организации.
- Повышение доверия клиентов и партнеров: Наличие СУИБ демонстрирует клиентам и партнерам организации высокий уровень профессионализма и надежности, что может способствовать увеличению доверия и улучшению отношений.
- Повышение конкурентоспособности: Внедрение современных СУИБ может дать организации конкурентные преимущества на рынке, так как это позволяет быстрее реагировать на угрозы и лучше адаптироваться к изменениям в отрасли.

ЗАКЛЮЧЕНИЕ

Таким образом, внедрение СУИБ приводит к улучшению контроля над информационными активами, снижению рисков и повышению уровня защиты конфиденциальных данных. Это, в свою очередь, способствует повышению конкурентоспособности, улучшению отношений с клиентами и партнерами, а также соблюдению требований регулятивных органов.

Внедрение СУИБ является целесообразным и актуальным для любой организации, поскольку позволяет обеспечить защиту конфиденциальной информации, улучшить процессы безопасности, соответствовать стандартам и минимизировать риски. Эта система помогает управлять рисками, улучшать процессы, повышать доверие клиентов и партнеров, а также повышать конкурентоспособность компании. В целом, внедрение СУИБ приводит к улучшению защиты

информационных активов и снижению рисков, что положительно сказывается на деятельности организации.

Список литературы

1. IT-специалисты в сфере информационной безопасности в 2022. − URL: https://habr.com/ru/articles/679086/. – [Электронный ресурс].

2. Кибербезопасность в 2022–2023. Тренды и прогнозы− URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/#id2. – [Электронный ресурс].

3. Фонд содействия развитию безопасных информационных технологий. Добро пожаловать, сеньоры! Рынок труда в сфере кибербезопасности в третьем квартале 2023 года − URL: https://fsrbit.ru/post/2132. – [Электронный ресурс].

4. Удовиченко А. Стратегия ИБ: а вы решили, как двигаться вперед? – 27.02.2019 г. − URL: https://habr.com/ru/companies/softline/articles/441920/. – [Электронный ресурс].

5. Модель безопасности AstraLinux — основа для апробации новых ГОСТов – 14.05.2021 г.− URL: https://astralinux.ru/about/press-center/news/model-bezopasnosti-astra-linux-osnova-dlya-aprobatsii-novykh-gostov/. – [Электронный ресурс].

6. Шиляев С. Проблемы информационной безопасности: алгоритм построения системы ИБ с нуля – 24.02.2015 г. − URL: https://kontur.ru/articles/1622 – [Электронный ресурс].

7. Реестр программного обеспечения. Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. − URL: https://reestr.digital.gov.ru/. [Электронный ресурс].

8. Указ Президента Российской Федерации от 01.05.2022 г. № 250О дополнительных мерах по обеспечению информационной безопасности Российской Федерации. − URL: http://www.kremlin.ru/acts/bank/47796. – [Электронный ресурс].

9. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. N 1653-ст. − URL: https://garant.belregion.ru/#/document/403510768/paragraph/764/doclist/32/showentries/0/highlight/ГОСТ%20Р%20ИСО%7СМЭК%2027001-2021:2. – [Электронный ресурс].

10.ГОСТ Р ИСО/МЭК 27002-2021. Методы и средства обеспечения безопасности. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности: издание официальное: утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. N 416-ст. − URL: https://garant.belregion.ru/#/document/402878331/paragraph/1/doclist/33/showentries/0/highlight/ГОСТ%20Р%20ИСО%7СМЭК%2027002-2021:4. – [Электронный ресурс].

References

1. IT specialists in the field of information security in 2022. − URL: https://habr.com/ru/articles/679086/. – [Electronic resource].

2. Cybersecurity in 2022-2023. Trends and forecasts − URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/#id2. – [Electronic resource].

3. Foundation for the Promotion of Secure Information Technologies. Welcome, senors! Cybersecurity labor market in the third quarter of 2023. − URL: https://fsrbit.ru/post/2132. – [Electronic resource].

4. Udovichenko A. IB strategy: have you decided how to move forward? – 02/27/2019 − URL: https://habr.com/ru/companies/softline/articles/441920/. – [Electronic resource].

5. AstraLinux security model — the basis for testing new GOST standards – 05/14/2021− URL: https://astralinux.ru/about/press-center/news/model-bezopasnosti-astra-linux-osnova-dlya-aprobatsii-novykh-gostov/. – [Electronic resource].

6. Shilyaev S. Problems of information security: algorithm for building an information security system from scratch – 02/24/2015. − URL: https://kontur.ru/articles/1622. – [Electronic resource].

7. Software registry. Ministry of Digital Development, Communications and Mass Communications of the Russian Federation. − URL: https://reestr.digital.gov.ru/. [Electronic resource].

8. Decree of the President of the Russian Federation No. 250 of 01.05.2022 on additional measures to ensure information security of the Russian Federation. − URL: http://www.kremlin.ru/acts/bank/47796. – [Electronic resource].

9. GOST R ISO/IEC 27001-2021. Information technology. Methods and means of ensuring security. Information security management systems. Requirements: national standard of the Russian Federation: official publication: approved and put into effect by the order of the Federal Agency for Technical Regulation and Metrology dated November 30, 2021 N 1653-st. − URL: https://garant.belregion.ru/#/document/403510768/paragraph/764/doclist/32/showentries/0/highlight/ГОСТ%20Р%20ИСО%7СМЭК%2027001-2021:2. – [Electronic resource].

10.GOST R ISO/IEC 27002-2021. Methods and means of ensuring security. Information technology. Methods and means of ensuring security. Code of Norms and Rules for the application of information security measures: official publication: approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated May 20, 2021 N 416-art. − URL: https://garant.belregion.ru/#/document/402878331/paragraph/1/doclist/33/showentries/0/highlight/ГОСТ%20Р%20ИСО%7СМЭК%2027002-2021:4. – [Electronic resource].

Федоров Алексей Васильевич, магистрант 2 курса кафедры информационная безопасность
Жихарев Александр Геннадиевич, доктор технических наук, доцент, доцент кафедры программного обеспечения вычислительной техники и автоматизированных систем
Кальченко Даниил Михайлович, магистрант 2 курса кафедры информационная безопасность

Fedorov Alexey Vasilyevich, 2nd year Master's student, Department of Information Security
Zhikharev Alexander Gennadievich, Doctor of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Engineering and Automated Systems Software
Daniil Mikhailovich Kalchenko, 2nd year Master's student, Department of Information Security

УДК 004.056.53 **DOI: 10.18413/2518-1092-2024-9-1-0-4**

Храмов М.А.
Корнев Л.В.
Шабля В.О.

ФЕНОМЕНОЛОГИЧЕСКИЙ АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ АУТЕНТИФИКАЦИИ

Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
ул. Красина, 4, г. Краснодар, 350063, Россия

e-mail: khramov.m.a@yandex.ru

Аннотация
В статье рассмотрены методы аутентификации пользователей локальных вычислительных сетей и автоматизированных рабочих мест с целью определения наиболее актуальных способов противодействия внутренним нарушителям, использующих учетные данные других пользователей для входа в систему. Определяется угроза информационной безопасности, реализуемая внутренним нарушителем информационной безопасности различными способами, для последующего использования полученного доступа к учетным записям других пользователей, как плацдарма для реализации компьютерных атак. Методом экспертной оценки проведен сравнительный анализ методов аутентификации пользователей локальных вычислительных сетей и автоматизированных рабочих мест. Проведенный в работе сравнительный анализ позволяет сделать предположение, что противодействие вышеуказанной угрозе информационной безопасности, возможно за счет ввода в систему контроля и управления доступом операционной системы функциональных элементов, ответственных за выполнение процедуры аутентификации, с использованием методов биометрической аутентификации, основанной на динамике работы пользователя.
Ключевые слова: проблемы информационной безопасности; анализ средств защиты информации; биометрическая аутентификация
Для цитирования: Храмов М.А., Корнев Л.В., Шабля В.О. Феноменологический анализ существующих методов аутентификации // Научный результат. Информационные технологии. – Т.9, №1, 2024. – С. 29-36. DOI: 10.18413/2518-1092-2024-9-1-0-4

Khramov M.A.
Kornev L.V.
Shablya V.O.

PHENOMENOLOGICAL ANALYSIS OF EXISTING AUTHENTICATION METHODS

Krasnodar Higher Military School named after Army General S.M. Shtemenko
4 Krasina str., Krasnodar, 350063, Russia

e-mail: khramov.m.a@yandex.ru

Abstract
The article discusses authentication methods for users of local area networks and automated workplaces in order to determine the most relevant ways to counter internal intruders using other users' credentials to log in. The threat to information security is determined, implemented by an internal information security violator in various ways, for subsequent use of the obtained access to the accounts of other users as a springboard for the implementation of computer attacks. A comparative analysis of authentication methods for users of local area networks and automated workplaces was carried out by the method of expert assessment. The comparative analysis carried out in the work suggests that countering the above-mentioned threat to information security is possible by introducing functional elements responsible for performing the authentication procedure into the operating system's access control and management system using biometric authentication methods based on the dynamics of the user's work.
Keywords: information security problems; analysis of information security tools; biometric authentication

For citation: Khramov M.A., Kornev L.V., Shablya V.O. Phenomenological analysis of existing authentication methods // Research result. Information technologies. – T. 9, №1, 2024. – P. 29-36. DOI: 10.18413/2518-1092-2024-9-1-0-4

ВВЕДЕНИЕ

В организациях, в которых принято решение о применении «Методики оценки угроз безопасности информации», утвержденной 5 февраля 2021 г. ФСТЭК России (далее – «Методика оценки угроз») для определения угроз безопасности информации, реализация которых возможна в информационных системах, определяются актуальные категории нарушителей, в зависимости от имеющихся прав и условий доступа к системам, а также от установленных возможностей нарушителей. При этом нарушители подразделяются на две категории: внутренних и внешних нарушителей. Выделяется тактика получения первоначального доступа к компонентам системы нарушителем, находящегося вне инфраструктуры, для использования их как плацдарма для дальнейших действий. Одной из техник достижения данной цели рассматривается несанкционированный доступ к защищаемым ресурсам за счет компрометации учетных данных легитимных пользователей [1, с. 67].

Противодействие угрозам безопасности информации, связанных с компрометацией учетных данных пользователей, осуществляется администраторами безопасности в соответствии с внутренними нормативными правовыми актами организации в области обеспечения безопасности информации. Методы борьбы с внутренними нарушителями, как правило, сводятся к выдаче долгосрочных паролей пользователям под личную подпись в соответствующем журнале учета выдачи, и к ознакомлению их с инструкцией по защите информации организации в вопросах, касающихся возложения на пользователей обязательств по неразглашению полученных учетных данных другим должностным лицам. Данный подход является организационным и позволяет обеспечить соблюдение принципа персональной ответственности пользователя за полученный им пароль, но не обеспечивает какого-либо предупреждения подобных случаев с технической стороны вопроса.

Как следствие, можно сделать объективный вывод, что существующий подход предоставления доступа пользователям к защищаемым ресурсам не отвечает требованиям модели угроз безопасности информации, в которой рассматривается наличие внутренних нарушителей. Реализация тактики получения доступа к защищаемым ресурсам сводится к легко исполнимой технике компрометации паролей учетных записей пользователей. Инструменты защиты информации, способных выявить подобный несанкционированный доступ отсутствуют, а организационных мер недостаточно.

В данной работе предлагается оценить возможные подходы к решению данной проблемы, основываясь на выводах предыдущих исследований, а именно – для повышения доверия к среде функционирования взаимодействующих субъектов и объектов доступа операционной системы возможно использовать тот же подход, что и в отношении подсистем, выполняющих функции авторизации. Архитектура операционных систем реализует выполнение функции авторизации несколькими модулями. Предлагается ввести в систему дополнительный компонент, ответственный за выполнение процедуры аутентификации, как и диспетчер учетных записей безопасности операционных систем.

ФЕНОМЕНОЛОГИЧЕСКИЙ АНАЛИЗ МЕТОДОВ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

Классифицировать методы аутентификации можно по факторам, используемых в методах аутентификации для проверки подлинности пользователя.

Выделяют следующие типы аутентификационной информации:

1. Фактор знания — наиболее распространенный вид аутентификации, который требует от пользователя знания некоторой информации.

1.1. Постоянные пароли — тип аутентификационной информации, который остаётся постоянным и не изменяется на протяжении определенного периода времени или до изменения пользователем.

1.2. Одноразовые пароли — временные и одноразовые пароли или коды, которые генерируются и используются для однократной аутентификации пользователя при входе в систему.

1.3. Графические пароли — тип аутентификационной информации, требующий от пользователя создать пароль не путем ввода символов или цифр, а путем выбора определенных изображений или паттернов на экране устройства.

1.4. Секретные вопросы — реализация фактора знания, характеризуемая тем, что при проверке подлинности пользователя, ему предъявляются определенные вопросы, на которые только он должен знать ответы [2, с. 2].

2. Фактор владения — вид аутентификации, который требует от пользователя иметь физическое устройство или объект, такой как ключ, смарт-карта, токен или мобильное устройство, для подтверждения своей подлинности. Так же необходимо наличие аппаратно-программные системы идентификации и аутентификации [2, с. 3].

2.1. Ключи и карты доступа — пользователь имеет физический объект, такой как ключ или карта доступа, который используется для получения доступа к системе или учетной записи.

2.2. Устройства аутентификации — это могут быть устройства типа токенов, смарт-карт, USB-ключей или мобильных устройств, которые генерируют одноразовые пароли или подтверждения для прохождения аутентификации.

2.3. Беспроводные устройства аутентификации — например, Bluetooth-устройства, которые автоматически аутентифицируют пользователя при нахождении в определенной зоне доступа.

2.4. Устройства с технологией NFC — такие устройства могут быть использованы для аутентификации пользователя на основе его физического присутствия и владения устройством.

3. Биометрический фактор — вид аутентификации, который использует уникальные физиологические или поведенческие характеристики пользователя.

3.1. Статические характеристики биометрической аутентификации — физиологические особенности или параметры, которые остаются постоянными у человека и могут быть использованы для его идентификации.

3.1.1 По отпечатку пальца — вид аутентификации, при котором индивидуальные физиологические особенности отпечатков пальцев пользователя используются для его аутентификации в системе.

3.1.2. По кисти руки — метод аутентификации пользователя с использованием уникальных биометрических характеристик руки, таких как геометрия ладони, длина пальцев, расстояния между суставами и другие особенности.

3.1.3. По сетчатке глаза — метод аутентификации человека на основе уникальных характеристик сосудистой сетчатки глаза. Уникальные особенности сетчатки, такие как узор сосудистой сетчатки и другие анатомические особенности, используются для создания уникального биометрического шаблона каждого человека.

3.1.4. По радужной оболочке глаза — метод аутентификации человека на основе уникальных особенностей радужной оболочки глаза. Используя особенности радужной оболочки, можно создать уникальный биометрический шаблон для аутентификации человека.

3.1.5. По форме лица — метод аутентификации человека на основе уникальных морфологических особенностей его лица. При данном методе биометрии сканируется лицо человека с помощью специальных камер или устройств, и на основе уникальных особенностей формы лица создается биометрический шаблон, который может быть использован для проверки пользователя.

3.1.6. По ДНК — метод идентификации человека на основе уникальной генетической информации, которая хранится в ДНК (дезоксирибонуклеиновой кислоте) каждого человека. ДНК содержит уникальные генетические характеристики, которые индивидуальны для каждого человека, за исключением идентичных близнецов. Используемые в настоящее время методы

получения и обработки ДНК – работают настолько долго, что такие системы используются только для специализированных экспертиз, в связи с чем, данный метод не будет рассматриваться в последующей анализе [3, с. 4].

3.2. Динамические характеристики биометрической аутентификации пользователя включают в себя физиологические или поведенческие аспекты, которые могут быть измерены и использованы для подтверждения аутентификации пользователя.

3.2.1. По рукописному почерку — метод аутентификации человека, основанный на уникальных особенностях его почерка, то есть стиля и способа написания текста от руки. Каждый человек имеет индивидуальные черты в своем почерке, такие как размер, форма и углы букв, интервалы между словами, давление пера и т. д., которые могут быть использованы для аутентификации личности.

3.2.2. По клавиатурному почерку — метод аутентификации пользователя на основе уникального образца нажатия клавиш на клавиатуре компьютера или устройства во время ввода текста.

3.2.3. По жестам управления на сенсорном экране — метод аутентификации человека на основе уникальных особенностей его жестов, совершаемых на сенсорном экране устройства.

3.2.4. По голосу — метод аутентификации личности на основе уникальных характеристик голоса человека.

3.2.5. С использованием системы акселерометров — метод аутентификации личности на основе уникальных характеристик движений и поведения пользователя, которые могут быть измерены с помощью акселерометра, устройства, способного измерять ускорение и изменения скорости движения объекта [4, с. 61].

3.2.6. С использованием биоэлектрических сигналов человека — метод аутентификации личности на основе уникальных электрических сигналов (электрокардиограмма, электроэнцефалограмма), которые генерируются человеческим организмом [5, с. 87].

4. Другие факторы.

4.1. С использованием поручителей — это метод аутентификации пользователей, при котором для подтверждения личности пользователя требуется участие третьей стороны, называемой поручителем или гарантом. Поручитель в данном случае является доверенным лицом или системой, которая выступает в качестве подтверждения личности пользователя [6, с. 114].

4.2. Аутентификация на основе блокчейна — метод аутентификации, который использует технологию блокчейна для проверки личности пользователя. Аутентификация на основе блокчейна основана на создании уникальной цифровой подписи, которая аутентификации пользователя. Пользователь создает свою цифровую подпись и сохраняет ее в блокчейне [7, с. 60].

4.3. Аутентификатор подлинности с использованием сертификатов, токенов и контрольных сумм [6, с. 112].

4.3.1. При аутентификации с использованием сертификатов, клиентский сертификат используется для подтверждения личности пользователя или устройства перед получением доступа к ресурсам.

4.3.2. При аутентификации с использованием токенов, пользователю может потребоваться ввести одноразовый код или использовать устройство для генерации токенов для подтверждения своей личности. Одним из преимуществ использования токенов, это возможность выдачи его пользователю на определенный срок или отзыв токена в связи с нарушением политики информационной безопасности.

4.3.3. При аутентификации с использованием контрольных сумм, сервер может сравнивать вычисленную контрольную сумму с ожидаемым значением для проверки целостности данных при передаче или хранении.

4.4. Цифровые отпечатки браузера — метод проверки подлинности пользователя, основанный на уникальных характеристиках и параметрах его веб-браузера. Каждый веб-браузер имеет уникальные характеристики, такие как версия браузера, операционная система, разрешение экрана,

установленные шрифты и т.д., которые могут быть использованы для создания цифрового отпечатка браузера [8, с. 103].

Объективно, аутентификационные данные, основанные на факторах «знания» и «владения» должны быть основой в вопросах допуска пользователей к защищаемым ресурсам информационных систем, что и соответствует текущему положению дел. Однако, все способы аутентификации, основанные на вышеуказанных факторах, не позволяют противодействовать внутреннему нарушителю требований информационной безопасности организации. У легитимного пользователя есть техническая возможность передать аутентификационные данные злоумышленнику.

В вопросах борьбы с вышеописанными внутренними нарушителями особыми преимуществами обладают биометрические способы аутентификации, а именно: неподдельность, надежность, удобство, сложность реализации атак, долгосрочное использование аутентификационной информации. Так же существует и ограничение со стороны регулятора, а именно, необходимость использования биометрического фактора только совместно с другими факторами аутентификации [9, с. 13].

В связи с вышеизложенным, предлагается сравнить между собой методы биометрической аутентификации, с целью решения проблемы с отсутствием инструментов технического контроля пользователей на факт компрометации своих учетных данных.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ АУТЕНТИФИКАЦИИ

Сравнение характеристик методов биометрической аутентификации проводится по пяти основных группам характеристик, актуальных в вопросах противодействия внутреннему нарушителю требований информационной безопасности. Для выбора рассматриваемых характеристик и ранжирования степени их проявления использовался метод экспертной оценки. Оценка каждой характеристики производилась независимо от совокупности используемых методов аутентификации. Каждой характеристике соответствующих методов аутентификации были присвоены значения исходя из степени проявления: 0 – низкая степень проявления; 0,5 – средняя степень проявления; 1 – высокая степень проявления.

Таблица

Сравнение характеристик методов биометрической аутентификации

Table

Comparison of characteristics of biometric authentication methods

Характеристики / Способы реализации	Стоимость реализации	Удобство использования	Мониторинг действий пользователя	Точность распознавания	Масштабируемость
Отпечатки пальцев	0,5	1	0	1	0,5
По кисти руки	0	1	0	1	0
По сетчатке глаза	0	0	0	1	0
По радужной оболочке глаза	0	0,5	0	1	0,5
По форме лица	0,5	1	0,5	1	0,5
По рукописному почерку	0,5	0,5	0,5	0,5	0,5
По клавиатурному почерку	1	1	1	0,5	1

Характеристики / Способы реализации	Стоимость реализации	Удобство использования	Мониторинг действий пользователя	Точность распознавания	Масштабируемость
По жестам управления на сенсорном экране	1	1	1	0,5	1
По голосу	0,5	0,5	0	0,5	0,5
С использованием системы акселерометров	0	1	0,5	0,5	0,5
С использованием биоэлектрических сигналов человека	0	0	0	0,5	0

Стоимость реализации биометрических методов аутентификации пользователей включает в себя все расходы, связанные с внедрением и использованием биометрических технологий для идентификации и аутентификации пользователей, и включает в себя: Стоимость оборудования, Стоимость программного обеспечения, техническую поддержку, настройку системы.

Удобство использования биометрических методов аутентификации пользователей характеризуется скоростью взаимодействия и отсутствием выполнения дополнительных действий со стороны пользователя.

Мониторинг действий пользователя при использовании биометрических методов аутентификации пользователей представляет собой процесс отслеживания и анализа поведения пользователей в системе, и является ключевым фактором выбора в работе наиболее подходящего метода противодействия внутреннему нарушителю.

Точность распознавания при использовании биометрических методов аутентификации пользователей отражает способность системы биометрической идентификации точно идентифицировать пользователя на основе его биометрических данных.

Масштабируемость при использовании биометрических методов аутентификации пользователей отражает сложность реализации метода на всех объектах организации, подлежащих защите.

Экспертной оценке подвергалось большинство перечисленных методов биометрической аутентификации, несмотря на неприменимость некоторых к использованию в системе защиты информации локальных вычислительных сетей и автоматизированных рабочих мест.

Исходя из оценки можно сделать вывод, что для работы со статической биометрической аутентификационной информацией требуется установка дополнительного оборудования, обеспечивающее однозначную аутентификацию пользователя. Однако, если рассматривать уже имеемую систему защиту информации в большинстве организаций и требования нормативных правовых актов в области информационной безопасности, большей актуальностью обладает стратегия внедрения способов биометрической аутентификации по поведенческим признакам человека, ввиду их доступности за счет программной реализации, и за счет ориентированности на постоянный мониторинг работы пользователя и подтверждение его соответствия заявленному идентификатору. Такими качествами обладает аутентификация по динамике работы пользователя с клавиатурой и сенсорным экраном.

В действительности, сенсорные экраны не являются основным способом взаимодействия пользователя с информационной системы, но, в свою очередь, аутентификация по динамике работы с клавиатурой обладает недостатками, а именно, она не дает один однозначный результат, в связи с тем, что зависит от многих свойств. Но, в качестве реализации многофакторной аутентификации пользователя, с фокусом на постоянный мониторинг легитимности пользователя, поведенческая

биометрическая аутентификация, основанная на анализе клавиатурного почерка пользователя, наиболее подходящий вектор развития системы аутентификации, как компонента системы контроля и управления доступом операционных систем локальных вычислительных сетей и автоматизированных рабочих мест.

ВЫВОДЫ

Сравнительный анализ методов аутентификации пользователей подтвердил преимущество методов биометрической аутентификации, основанных на динамических характеристиках пользователей, в системе защиты информации, где данные методы реализованы в качестве дополнительного фактора аутентификации, сфокусированных на обеспечении постоянного мониторинга действий пользователя и периодической проверки соответствия пользователя заявленной паре идентификатора и аутентификационной информации, предъявленной при авторизации в системе.

Необходимым свойством динамической биометрической аутентификации для построения данной модели системы защиты информации является невозможность компрометации аутентификационной информации пользователем, нарушающего требования безопасности информации организации, другим должностным лицам.

Проведенный в работе сравнительный анализ позволяет предположить, что для противодействия тактике реализации угроз информационной информации внутренних нарушителей, которая сводится к использованию чужих учетных данных, как плацдарма для реализации угроз в информационной системе, а именно, за счет ввода в систему контроля и управления доступом операционной системы функциональных элементов, ответственных за выполнение процедуры аутентификации, с использованием методов биометрической аутентификации, основанной на динамике работы пользователя.

Список литературы

1. Методический документ. Методика оценки угроз безопасности информации [Электронный ресурс]: утв. ФСТЭК России 05.02.2021 // URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g // (дата обращения: 03.03.2024).
2. Комеков Э.А. Системы аутентификации // Вестник науки и образования. 2022. № 1. С. 1-4.
3. Сидоркина И.Г. Классификация методов аутентификации человека // Вестник Волжского университета им. В.Н. Татищева. 2009. № 1. С. 1-6.
4. Корякова В.А. Аутентификация пользователя смартфона на основе данных, полученных с акселерометра // Прикаспийский журнал: управление и высокие технологии. 2023. № 61(1). С. 59-72.
5. Кураков В.И. Анализ уязвимостей биометрических методов аутентификации // Международный научный журнал «Вестник науки». 2022. № 5(50). С. 87-98.
6. Вишняков В.А. Модели и средства аутентификации пользователей в корпоративных системах управления и облачных вычислениях // Доклады Белорусского государственного университета информатики и радиоэлектроники. 2016. № 3(97). С. 111-114.
7. Посметухова К.Н. Обзор и краткий анализ современных методов аутентификации // Наука и реальность. 2023. № 2(14). С. 58-62.
8. Осин А.В. Обзор методов идентификации пользователя на основе цифровых отпечатков // Труды учебных заведений связи. 2023. № 5. С. 91-111.
9. ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения.

References

1. Methodological document. Methodology for assessing information security threats [Electronic resource]: approved by FSTEC of Russia 05.02.2021 // URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g // (accessed: 03/03/2024).
2. Komekov E.A. Authentication systems // Bulletin of Science and Education. 2022. No. 1. pp. 1-4.

3. Sidorkina I.G. Classification of human authentication methods // Bulletin of the V.N. Tatishchev Volga State University. 2009. No. 1. pp. 1-6.

4. Koryakova V.A. Smartphone user authentication based on data obtained from the accelerometer // Caspian Journal: Management and high technologies. 2023. No. 61(1). pp. 59-72.

5. Kurakov V.I. Vulnerability analysis of biometric authentication methods // The international scientific journal "Bulletin of Science". 2022. No. 5(50). pp. 87-98.

6. Vishnyakov V.A. Models and means of user authentication in corporate management systems and cloud computing // Reports of the Belarusian State University of Informatics and Radioelectronics. 2016. No. 3(97). pp. 111-114.

7. Posmetukhova K.N. Review and brief analysis of modern authentication methods // Science and reality. 2023. No. 2(14). pp. 58-62.

8. Osin A.V. Review of user identification methods based on digital fingerprints // Proceedings of educational institutions of communications. 2023. No. 5. pp. 91-111.

9. GOST R 58833-2020 Information protection. Identification and authentication. General provisions.

Храмов Максим Андреевич, аспирант кафедры информационной безопасности
Корнев Лев Викторович, аспирант кафедры информационной безопасности
Шабля Владимир Олегович, аспирант кафедры информационной безопасности

Khramov Maxim Andreevich, postgraduate student of the Department of Information Security
Kornev Lev Viktorovich, postgraduate student of the Department of Information Security
Shablya Vladimir Olegovich, postgraduate student of the Department of Information Security

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ
AUTOMATION AND CONTROL

УДК 004.4 **DOI: 10.18413/2518-1092-2024-9-1-0-5**

Постнов В.Р.
Абрамова О.Ф.

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ УПРАВЛЕНИЯ В СЕТИ ПИЦЦЕРИЙ

Волжский политехнический институт (филиал) ФГБОУ ВО «Волгоградский государственный технический университет», ул. Энгельса, 42а, г. Волжский, Волгоградская область, 404121, Россия

e-mail: astra@post.volpi.ru

Аннотация
В данной статье представлены результаты анализа осуществимости и образ автоматизированной системы управления бизнес-процессами для пиццерий. Эпоха компьютеризации не стоит на месте, из-за чего автоматизированные системы внедряются во сферы деятельности. Она коснулась всех областей: торговля, производство, информация. Не обошлось без внедрения в сферы питания таких как АИК-БИСТРО, ДОДО-ПИЦЦА, и им подобные. Данная система позволяет быстро обслуживать клиентов за счёт структурированности предприятия, и территориальной распространенности, благодаря чему приносит больше прибыли за счёт большого потока потребителей, принося сотни тысяч прибыли, помимо закупочных ингредиентов и расходных материалов. Взяв в расчет пандемию коронавирусной инфекции, многие сети быстрого питания перешли на доставку, что позволило им закрепиться на рынке и уверенно развиваться. Выявленные минусы бизнес-процессов предприятия по принятию, выдаче заказов и их доставки были учтены в проведенном анализе, что позволило избежать грубых нарушений в предлагаемом образе системы за счет улучшения обратной связи с потребителями и максимальной оптимизации процесса доставки товара. Так же учтен процесс изготовления продукции, который подвергся структуризации, избавившись от ненужных позиций, что позволило сконцентрироваться на потенциальной прибыли.
Ключевые слова: автоматизация; прибыль; система; оптимизация
Для цитирования: Постнов В.Р., Абрамова О.Ф. Разработка информационной системы для управления в сети пиццерий // Научный результат. Информационные технологии. – Т.9, №1, 2024. – С. 37-45. DOI: 10.18413/2518-1092-2024-9-1-0-5

Postnov V.R.
Abramova O.F.

DEVELOPMENT OF AN INFORMATION SYSTEM FOR MANAGEMENT IN A NETWORK OF PIZZERIA

Volzhsky Polytechnic Institute (branch) Volgograd State Technical University, 42a Engels str., Volzhsky, Volgograd region, 404121, Russia

e-mail: astra@post.volpi.ru

Abstract
This article presents the results of the feasibility analysis and an image of an automated business process management system for pizzerias. The era of computerization does not stand still, which is why automated systems are being introduced into all spheres of activity. She touched all areas: trade, production, information. It was not without the introduction into the field of nutrition such as AIK-BISTRO, DODO-PIZZA, and the like. This system allows you to quickly serve customers due to the structuring of the enterprise, and territorial distribution, which makes it more profitable due to a large flow of consumers, bringing hundreds of thousands of profits, in addition to purchasing ingredients and consumables. Taking into account the coronavirus pandemic, many fast

food chains switched to delivery, which allowed them to gain a foothold in the market and develop confidently. The identified disadvantages of the company's business processes for accepting, issuing orders and delivering them were taken into account in the analysis, which made it possible to avoid gross violations in the proposed image of the system by improving customer feedback and maximizing the optimization of the product delivery process. Also, the manufacturing process of products was taken into account, which underwent structuring, getting rid of unnecessary positions, which allowed us to focus on potential profits.
Keywords: automation; profit; system; optimization
For citation: Postnov V.R., Abramova O.F. Development of an information system for management in a network of pizzeria // Research result. Information technologies. – T.9, №1, 2024. – P. 37-45. DOI: 10.18413/2518-1092-2024-9-1-0-5

ВВЕДЕНИЕ

Сети быстрого питания – это повседневная потребность современного потребителя, которая пользуется спросом даже спустя 74 года со дня основания первых сетей в далеком СССР. Со временем они проходят модернизацию, оптимизацию, структуризацию для получения максимальной эффективности и обогащения владельцев. Эта структура огромна, каждый человек может найти продукцию, удовлетворяющую его личные потребности и предпочтения.

Однако, многие сети быстрого питания не могут выстроить адекватную и понятную систему работы что внутри предприятия, что в работе с клиентами.

Для решения этих проблем сети быстрого питания АИС “Быстро-пицца” был предложен проект по автоматизации и оптимизации рабочих бизнес-процессов, начиная от принятия заказа, его приготовления, до получения выходной продукции.

ОСНОВНАЯ ЧАСТЬ

Для решения поставленных задач необходимо провести тщательное исследование и анализ работы всех отделов заведения. Деятельность предприятия по изготовлению пиццы включает основной бизнес-процесс “Обслуживание клиентов” (рис. 1), который можно декомпозировать на 3 этапа (рис. 2):

1. Получение заказа.
2. Выполнение заказа.
3. Выдача заказа.

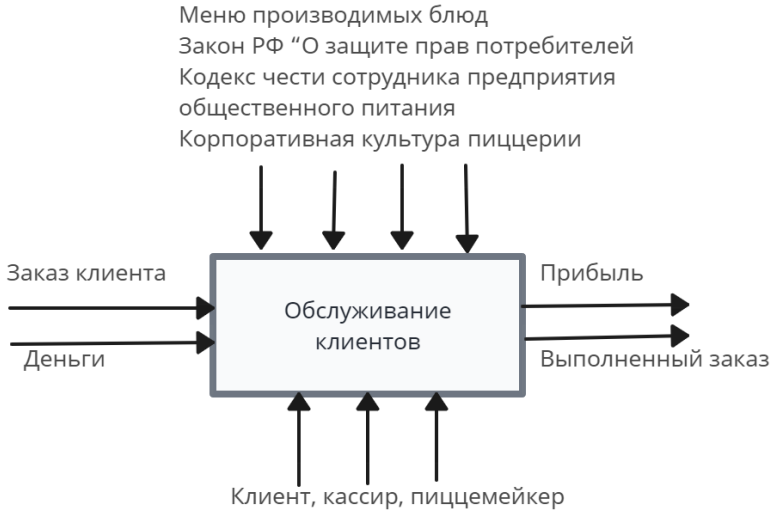


Рис. 1. Модель основного бизнес-процесса в нотации IDEF0
Fig. 1. The model of the main business process in the IDEF0 notation

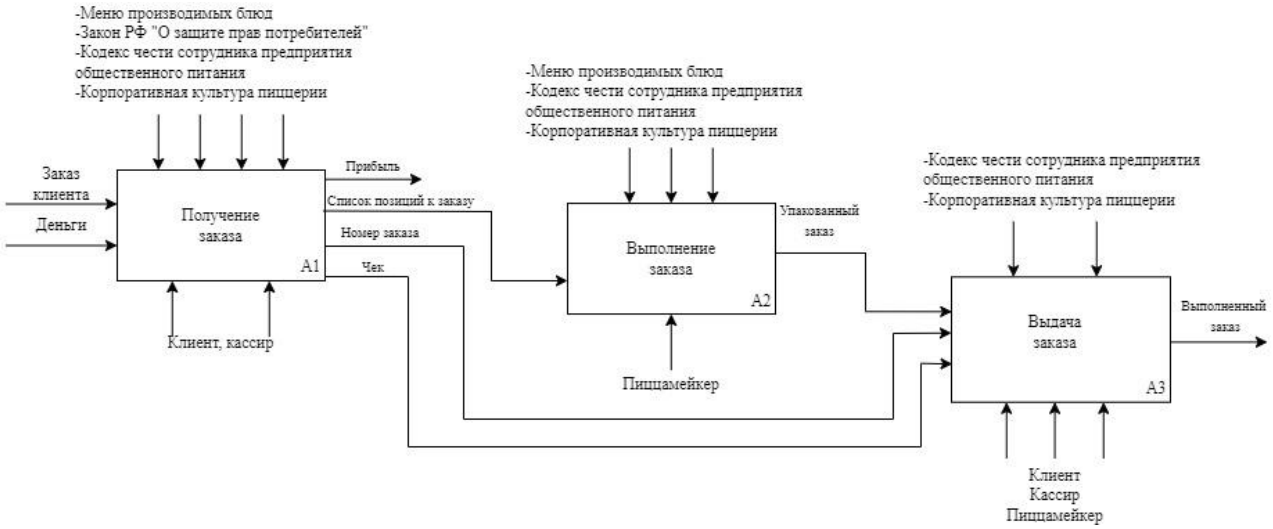


Рис. 2. Декомпозиция основного бизнес-процесса пиццерии
Fig. 2. Decomposition of the pizzeria's main business process

Рассмотрим бизнес-функции подробнее.

Получение заказа – на данном этапе кассир принимает заказ у клиента, который стоит в очереди первый. Менеджер коммуницирует с клиентом, уточняет детали заказа, получает оплату и выдает чек с номером заказа, а после сообщает пиццемейкерам, что заказал клиент.

1. Входные данные: заказ клиента
2. Управляющие данные: меню производимых блюд, Закон РФ “О защите прав потребителей”, кодекс чести сотрудника предприятия общественного питания, корпоративная культура пиццерии.
3. Выходные данные: прибыль, список позиций к заказу, номер заказа, чек.
4. Механизмы: клиент, кассир

Выполнение заказа – пиццамейкеры начинают готовить заказ и упаковывать для дальнейшей передачи.

1. Входные данные: словесная информация о заказе.
2. Управляющие данные: меню производимых блюд, корпоративная культура пиццерии.
3. Выходные данные: упакованный заказ.
4. Механизмы: пиццамейкер.

Выдача заказа – кассир ожидает клиента, чтобы отдать упакованный заказ.

1. Входные данные: упакованный заказ, номер заказа.
2. Управляющие данные: корпоративная культура пиццерии, кодекс чести сотрудника предприятия общественного питания.
3. Выходные данные: выполненный заказ.
4. Механизмы: кассир, пиццамейкер, клиент.

Для выявления всех проблем необходимо также исследовать потоки данных на предприятии. Для этого будем использовать нотацию DFD и построим модель потоков данных «как есть» (рис. 3), которая показывает, что в работе заведения все операции архаичны с точки зрения оптимизации обработки и передачи данных, отсутствует четкая последовательность действий.

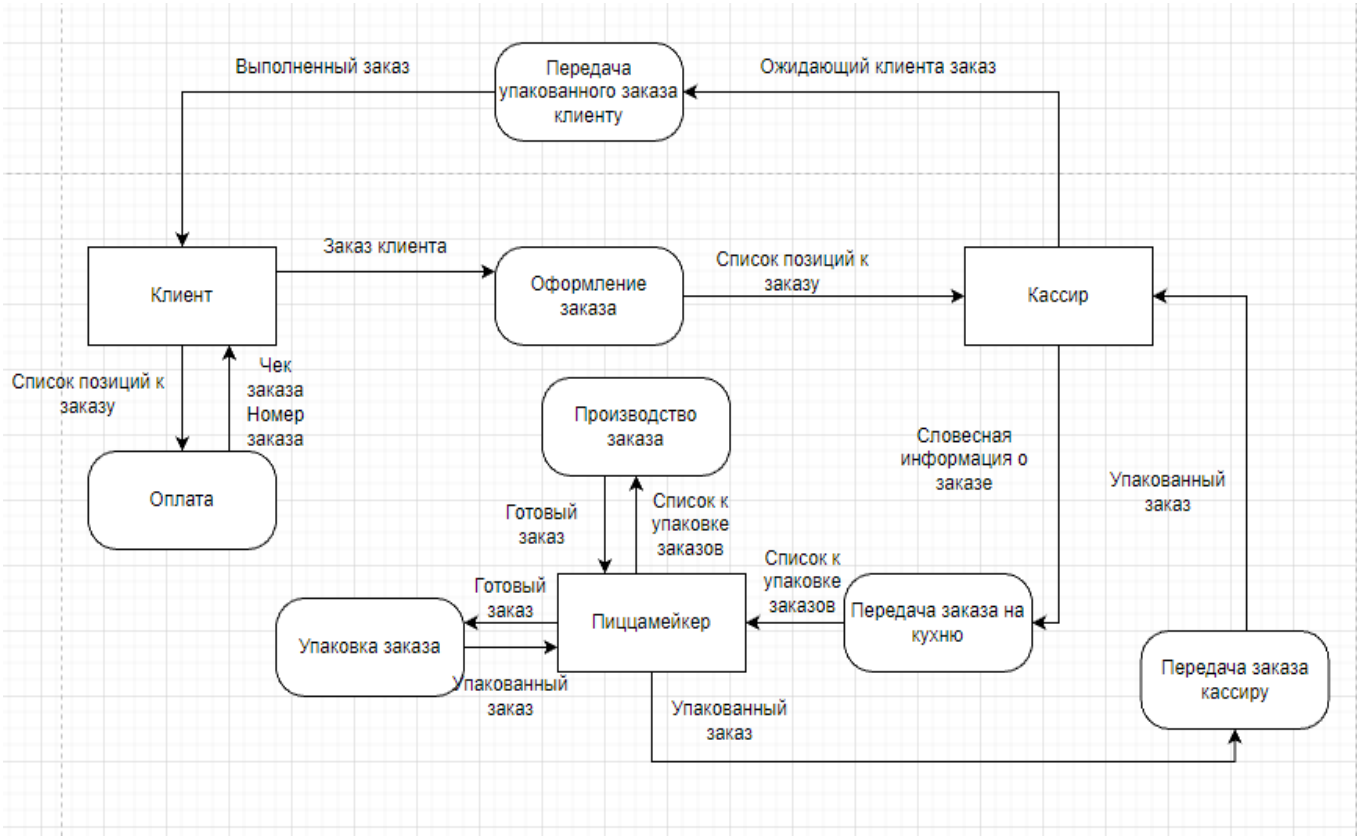


Рис. 3. Модель потоков данных «как есть»
Fig. 3. " The "as is" data flow model

Таким образом, проанализировав построенные в ходе исследования модели процессов и потоков данных, предлагаются следующие решения по улучшению работы предприятия:

1. Создание электронной очереди: заменить кассира на покупку и установку терминала. Таким образом можно будет создать электронную очередь и оформлять заявки либо дистанционно с устройства клиента, либо с терминала в пиццерии. Тем самым получиться сэкономить на сотрудниках и расширить возможности для клиентов. Стоимость терминала самообслуживания 120 000 руб., зарплата кассира 30 000 руб., смарт-терминал для кухни 24 000 руб. Итого, при покупке 2 шт. терминалов самообслуживания, и 1 шт. терминала на кухню затраты будут 264 000 руб., что равно ~9-ти месячной зарплате кассира.
2. При создании электронной очереди и установке терминалов повысится быстродействие передачи заказов на кухню, что ускорит производство заказов в целом, а, следовательно, увеличит количество потенциальных клиентов.
3. Стоит отметить, что клиент на данный момент не информирован о статусе оформленного заказа. За счет автоматизации в реализуемом приложении можно будет выдавать уведомления о готовности заказа, что повысит клиентоориентированность пиццерии.
4. В настоящее время сотрудники не информируются о качестве выпущенной ими продукции, что снижает мотивацию и вовлеченность в рабочий процесс. Добавив возможность для клиента оставить отзыв о заказе онлайн, можно узнать мнение клиента, чтобы повысить качество услуг. Данный способ так же повысит клиентоориентированность.

Опираясь на результаты исследования деятельности предприятия и сделанные выводы об эффективных улучшениях, была предложена модель требований (рис. 4) для реализации автоматизированного решения. Модель представлена в нотации UML и позволяет отследить запланированные к реализации варианты использования системы, а также уровни доступа потенциальных пользователей к функционалу. В системе выделены следующие роли: клиент, пиццамейкер, гость. Для них предусмотрены следующие варианты использования:

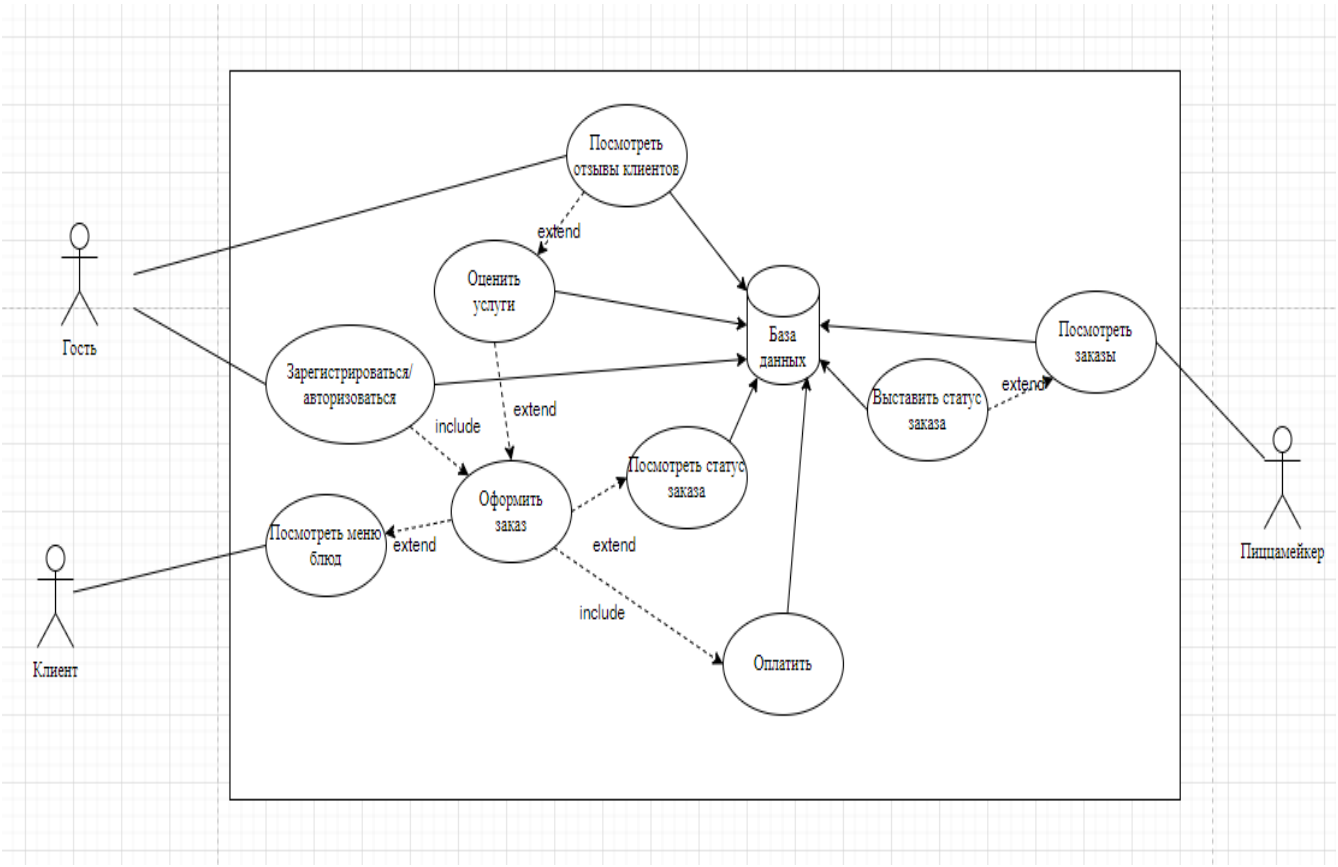


Рис. 4. Модель требований в нотации UML
Fig. 4. Requirements model in UML notation

«Гость» выступает незарегистрированным пользователем, имеющим возможность просматривать меню, оформить заказ, авторизоваться и стать «клиентом».

«Клиент» имеет возможность: авторизоваться на сайте, просмотреть список блюд, оформить заказ, оплатить заказ после оформления, оценить заказ, посмотреть статус оформленного заказа, просмотреть отзывы других клиентов.

«Пиццамейкер» просматривает заказы, обновляет статус заказа в процессе работы, просматривает отзывы клиентов для улучшения работы и качества выпускаемой им продукции.

Модель потоков данных «как должно быть» указана на рисунке 5.

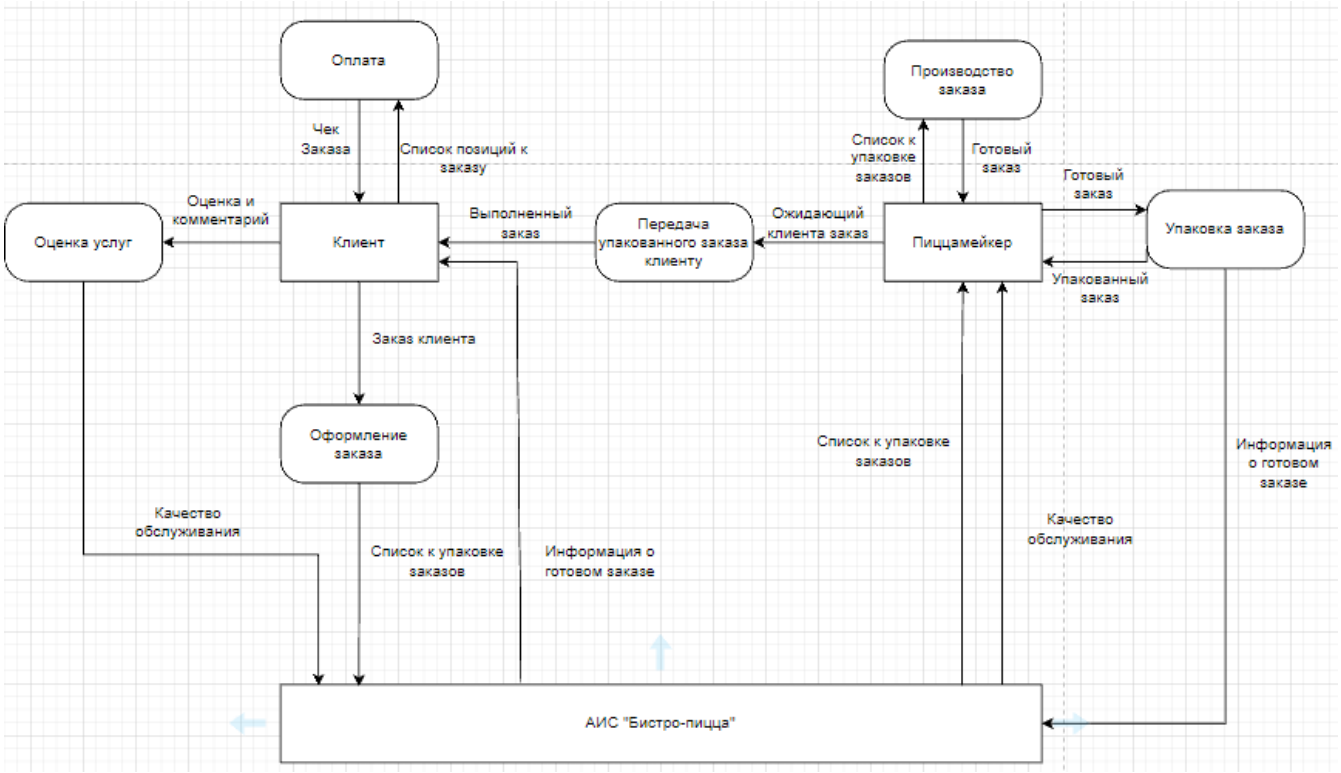


Рис. 5. Модель потоков данных «как должно быть»
Fig. 5. The "as it should be" data flow model

Рассмотрим основные варианты использования (ВИ) системы подробнее.

Вариант использования **“Оформить заказ”**

Описание: оформление заказа для последующей оплаты

Действующие экторы: клиент, гость

Предусловия: авторизация в системе, наличие позиций в корзине.

Сценарий:

1. Клиент переходит в корзину, система отображает список позиций к заказу с указанием количества.
2. Клиент может отредактировать заказ, изменив количество позиций в целом, и штук одной позиции в частности.
3. Клиент нажимает кнопку “Оформить заказ”.

Альтернативные потоки №1:

1. Клиент переходит в корзину.

a. Если список заказов отсутствует, то система отображает сообщение “Добавьте товары к заказу”.

Альтернативные потоки №2:

1. Гость переходит в корзину.

a. Если список заказов отсутствует, то система отображает сообщение “Добавьте товары к заказу”.

b. Если список заказов есть, то система отображает вместо кнопки “оформить заказ”, кнопку “Зарегистрироваться”.

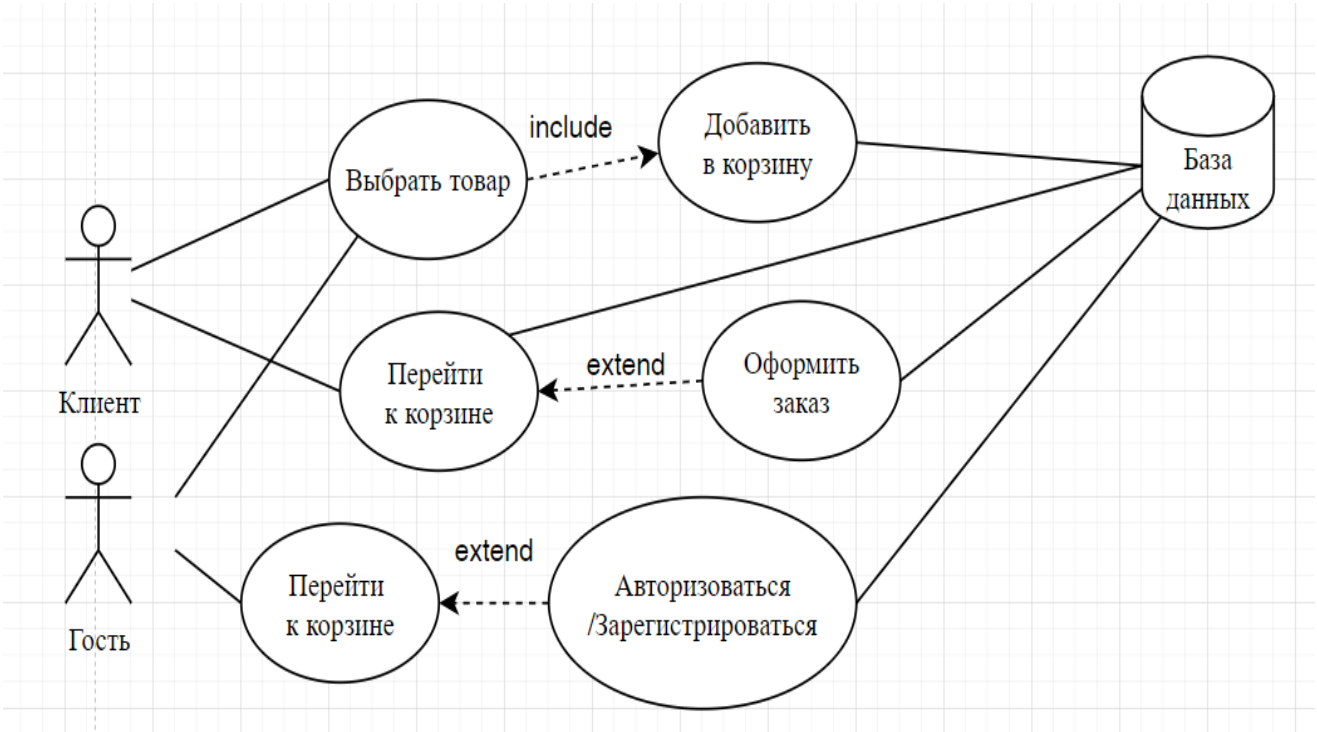


Рис. 6. ВИ «Оформление заказа»
Fig. 6. The use case of the "Checkout" system

Вариант использования “Оценить услуги”

Описание: клиент может оценить услуги после получения заказа в течении 24 часов.

Действующие экторы: клиент

Предусловия: наличие оформленного заказа, готовый заказ.

Сценарий:

1. Клиент переходит в раздел «Заказы», система отображает список всех его заказов. На всех готовых и оплаченных заказах присутствует кнопка “Оставить отзыв”.
2. Клиент нажимает кнопку “Оставить отзыв”, система открывает окно отзыва, в котором есть возможность оценить качество заказа с помощью пятизвездочной шкалы и комментария.
3. Клиент выставляет оценку, пишет комментарий и нажимает кнопку “Отправить”. Система сохраняет данные.
4. Система выводит сообщение клиенту “Спасибо за отзыв”.

Альтернативные поток 1

1. Клиент не выставил оценку, пишет комментарий и нажимает кнопку “Отправить”.

a. Клиент не выставил оценку.

b. Система выводит сообщение клиенту “Оцените, пожалуйста, нашу пиццу!”.

2. Клиент выставляет оценку, не пишет комментарий и нажимает кнопку “Отправить”.

a. Клиент пропускает поле с комментарием.

b. Система выводит сообщение: «Может быть вы хотели бы что-то нам сказать?».

c. Клиент может добавить текст в поле комментария либо нажать кнопку «Нет».

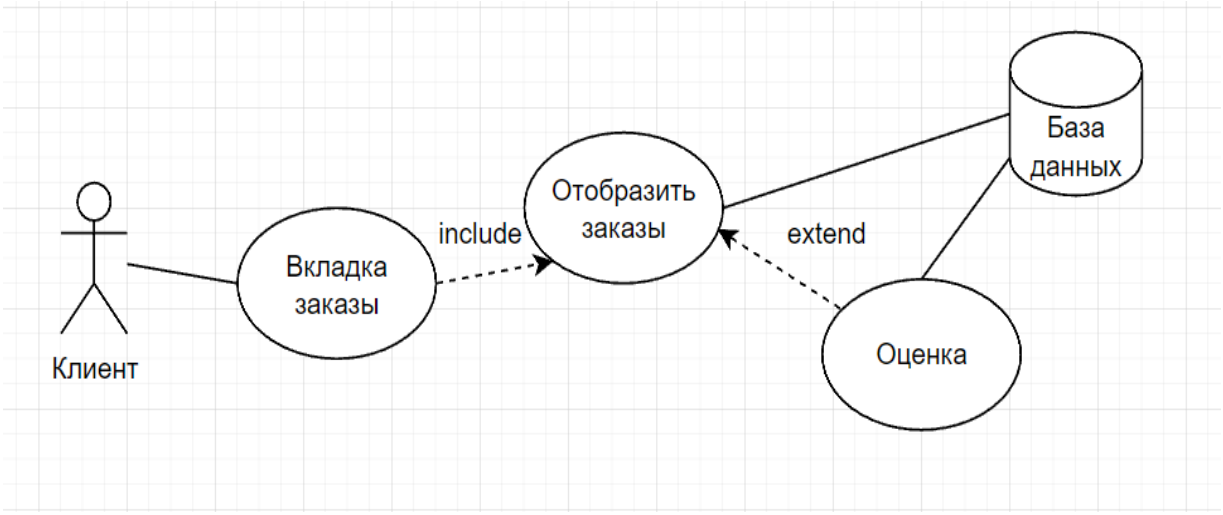


Рис. 7. ВИ «Оценка услуг»
Fig. 7. The use case of "Service assessment"

Вариант использования “Оплатить”
Описание: оплата через систему платежей.
Действующие экторы: клиент
Предусловия: присутствует собранный заказ.
Сценарий:
1. Клиент переходит на страницу оплаты и нажимает кнопку “Оформить заказ”, система перенаправляет пользователя на оплату.
2. Клиент производит оплату заказа через систему оплаты и возвращается обратно к странице заказов.
3. Система записывает информацию о заказе в базу данных.
Альтернативные потоки:
1. При проблемах с коммуникациями в системе оплаты и связи с банковой системой приложение выдает сообщение «Возникли проблемы с оплатой. Попробуйте еще раз!».

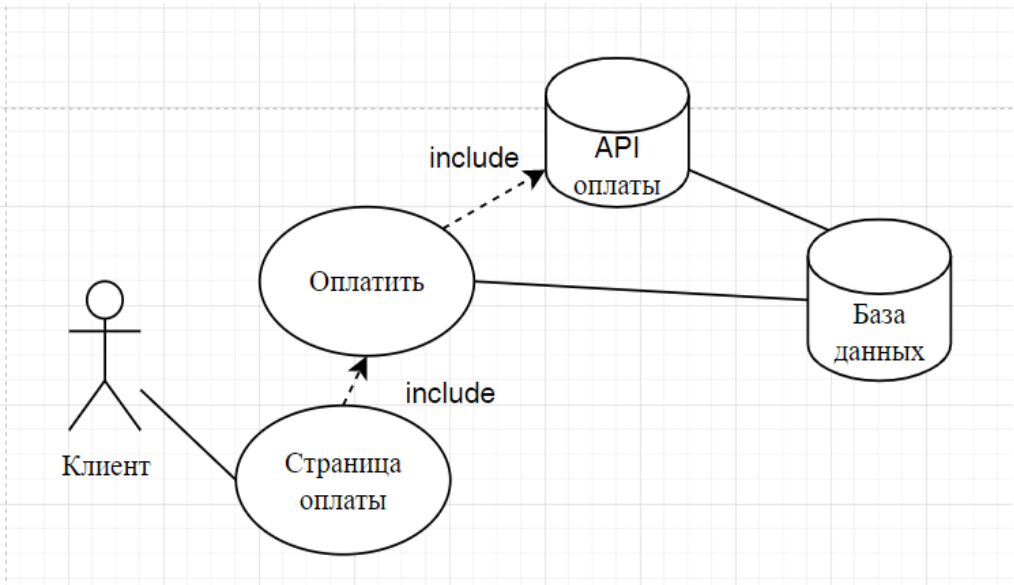


Рис. 8. ВИ Оплата
Fig. 8. The use case of "Payment"

ЗАКЛЮЧЕНИЕ

Благодаря четко сформулированной цели, а также проанализировав построенные в ходе анализа осуществимости модели бизнес-процессов организации, были сформулированы рекомендации по улучшению работы пиццерии, что позволит значительно увеличить прибыль за счет обслуживания большего числа посетителей, улучшению выпускаемой работниками продукции и повышения скорости обслуживания.

Список литературы

1. Васильев С.С. Исследование и анализ проблем в области автоматизации бизнес-процессов отдела снабжения / С.С. Васильев, О.Ф. Абрамова, А.С. Адамов // Форум молодых ученых. – 2017. – № 5(9). – С. 382-392.
2. Фофилов Н.А. Исследование и анализ внутренних коммуникаций в организации / Н.А. Фофилов, О.Ф. Абрамова // Академия педагогических идей Новация. Серия: Студенческий научный вестник. – 2018. – № 6. – С. 114-118
3. Галушкин А.В. Методология разработки информационных систем. Москва: Лань, 2014.
4. Гендер И. Разработка информационных систем. Москва: Эксмо, 2013.
5. Глушков В.М. Разработка информационных систем. Москва: Наука, 2017.
6. Кузьмин А.П. Проектирование малого предприятия и его информационной системы. Москва: Независимая фирма "Консультант", 2016.

References

1. Vasiliev S.S. Research and analysis of problems in the field of automation of business processes in the supply department / S.S. Vasiliev, O.F. Abramova, A.S. Adamov // Forum of young scientists. – 2017. – No. 5(9). – P. 382-392.
2. Fofilov N.A. Research and analysis of internal communications in an organization / N.A. Fofilov, O.F. Abramova // Academy of Pedagogical Ideas Novation. Series: Student Scientific Bulletin. – 2018. – No. 6. – P. 114-118
3. Galushkin A.V. Methodology for developing information systems. Moscow: Lan, 2014.
4. Gender I. Development of information systems. Moscow: Eksmo, 2013.
5. Glushkov V.M. Development of information systems. Moscow: Nauka, 2017.
6. Kuzmin A.P. Design of a small enterprise and its information system. Moscow: Independent company "Consultant", 2016.

Постнов Всеволод Романович, студент кафедры «Информатика и технология программирования»
Абрамова Оксана Федоровна, доцент кафедры «Информатика и технология программирования»

Postnov Vsevolod Romanovich, Student of the Department of Informatics and Programming Technology
Abramova Oksana Fedorovna, Associate Professor of the Department of Informatics and Programming Technology

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРИНЯТИЕ РЕШЕНИЙ
ARTIFICIAL INTELLIGENCE AND DECISION MAKING

УДК 004.934.5 **DOI: 10.18413/2518-1092-2024-9-1-0-6**

Недопекин А.Е.
Жилин В.В.

СЕГМЕНТАЦИЯ ИЗОБРАЖЕНИЙ ДЛЯ ЗАДАЧИ ДИАГНОСТИКИ ПЛОСКО-ВАЛЬГУСНОЙ ДЕФОРМАЦИИ СТОП

Марийский государственный университет, пл. Ленина, 1, г. Йошкар-Ола, Республика Марий Эл, 424000, Россия

e-mail: agasfer911@yandex.ru, zhilin.valentin.72@gmail.com

Аннотация
Плоско-вальгусная деформация стопы (ПВДС) является распространенным состоянием, которое может привести к различным проблемам со здоровьем, таким как болевые синдромы и искривление позвоночника. Для эффективной диагностики при помощи программных средств требуется точная сегментация заднего отдела стопы на изображениях. В данном исследовании было проведено сравнение двух методов сегментации изображений: пороговая обработка и модель на основе сверточной нейронной сети (CNN), а именно архитектуры U-Net. Пороговая обработка, хотя и проста в реализации, не всегда эффективна на изображениях с неравномерной яркостью или шумами. В то время как модель на основе нейронной сети представляет собой более сложный, но более точный метод, способный адаптироваться к различным условиям изображений. Проведенное исследование показало, что модель на основе нейронной сети демонстрирует высокую точность сегментации заднего отдела стопы на изображениях различных пациентов. Точность этой модели составила 97% на тестовых данных и 95% на валидационных данных, что подтверждает ее эффективность. Модель на основе сверточной нейронной сети, такая как архитектура U-Net, представляет собой предпочтительный выбор для сегментации изображений заднего отдела стопы. Ее способность адаптироваться к различным условиям изображений, и высокая точность делают ее эффективным инструментом в клинической практике.
Ключевые слова: сегментация; нейронная сеть; пороговая обработка
Для цитирования: Недопекин А.Е., Жилин В.В. Сегментация изображений для задачи диагностики плоско-вальгусной деформации стоп // Научный результат. Информационные технологии. – Т.9, №1, 2024. – С. 46-57. DOI: 10.18413/2518-1092-2024-9-1-0-6

Nedopekin A.E.
Zhilin V.V.

IMAGE SEGMENTATION FOR THE TASK OF DIAGNOSING FLAT-VALGUS DEFORMITY OF THE FEET

Mari State University, Lenin Square, 1, Yoshkar-Ola, Republic of Mari El, 424000, Russia

e-mail: agasfer911@yandex.ru, zhilin.valentin.72@gmail.com

Abstract
Flat-valgus deformity of the foot is a common condition that can lead to various health problems such as pain syndromes and curvature of the spine. For effective diagnosis using software tools, accurate segmentation of the posterior part of the foot in the images is required. In this study, two image segmentation methods were compared: threshold processing and a model based on a convolutional neural network (CNN), namely the U-Net architecture. Threshold processing, although easy to implement, is not always effective on images with uneven brightness or noise. Whereas a neural network-based model is a more complex but more accurate method capable of adapting to different image conditions. The study showed that the neural network-based model

demonstrates high accuracy of posterior foot segmentation in images of various patients. The accuracy of this model was 97% on test data and 95% on validation data, which confirms its effectiveness. A convolutional neural network-based model, such as the U-Net architecture, is the preferred choice for image segmentation of the hindfoot. Its ability to adapt to different imaging conditions and high accuracy make it an effective tool in clinical practice.
Keywords: segmentation; neural network; threshold processing
For citation: Nedopekin A.E., Zhilin V.V. Image segmentation for the task of diagnosing flat-valgus deformity of the feet // Research result. Information technologies. – T. 9, №1, 2024. – P. 46-57. DOI: 10.18413/2518-1092-2024-9-1-0-6

ВВЕДЕНИЕ

Плоско-вальгусная деформация стопы (ПВДС) является распространенным состоянием, характеризующимся плоскостью или выпуклостью стопы. Стоит отметить, что ПВДС может быть, как самостоятельным состоянием, так и одним из симптомов других медицинских проблем, таких как плоскостопие, артрит или деформации костей [16]. Данная патология особенно часто встречается у взрослых, но не обходит стороной и детей разных возрастных групп [3, 6]. При деформации стопы снижается опорная и рессорная функции, что приводит к различным проблемам со здоровьем, таким как болевые синдромы в суставах, искривление позвоночника, нарушение осанки, частая усталость и утомленность [19].

По данным Всемирной Организации Здравоохранения (ВОЗ), более половины населения Земли имеет плоскостопие разной степени. На долю женщин приходится 90% заболеваемости плоскостопием. На территории России данная проблема у 60% населения [18].

Причиной развития деформации стопы являются наследственные болезни, слабость мышц и связок или их перенапряжение. Неправильно подобранная обувь также является одним из немаловажных факторов развития болезни. Большая подверженность женщин плоскостопию вызвана тем, что часто они с ранних лет носят обувь с высокими каблуками, в тот период, когда еще стопа окончательно не сформировалась [13].

Своевременная диагностика заболевания и принятие соответствующих мер имеют решающее значение для своевременного лечения ПВДС. Определение ПВДС на ранней стадии позволяет предпринять эффективные меры для предотвращения прогрессирования заболевания и минимизации его последствий для здоровья.

Одним из способов установления степени плоскостопия является, определение углов заднего отдела стоп. Суть заключается в проведении двух осей, первая ось обозначена как *hn*, а вторая ось *hk*, на рисунке 1. После того как оси были проведены, производится вычисление угла между *hn* и *hk*. Также угол без привязки к конкретным числовым диапазонам называют углом пронации [2]. Угол принято считать вальгусным или варусным, в зависимости от направления его отклонения от нормального положения. Если угол между осями *hn* и *hk* превышает 6°, то он считается вальгусным. Если угол меньше -6°, то его считают варусным [12]. Данный метод является важным инструментом для определения степени плоскостопия и позволяет оценить структурные особенности стопы для выбора наиболее эффективного лечения.

Целью данной работы является разработка программного решения (модели) для сегментации изображения с последующей подготовкой его для дальнейшей обработки. Конкретно, целью является подготовка изображения для использования в алгоритме автоматической диагностики плоско-вальгусной деформации стопы (ПВДС). Для достижения этой цели требуется провести сбор, анализ и обработку набора данных, а также реализовать программное решение (модель) для сегментации заднего отдела стопы.

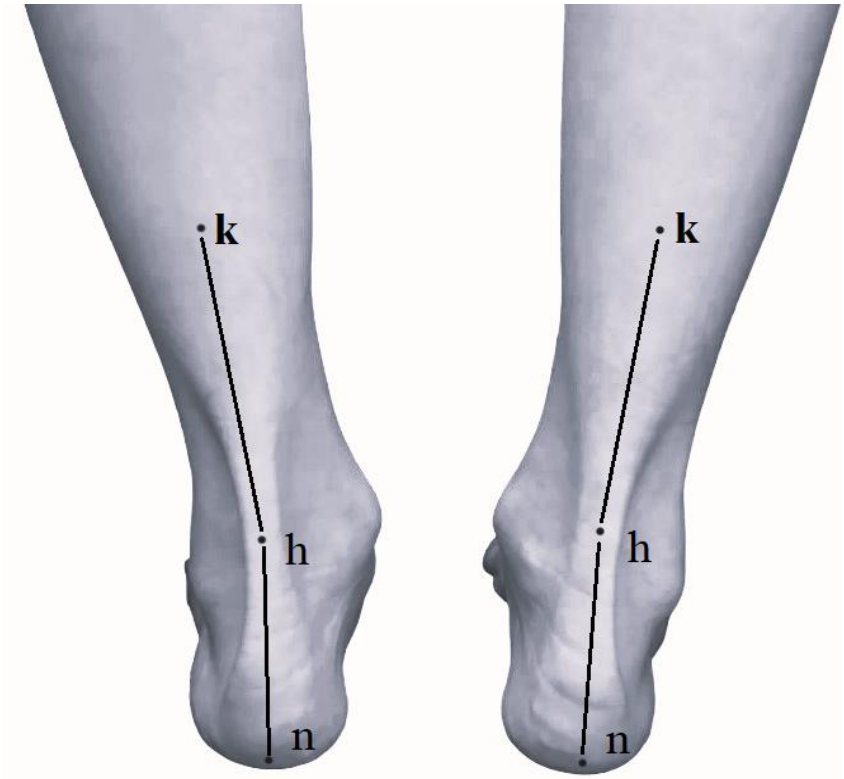


Рис. 1. Пример осей для определения угла пронации
Fig. 1. Example of axes for determining the pronation angle

Автоматизация процесса диагностики предполагает обработку фотоизображения заднего отдела стопы и вывод результата. Результат обработки включает в себя рассчитанный угол пронации, степень плоскостопия, а также исходное фотоизображение с размеченными точками и значениями углов.

Для минимизации ошибок необходимо провести обработку входящего изображения. Обработка включает в себя сегментацию изображения, что означает удаление заднего фона и выделение объекта интереса. В данном случае объектом является задний отдел стопы.

ОБЗОР МЕТОДОВ СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЙ

Сегментация изображения – это процесс выделения и классификации объектов интереса на изображении путем разделения его на несколько сегментов или регионов. Цель сегментации состоит в том, чтобы выделить объекты или области на изображении, которые представляют интерес для дальнейшего анализа или обработки [8].

Сегментация играет важную роль в обработке изображений и компьютерном зрении, поскольку позволяет автоматически выделять объекты, определять их контуры, а также проводить качественный анализ структуры и свойств объектов на изображении [12].

Существует несколько методов сегментации изображений, каждый из которых имеет свои преимущества и недостатки, и выбор конкретного метода зависит от характеристик изображений и целей исследования.

Пороговая обработка – это метод сегментации изображения, основанный на установлении порогового значения яркости или цвета, выше или ниже которого все пиксели изображения классифицируются как объекты или фон [9].

Принцип работы пороговой обработки заключается в том, что пиксели, значения яркости или цвета которых превышают заданный порог, считаются объектами интереса, в то время как остальные пиксели считаются фоновыми. Порог может быть выбран вручную или автоматически на основе характеристик изображения [17].

Основные преимущества пороговой обработки включают ее простоту и высокую скорость работы. Этот метод легко реализуется и быстро выполняется на практике. Он также обладает низкими требованиями к вычислительным ресурсам и может быть применен к изображениям в реальном времени.

Однако пороговая обработка может быть неэффективной в случае изображений с неравномерной яркостью или наличием шумов. В таких случаях выбор оптимального порога может быть затруднительным, что может привести к неправильной сегментации объектов или неполному выделению деталей на изображении.

Для улучшения эффективности пороговой обработки можно использовать различные методы предварительной обработки изображения, такие как сглаживание или фильтрация, для устранения шумов или улучшения равномерности яркости. Также можно применять адаптивную пороговую обработку, которая позволяет автоматически выбирать пороговые значения в зависимости от характеристик каждой области изображения [1].

В целом, пороговая обработка остается одним из наиболее простых и широко используемых методов сегментации изображений, несмотря на свои ограничения. Она находит применение во многих областях, включая медицинскую диагностику, компьютерное зрение, а также в обработке изображений и видео.

Методы, использующие машинное обучение, представляют собой класс алгоритмов сегментации, которые основаны на обучении моделей машинного обучения для автоматического выделения объектов на изображении. Эти методы отличаются от классических подходов к сегментации, таких как пороговая обработка или алгоритмы активных контуров [10], тем, что они способны обучаться на больших наборах, размеченных данных и адаптироваться к различным типам изображений и объектов.

Одним из наиболее популярных методов машинного обучения для сегментации изображений является сегментация с использованием сверточных нейронных сетей (CNN). CNN – это класс нейронных сетей, специально разработанный для обработки изображений. Они состоят из нескольких слоев, включая сверточные слои, слои подвыборки и полносвязанные слои, которые позволяют модели извлекать иерархические признаки из изображений и использовать их для точного выделения объектов [7].

Преимущества методов, использующих машинное обучение, включают их способность к обучению на больших объемах данных и адаптацию к различным типам изображений и объектов. Однако для их эффективной работы требуется наличие больших размеченных наборов данных для обучения моделей. Также эти методы могут потребовать значительных вычислительных ресурсов для обучения и прогнозирования моделей, особенно в случае использования CNN [11].

Одной из самых популярных архитектур для сегментации медицинских изображений является U-Net [4]. Он состоит из энкодера, который сжимает изображение и извлекает признаки, и декодера, который восстанавливает размер изображения и производит пиксельную классификацию. U-Net хорошо работает с небольшими объемами данных и имеет хорошую способность к обучению на малом количестве размеченных изображений [15].

Каждый из этих методов имеет свои особенности и может быть применен в зависимости от конкретной задачи и требований к точности и скорости обработки данных. Важно выбрать подходящий метод сегментации, который обеспечит наиболее качественный результат.

АНАЛИЗ И ПОДГОТОВКА НАБОРА ДАННЫХ

Для обучения моделей сегментации изображений требуются размеченные наборы данных, состоящие из пар изображений и соответствующих им масок сегментации. Изображения могут быть различного разрешения и содержать объекты разных размеров и форм. Чем больше и разнообразнее набор данных, тем лучше модель сможет обучиться и обобщить свои знания на новые изображения. Также важно провести предварительную обработку данных, такую как изменение размера

изображений, нормализация и аугментация данных, чтобы улучшить качество обучения и повысить устойчивость модели.

Необработанный (или исходный) набор данных состоит из 355 фотоизображений. Изображение содержит задний отдел стоп, пациентов разной возрастной категории. Пример изображен на рисунке 2.

Данные были получены в рамках исследовательской работы по диагностике ПВДС. Среди исходных данных присутствуют изображения заднего отдела стопы как здоровых пациентов, так и пациентов с ярков выраженной деформацией стопы и с большим отклонением от нормального положения угла.

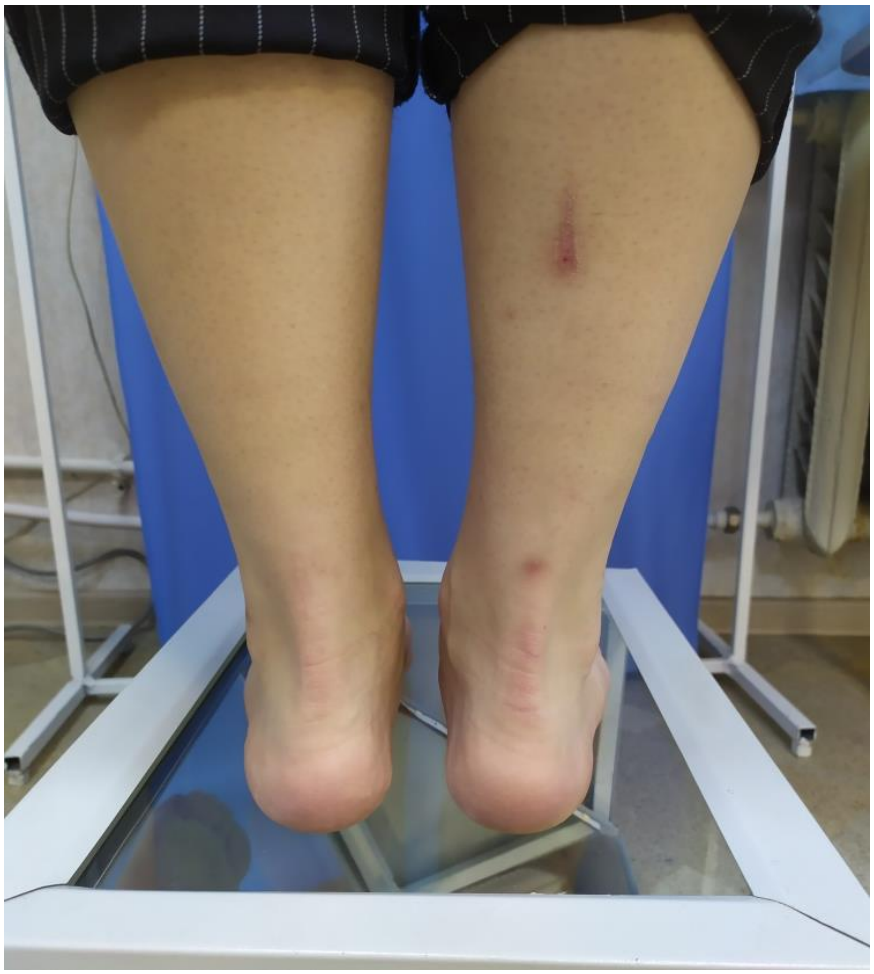


Рис. 2. Пример исходного изображения
Fig. 2. An example of the original image

Если в случае обработки данных традиционными алгоритмами компьютерного зрения, количество данных несущественно, то для обучения модели нейронной сети для сегментации изображения на архитектуре U-Net, имеющееся количество данных является недостаточным.

Одним из вариантов решения данной проблемы является аугментация данных. Аугментация данных – это процесс создания новых обучающих примеров путем применения различных трансформаций к существующим изображениям. Применение аугментации данных позволяет создать больше разнообразных обучающих примеров из ограниченного набора данных, что может значительно улучшить качество и обобщающую способность модели [5]. Однако при выборе конкретных трансформаций для аугментации данных важно учитывать особенности задачи и требования к конечной модели.

В рамках обучения модели нейронной сети для сегментации изображений на архитектуре U-Net были проведены различные трансформации данных. Схематичное представление изображено на рисунке 3.

Рис. 3. Схема аугментации изображения
Fig. 3. Pipeline of Image Augmentation

Эти трансформации включали:

1. Зашумление: Добавление случайного шума к изображениям, чтобы модель могла обучаться на изображениях с различными уровнями шума, что помогает ей стать более устойчивой к шуму в реальных условиях.
2. Размытие: Применение различных фильтров размытия к изображениям, чтобы модель могла обучаться на изображениях с различными уровнями резкости, что помогает ей лучше обнаруживать границы объектов.
3. Изменение яркости и контрастности: Изменение яркости и контрастности изображений, чтобы модель могла обучаться на изображениях с различными уровнями освещенности и контраста.
4. Отражение: Применение отражений по горизонтали или вертикали к изображениям, чтобы модель могла обучаться на изображениях с различными зеркальными отражениями.
5. Повороты: Повороты изображений на различные углы, чтобы модель могла обучаться на изображениях с различными ориентациями объектов.
6. Масштабирование: Увеличение или уменьшение размера изображений, чтобы модель могла обучаться на изображениях с различными масштабами объектов.

Применение методов аугментации данных позволило увеличить количество доступных данных до 5 тысяч изображений. Это значительное увеличение объема данных способствует более эффективному обучению модели нейронной сети для сегментации изображений стопы на архитектуре U-Net. Большее количество разнообразных данных помогает модели лучше обобщить особенности объектов и сделать более точные прогнозы при сегментации новых изображений.

Для обучения модели помимо аугментации данных требуется провести аннотацию, то есть создать маски сегментации, которые точно определяют задний отдел стопы на каждом изображении. Эти маски затем используются в качестве размеченных данных для обучения нейронной сети. Процесс аннотации данных включает в себя создание точных контуров объектов

на изображениях, что играет ключевую роль в обучении модели и повышении ее эффективности при сегментации. Для этой цели был использован сервис CVAT.ai. Результат аннотации изображен на рисунке 4, представляет из себя бинарную маску исходного изображения.

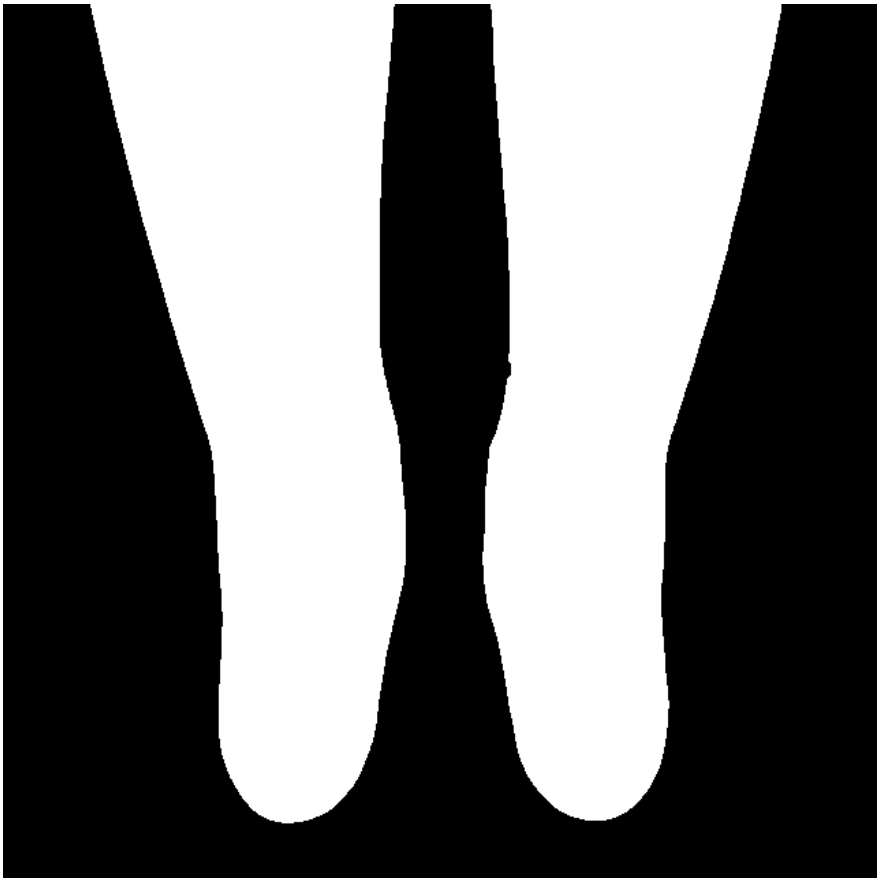


Рис. 4. Результат аннотации исходного изображения
Fig. 4. The result of the annotation of the original image

Для реализации сегментации заднего отдела стопы на изображениях была использована модель на основе архитектуры U-Net. Модель состоит из восьми сверточных слоев, включая слои субдискретизации, пространственного отсева и транспонированных сверток. Активация LeakyReLU (Rectified Linear Unit) применяется для большинства слоев, за исключением последнего, где используется сигмоидальная функция активации для получения бинарных масок сегментации. Для обучения модели был использован оптимизатор Adam и функция потерь бинарная кросс энтропия.

Входной слой принимает изображения заднего отдела стопы, а выходной слой генерирует соответствующие маски сегментации. Обучение проводилось в среде Google Colab, что обеспечило доступ к вычислительным ресурсам в облаке и ускорило процесс обучения. Для обучения модели были использованы следующие гиперпараметры: размер изображений составлял 640x640 пикселей, при этом тестовая выборка составляла 85%, а валидационная – 15%. Размер пакета данных был установлен на уровне 64, и число эпох составило 25. Эти гиперпараметры были настроены для оптимального обучения модели сегментации заднего отдела стопы на основе архитектуры U-Net.

АНАЛИЗ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ РАЗЛИЧНЫХ МЕТОДОВ СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЙ

В результате обучения данная модель показала высокую точность сегментации, достигнув значений 97% на тестовых данных и 95% на валидационных данных, что подтверждает ее

эффективность в выделении интересующих объектов, в данном случае заднего отдела стопы. Точность сегментации была вычислена с использованием формулы (1), где TP (True Positive) – количество пикселей, которые были правильно классифицированы моделью как принадлежащие объекту интереса (задний отдел стопы), а FP (False Positive) – количество пикселей, которые модель неправильно классифицировала как принадлежащие объекту интереса при этом они к нему не относятся.

$$Accuracy = \frac{TP}{TP+FP} \quad (1)$$

Для достижения положительных результатов с помощью пороговой обработки требуется правильно выбрать пороговое значение яркости или цвета, учитывая особенности изображения и цели сегментации. Кроме того, может потребоваться предварительная обработка изображения, такая как сглаживание или фильтрация, для уменьшения шумов или улучшения равномерности яркости. Но даже после ряда обработок желаемый результат едва достигается. При использовании пороговой обработки в данном случае было достигнуто приблизительно 82% точности. Для расчета точности, также была применена формула (1).

Пороговое значение для сегментации было выбрано адаптивно с использованием метода Отцу (Otsu), реализованного в библиотеке OpenCV. Этот метод автоматически определяет оптимальный порог для бинаризации изображения, учитывая его гистограмму интенсивности пикселей в градациях серого.

Проанализировав результаты, полученные с помощью пороговой обработки и нейронной сети, можно выделить их основные отличия и преимущества. Пороговая обработка, хотя и проста в реализации и имеет высокую скорость работы, часто оказывается неэффективной на изображениях с неравномерной яркостью или шумами, что может привести к недостаточной точности сегментации. Результат пороговой обработки изображен на рисунке 5.

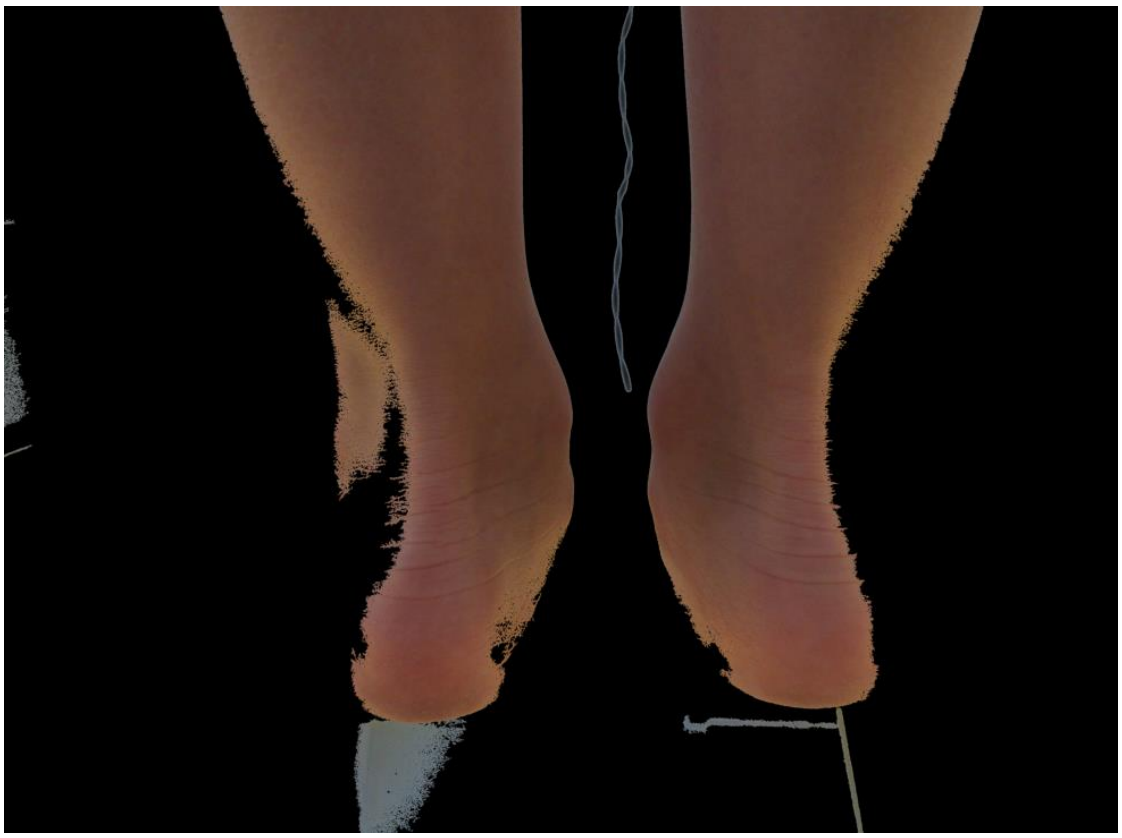


Рис. 5. Результат пороговой обработки
Fig. 5. The result of threshold processing

В то время как пороговая обработка имеет свои ограничения, модель на основе нейронной сети продемонстрировала хорошие результаты. Результат выполнения изображен на рисунке 6. Оно содержит тестовое изображение, две маски (soft и binary) и изображение с наложенной маской.

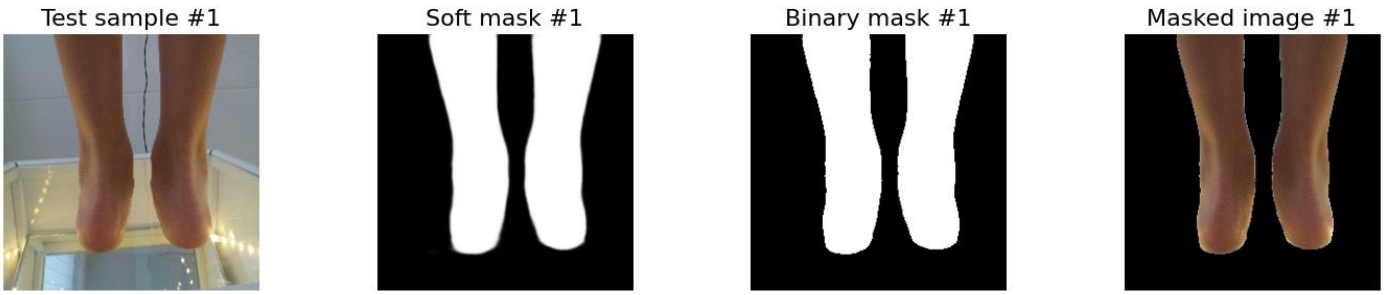


Рис. 6. Результат сегментации
Fig. 6. The result of segmentation

Первая маска (soft mask), полученная с помощью нейронной сети, представляет собой мягкую маску, где каждый пиксель имеет значение от 0 до 1, отражающее степень уверенности модели в том, что данный пиксель принадлежит объекту интереса. Это позволяет учитывать плавные переходы и размытость в выделении объектов.

Вторая маска (binary mask) является бинарной маской, где каждый пиксель может быть представлен только в двух состояниях: 0 или 1. Значения 1 обозначают пиксели, принадлежащие объекту интереса, в то время как значения 0 обозначают пиксели фона. Эта маска обеспечивает более четкое разделение между объектом и фоном, что полезно при определении точных контуров объектов для последующего анализа.

Изображение с наложенной маской представляет собой результат наложения бинарной маски на тестовое изображение. Это позволяет визуализировать, какие части изображения были выделены как объект интереса моделью на основе нейронной сети.

Полученные результаты на новых данных свидетельствует о высокой эффективности модели в точной сегментации заднего отдела стопы на изображениях различных пациентов. Она успешно справилась с разнообразными условиями освещения, шумами и другими искажениями, что подтверждает ее способность адаптироваться к различным типам изображений и объектов. Такие высокие показатели точности делают модель на основе нейронной сети предпочтительным выбором для сегментации.

ЗАКЛЮЧЕНИЕ

В представленном исследовании было проведено сравнение методов пороговой и нейросетевой сегментации применительно к изображениям заднего отдела стоп. Пороговая обработка, хотя и обладает простотой и высокой скоростью работы, часто неэффективна на изображениях с неравномерной яркостью или шумами, в то время как модель на основе нейронной сети продемонстрировала высокую точность сегментации заднего отдела стопы на изображениях различных пациентов, достигнув точности в 97% на тестовых данных и 95% на валидационных данных. Это подтверждает превосходство модели нейронной сети в обработке изображений с различными условиями освещения и шумами, делая ее предпочтительным выбором для сегментации.

Список литературы

1. Балсаидов А.Ш. Предварительная обработка изображений для наилучшего распознавания текста // Компьютерная обработка тюркских языков. TURKLANG 2022: ТРУДЫ X Международной конференции, Нур-Султан, 16–18 июня 2022 года. – Нур-Султан: ИП «Булатов А.Ж.», 2022. – С. 84-91. – EDN WTODZA.

2. Боровлева А.В., Дубровин Г.М. Результаты лечения мобильной плоско-вальгусной деформации стоп у детей // Молодежь - практическому здравоохранению: XIII Всероссийская с международным участием научная конференция студентов и молодых ученых-медиков, Иваново, 13 ноября 2019 года. – Иваново: Ивановская государственная медицинская академия, 2019. – С. 164-168. – EDN FMKDYN.

3. Борзунов А.В. Распространенность плоскостопия у детей и взаимосвязь плоскостопия и гипермобильного синдрома // Вестник физиотерапии и курортологии. – 2015. – Т. 21, № 2. – С. 106а-106. – EDN YRGSAT.

4. Бруттан Ю.В., Новиков А. Исследование нейронных сетей для анализа медицинских изображений // Вестник Псковского государственного университета. Серия: Технические науки. – 2020. – № 11. – С. 49-54. – EDN JPRRRZ.

5. Дементьев В.Е., Андриянов Н.А., Васильев К.К. Использование аугментации изображений и реализация дважды стохастических моделей для повышения эффективности нейросетевых алгоритмов распознавания образов в сверточных нейронных сетях // Системы синхронизации, формирования и обработки сигналов. – 2020. – Т. 11, № 5. – С. 15-22. – EDN NVNEJT.

6. Дубровин Г.М., Бакурская Е.С. Особенности скрининговой оценки мобильной плоско-вальгусной деформации стоп и способ ее коррекции у детей // Весенние дни ортопедии: Тезисы Международного конгресса, Москва, 01–02 марта 2019 года / Под редакцией Н.В. Загороднего. – Москва: Российский университет дружбы народов (РУДН), 2019. – С. 66-69. – EDN XTCLHO.

7. Дычков И.Н. Сверточные нейронные сети // Тенденции развития науки и образования. – 2021. – № 73-1. – С. 38-41. – DOI 10.18411/lj-05-2021-08. – EDN MQYWDB.2

8. Купоросов А.А. Сегментация изображения на основе метода оптимизация роя частиц // Информатика, управляющие системы, математическое и компьютерное моделирование (ИУСМКМ-2019): Материалы студенческой секции X Международной научно-технической конференции в рамках V Международного Научного форума Донецкой Народной Республики, Донецк, 22–24 мая 2019 года. – Донецк: Донецкий национальный технический университет, 2019. – С. 262-266. – EDN MEUIHM.

9. Метод пороговой сегментации изображений морских судов / Ш.С. Фахми, С.А. Селиверстов, В.В. Вислогузов, В.В. Крымский // Морские интеллектуальные технологии. – 2019. – № 4-2(46). – С. 69-78. – EDN JJWOZE.

10. Модель обучаемого активного контура для сегментации гистологических изображений / А.В. Хвостиков, А.С. Крылов, И.А. Михайлов, П.Г. Мальков // Научная визуализация. – 2019. – Т. 11, № 3. – С. 64-75. – EDN WKQNJU.

11. Муаль М.Н.Б., Козырев Д.В. Применение сверточных нейронных сетей для обнаружения и распознавания изображений на основе самописного генератора // Современные информационные технологии и ИТ-образование. – 2022. – Т. 18, № 3. – С. 507-515. – DOI 10.25559/SITITO.18.202203.507-515.

12. Ортопедическая диагностика: Руководство-справочник / Маркс В.О. Минск: Наука и техника; 1978. 512 с.

13. Самойлова Р.С., Самойлов С.П., Самойлова А.С. Стопа - фундамент тела // Авиценна. – 2018. – № 16. – С. 35-38. – EDN YSWFZU.

14. Сегментация изображений микрообъектов / В.С. Пятлин, Е.И. Лойко, В.Ю. Цвирко, Д.С. Дулевич // Научные горизонты. – 2019. – № 4(20). – С. 187-192. – EDN GHXEBE.

15. Система распознавания повреждений металлических конструкций / В.Е. Дементьев, Р.А. Савинов, М.Н. Суетин, А.Г. Подлобошников // Автоматизация процессов управления. – 2021. – № 2(64). – С. 40-45. – DOI 10.35752/1991-2927-2021-2-64-40-45.

16. Теплов П.А. От плоскостопия к здоровой стопе // Глобальные проблемы современности. – 2022. – Т. 3, № 2. – С. 46-48. – EDN JDNOGZ.

17. Тимофеев Б.С., Мотыко А.А. Адаптивная локальная бинаризация изображений // Телевидение: передача и обработка изображений. – 2016. – Т. 1. – С. 109-114. – EDN XINNZH.

18. Чемеричина А.А. Профилактика нарушений опорно-двигательного аппарата у детей и подростков в школьных образовательных учреждениях // Молодежь и наука: шаг к успеху: Сборник научных статей 6-й Всероссийской научной конференции перспективных разработок молодых ученых, в 3-х томах, Курск, 22–23 марта 2022 года. Том 2. – Курск: Юго-Западный государственный университет, 2022. – С. 426-430. – EDN PGONXE.

19. Шевелева Н.И., Дубовихин А.А., Минбаева Л.С. Проблема плоскостопия на современном этапе // Вопросы практической педиатрии. – 2020. – Т. 15, № 2. – С. 68-74. – DOI 10.20953/1817-7646-2020-2-68-74.

References

1. Balsaidov A.S. Preliminary image processing for the best text recognition // Computer processing of Turkic languages. TURKLANG 2022: PROCEEDINGS OF the X International Conference, Nur Sultan, June 16-18, 2022. – Nur Sultan: IP Bulatov A.Zh., 2022. – pp. 84-91. – EDN WTODZA.

2. Borovleva A.V., Dubrovin G.M. Results of treatment of mobile flat-valgus deformity of feet in children // Youth - practical healthcare: XIII All-Russian scientific conference of students and young medical scientists with international participation, Ivanovo, November 13, 2019. – Ivanovo: Ivanovo State Medical Academy, 2019. – pp. 164-168. – EDN FMKDYN.

3. Borzunov A.V. The prevalence of flat feet in children and the relationship between flat feet and hypermobility syndrome // Bulletin of Physiotherapy and Balneology. - 2015. – vol. 21, No. 2. – pp. 106a-106. – EDN YRGSAT.

4. Bruttan Yu.V., Novikov A. The study of neural networks for the analysis of medical images // Bulletin of the Pskov State University. Series: Technical Sciences. - 2020. – No. 11. – pp. 49-54. – EDN JPRRRZ.

5. Dementiev V.E., Andrianov N.A., Vasiliev K.K. The use of image augmentation and the implementation of doubly stochastic models to improve the efficiency of neural network algorithms for pattern recognition in convolutional neural networks // Systems of synchronization, signal generation and processing. – 2020. – Vol. 11, No. 5. – pp. 15-22. – EDN NVNEJT.

6. Dubrovin G.M., Bakurskaya E.S. Features of screening assessment of mobile flat-valgus deformity of the feet and the method of its correction in children // Spring Days of Orthopedics: Abstracts of the International Congress, Moscow, March 01-02, 2019 / Edited by N.V. Zagorodny. – Moscow: Peoples' Friendship University of Russia (RUDN), 2019. – pp. 66-69. – EDN XTCLHO.

7. Dychkov I.N. Convolutional neural networks // Trends in the development of science and education. – 2021. – No. 73-1. – pp. 38-41. – DOI 10.18411/lj-05-2021-08. – EDN MQYWDB.2

8. Kuporosov A.A. Image segmentation based on the particle swarm optimization method // Informatics, control systems, mathematical and computer modeling (IUSMKM-2019): Materials of the student section of the X International Scientific and Technical Conference within the framework of the V International Scientific Forum of the Donetsk People's Republic, Donetsk, May 22-24, 2019. – Donetsk: Donetsk National Technical University, 2019. – pp. 262-266. – EDN MEUIHM.

9. The method of threshold segmentation of images of marine vessels / S.S. Fahmi, S.A. Seliverstov, V.V. Visloguzov, V.V. Krymsky // Marine intelligent technologies. – 2019. – № 4-2(46). – Pp. 69-78. – EDN JJWOZE.

10. The model of the trained active contour for segmentation of histological images / A.V. Khvostikov, A.S. Krylov, I.A. Mikhailov, P.G. Malkov // Scientific visualization. – 2019. – Vol. 11, No. 3. – pp. 64-75. – EDN WKQNJU.

11. Mual M.N.B., Kozyrev D.V. Application of convolutional neural networks for image detection and recognition based on a self-written generator // Modern information technologies and IT education. – 2022. – Vol. 18, No. 3. – pp. 507-515. – DOI 10.25559/SITITO.18.202203.507-515.

12. Orthopedic diagnostics: Handbook / Marx V.O. Minsk: Science and technology; 1978. 512 p.

13. Samoilova R.S., Samoilov S.P., Samoilova A.S. Foot – the foundation of the body // Avicenna. – 2018. – No. 16. – pp. 35-38. – EDN YSWFZU.

14. Segmentation of images of microobjects / V.S. Pyatlin, E.I. Loiko, V.Yu. Tsvirko, D.S. Dulevich // Scientific horizons. – 2019. – № 4(20). – Pp. 187-192. – EDN GHXEBE.

15. The system for recognizing damage to metal structures / V.E. Dementiev, R.A. Savinov, M.N. Suetin, A.G. Podloboshnikov // Automation of control processes. – 2021. – № 2(64). – Pp. 40-45. – DOI 10.35752/1991-2927-2021-2-64-40-45.

16. Teplov P.A. From flat feet to a healthy foot // Global problems of modernity. – 2022. – Vol. 3, No. 2. – pp. 46-48. – EDN JDNOGZ.

17. Timofeev B.S., Motyko A.A. Adaptive local image binarization // Television: transmission and image processing. – 2016. – Vol. 1. – pp. 109-114. – EDN XINNZH.

18. Chemerichina A.A. Prevention of disorders of the musculoskeletal system in children and adolescents in school educational institutions // Youth and science: a step to success: A collection of scientific articles of the 6th All-Russian Scientific Conference of promising developments of young scientists, in 3 volumes, Kursk, March 22-23, 2022. Volume 2. – Kursk: Southwestern State University, 2022. – pp. 426-430. – EDN PGONXE.

19. Sheveleva N.I., Dubovikhin A.A., Minbayeva L.S. The problem of flat feet at the present stage // Questions of practical pediatrics. – 2020. – Vol. 15, No. 2. – pp. 68-74. – DOI 10.20953/1817-7646-2020-2-68-74.

Недопекин Александр Евгеньевич, кандидат физико-математических наук, доцент, доцент кафедры прикладной математики и информатики
Жилин Валентин Валерьевич, магистрант

Nedopekin Alexander Evgenievich, Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Applied Mathematics and Computer Science
Zhilin Valentin Valeryevich, master's degree

УДК 004.855.5 **DOI: 10.18413/2518-1092-2024-9-1-0-7**

Коржавых В.В.

СРАВНЕНИЕ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ НА ПРИМЕРЕ ПРОГНОЗИРОВАНИЯ СРЕДНЕМЕСЯЧНОГО ПОТРЕБЛЕНИЯ ЭЛЕКТРОЭНЕРГИИ ИНТЕРВАЛЬНЫХ ПРИБОРОВ УЧЕТА ПОТРЕБИТЕЛЕЙ

Филиал Публичного акционерного общества «Россети Центр» – «Белгородэнерго»,
Валуйский район электрических сетей,
ул. Суржикова, 114, г. Валуйки, Белгородская обл., 309990, Россия

e-mail: Korzhavyh.VV@mrsk-1.ru

Аннотация
Поиск и снижение потерь электроэнергии – одно из ключевых направлений деятельности сетевых организаций для улучшения финансовых результатов. Прогнозирование потребления электроэнергии на основе большого количества критериев и сравнение с фактическими данными является преимущественным способом обнаружения потерь. Однако, данный процесс требует высокой доли автоматизации. Поэтому, для решения этой задачи в настоящей работе рассмотрено применение трех алгоритмов машинного обучения, а также выполнено сравнение их эффективности. Автором сформирована обучающая выборка из базы данных Валуйского района электрических сетей на основе данных приборов учета, входящих в систему АИИСКУЭ, а также проведены эксперименты по реализации на ней следующий алгоритмов: k-ближайших соседей, линейной регрессии и случайного леса. Для сравнения полученных моделей автором были использованы такие показатели эффективности как среднеквадратичная ошибка (MSE), абсолютная средняя ошибка (MAE) и коэффициент детерминации (R^2). Результаты эксперимента показали наибольшую эффективность метода случайного леса в сравнении с остальными рассматриваемыми алгоритмами.
Ключевые слова: машинное обучение; потери электроэнергии; алгоритм k-ближайших соседей; линейная регрессия; случайный лес; среднеквадратичная ошибка; средняя абсолютная ошибка; коэффициент детерминации
Для цитирования: Коржавых В.В. Сравнение эффективности алгоритмов машинного обучения на примере прогнозирования среднемесячного потребления электроэнергии интервальных приборов учета потребителей // Научный результат. Информационные технологии. – Т.9, №1, 2024. – С. 58-73. DOI: 10.18413/2518-1092-2024-9-1-0-7

Korzhavykh V.V.

COMPARISON OF THE EFFICIENCY OF MACHINE LEARNING ALGORITHMS BY THE EXAMPLE OF FORECASTING THE AVERAGE ELECTRICITY CONSUMPTION OF INTEGRATED CONSUMER METERING DEVICES

Branch of the Public Joint Stock Company “Rosseti Center” – “Belgorodenergo”,
Valuysky district of electrical networks,
114 Surzhikova st., Valuiki, Belgorod region, 309990, Russia

e-mail: Korzhavyh.VV@mrsk-1.ru

Abstract
Finding and reducing electricity losses is one of the key activities of network organizations to improve financial results. Forecasting based on a large number of criteria and comparing with actual electricity consumption is the preferred way to detect losses. However, this process requires a high degree of automation. Therefore, to solve this problem, this paper considers the use of three machine learning algorithms, as well as a comparison of their effectiveness. The author formed a

training sample from the database of one of the districts of electrical networks, and also conducted experiments on the implementation of the following algorithms on it: k-nearest neighbors, linear regression and random forest. To compare the resulting models, the author used such performance indicators as mean square error (MSE), absolute mean error (MAE) and coefficient of determination (R^2). The results of the experiment showed the greatest efficiency of the random forest method in comparison with other considered algorithms.
Keywords: machine learning; power loss; k-nearest neighbors' algorithm; linear regression; random forest; mean square error; mean absolute error; coefficient of determination
For citation: Korzhavykh V.V. Comparison of the efficiency of machine learning algorithms by the example of forecasting the average electricity consumption of integrated consumer metering devices // Research result. Information technologies. – T.9, №1, 2024. – P. 58-73. DOI: 10.18413/2518-1092-2024-9-1-0-7

ВВЕДЕНИЕ

Фактические (отчетные) потери электроэнергии – разность между электроэнергией, поступившей в сеть, и электроэнергией, отпущенной потребителям, определяемая по данным системы учета поступления и полезного отпуска электроэнергии [5]. Фактические потери разделяются на техническую и коммерческую составляющую. Снижение технической составляющей – модернизация оборудования, а коммерческой – повышение "платежной дисциплины" контрагентов, пресечение "хищений" электроэнергии посредством анализа и контроля за потреблением. Решения задачи поиска и оптимизации потерь электрической энергии является наиболее актуальной проблемой не только в России, но и во всем мире. Статистика Международного энергетического агентства (International Energy Agency, IEA) говорит о том, что страны с развитой экономикой имеют уровень потерь не более 8–10%, а развивающиеся страны – от 10% до 30% [9]. По данным ежегодного исследования Emerging Markets Smart Grid: Outlook, проводимого компанией Northeast Group, LLC, 30% от $89 млрд потерь приходилось на три страны: Индия ($16,2 млрд), Бразилия ($10,5 млрд) и Россия ($5,1 млрд) [10]. Если снижение технической составляющие потерь – это дорогостоящий процесс, требующий значительных инвестиций и дальний горизонт окупаемости, то работа над коммерческими потерями в большей части сводиться к анализу различных критериев потребления электроэнергии из баз данных сетевой организации и формированию адресных списков для проведения проверок системы учета, снятия контрольных показаний и т.д. Качественное проведение анализа и непосредственной работы приводит к существенному снижению коммерческой составляющей потерь. Однако особенности законодательства Российской Федерации в отрасли электроэнергетики, ограниченное количество человеческих ресурсов сетевых компаний и растущее число аналитических критериев способствует поиску новых подходов и механизмов для решения вышеуказанной задачи. Внедрение информационных технологий - процессов, использующих совокупность средств и методов сбора, обработки, накопления и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса, явления, информационного продукта [6] становиться необходимостью в современных условиях работы. Часто анализ потребления электроэнергии сводится к установлению объемов в кВтч (киловатт-часах) и сравнению его с текущим потреблением. Другими словами – составление прогноза потребления электроэнергии. Технологией, успешно справляющийся с решением такого рода задач является подраздел искусственного интеллекта, называющийся машинным обучением. Смысл машинного обучения состоит в использовании нужных признаков для построения моделей, подходящих для решения правильно поставленных задач. Признаки определяют "язык", на котором описываются объекты предметной области. Задача – это абстрактное представление проблемы с участием объектов предметной области, которую необходимо решить. Модель – результат машинного обучения, примененного к обучающим данным. Можно сказать, что модели обеспечивают разнообразие предмета машинного обучения, тогда как задачи и признаки придают ему единство [15]. Методы обучения можно разделить на обучение с учителем и без учителя. Обучение без учителя подходит для разделения данных на группы имеющие схожие характеристики или свойства (задача

кластеризации). Обучение с учителем предполагает какой-либо обучающий набор размеченных данных, например среднемесячное потребление приборов учета входящих в АИИСКУЭ к площади помещения домовладения. На его основе формируется прогноз потребления электроэнергии. (задача регрессии). Полученную модель можно использовать для прогноза потребления приборов учета, не входящих в АИИСКУЭ, для выявления наибольшей разницы прогнозных-фактических значений среднемесячного потребления, по результатам которых бригады направляются для проведения проверок по адресной части. Разумеется, модель, основанная только на одном критерии, не сможет претендовать на высокую точность прогноза, поэтому для ее формирования нужно большее их количество. Для оценки качества модели и сравнения ее с другими моделями машинного обучения используются специальные метрики. В рамках данного исследования выбраны такие метрики как среднеквадратичная ошибка (MSE), формула которой приведена ниже:

$$MSE(y_i, \widehat{y_i}) = \frac{1}{N}\sum_{i=1}^{n}(y_i - \widehat{y_i})^2$$

где, y_i – фактическое значение переменной, $\widehat{y_i}$ – прогнозируемое значение переменной, n – размер выборки данных. Если не возводить в квадрат разницу между прогнозируемым и фактическим значением переменной, а взять ее по модулю, то получим метрику абсолютной средней ошибки (MAE):

$$MAE(y_i, \widehat{y_i}) = \frac{1}{N}\sum_{i=1}^{n}|y_i - \widehat{y_i}|$$

MAE является более наглядной из-за линейности шкалы оценки. В целом, данные виды метрик зависимы от шкалы измерений [18] и обладают чувствительностью к выбросам данных [19]. Таким образом, такой способ подготовки данных перед моделированием как нормализация, является обязательным. Для оценки “адекватности” модели, соответствии прогнозных данных модели фактическим, используется коэффициент детерминации:

$$R^2 = 1 - \frac{(RMSE)^2}{D}$$

где, $RMSE$– метрика, равная квадратному корню из MSE, D– дисперсия. После раскрытия формул:

$$R^2 = 1 - \frac{\sum_{i=1}^{n}(y_i - \widehat{y_i})^2}{\sum_{i=1}^{n}(y_i - \langle y \rangle)^2}$$

где, $\langle y \rangle$– среднее, прогнозируемое значение.

Подытожив все вышесказанное, стало возможным определить цель данного исследования – подготовить набор данных сетевой организации, описать и применить к ней алгоритмы машинного обучения с учителем, сравнить полученные результаты с помощью метрик качества MSE, MAE и коэффициента детерминации.

ИССЛЕДУЕМЫЕ ДАННЫЕ

В качестве исходных взяты данные из базы SAP RT2 Валуйского района электрических сетей о приборах учета потребителей – физических лиц. Формат данных – файл MS Excel расширения xlsx. Внешний представлен на рисунке 1.

Договор	Статус "сезонного потребителя"	Место прибора	Количество проживающих	Наличие электроотопительной установки	Наличие электроводонагревателя	Количество комнат	Класс точности	Фазность	Разрядность	Максимальная мощность точки поставки	Площадь	Количество КП	Среднее 2019	Среднее 2020	Среднее 2021	Среднее 2022
486226	Не определен	в квартире (доме)	2	0	0	4	1	1	5,1	3.000	90	9	66	64	61	18
486242	Не определен	в квартире (доме)	4	0	0	4	2	1	5,1	3.000	89	12	143	192	300	243
486251	Не определен	в квартире (доме)	2	0	0	4	2	1	5,1	3.000	58	10	183	177	181	175
486264	Не определен	в квартире (доме)	2	0	0	3	1	1	5,1	3.000	42	10	115	93	189	206
486275	Дачники	в квартире (доме)	1	0	0	4	1	1	6,1	3.000	72	9	45	62	99	82
486296	Не определен	на фасаде	5	0	0	5	1	1	5,1	3.000	88	9	99	84	186	204
486309	Не определен	в квартире (доме)	1	0	0	3	1	1	6,1	3.000	37	10	94	99	82	97
486321	Не определен	в квартире (доме)	4	0	0	4	1	1	5,1	3.000	103	9	58	74	399	381
486326	Не определен	в квартире (доме)	1	0	0	4	1	1	5,1	3.000	49	9	99	94	73	59
486356	Не определен	в квартире (доме)	5	0	0	4	1	1	5,1	3.000	100	9	59	112	259	188
486363	Не определен	в квартире (доме)	3	0	0	4	1	1	6,1	3.000	56	10	421	471	212	210
486423	Не определен	в квартире (доме)	3	0	0	4	2	1	5,1	3.000	56	9	224	273	307	234
486431	Не жилой	в хозпостройке (гараже)	2	0	0	6	1	3	6	0.000	250	11	372	404	1940	1713
486526	Хоз. постр	в квартире (доме)	2	0	0	4	1	3	5,1	3.000	92	10	91	88	94	98
486553	Не определен	в квартире (доме)	4	0	0	4	1	1	5,1	3.000	56	12	214	196	230	204
486579	Не определен	в хозпостройке (гараже)	4	0	0	4	1	3	5,1	3.000	67,4	11	215	465	223	157

Рис. 1. Набор исследуемых данных
Fig. 1. Data set under study

Критерий Договор является уникальным идентификатором для последующего объединения прогноза с адресной частью контрагента. Статус сезонности потребителя является категориальной переменной, определяющей статус домовладения. К примеру, статус «Хоз. постр.» говорит о том, что домовладение является гаражом, а не жилым домом. Место прибора – определяет физическое местоположение прибора учета. Наличие электроотопительной установки и электроводагревателя являются булевыми переменными. Остальные критерии достаточно наглядны. Первоначальный анализ набора данных представлен в таблице 1.

Таблица 1

Набор исследуемых данных

Table 1

Data set under study

№	Критерий	Тип данных	Диапазон значений
1	Статус "сезонного потребителя"	Текстовый	
2	Место прибора	Текстовый	
3	Количество проживающих	Числовой	0…9
4	Наличие электроотопительной установки	Булев	0,1
5	Наличие электроводонагревателя	Булев	0,1
6	Количество комнат	Числовой	0…96
7	Класс точности	Числовой	0…2,5
8	Фазность	Булев	1,3
9	Разрядность	Числовой	0…7
10	Максимальная мощность точки поставки	Числовой	3…15
11	Площадь	Числовой	3..327
12	Количество КП	Числовой	0…26
13	Среднее 2019	Числовой	0…2452
14	Среднее 2020	Числовой	0…1940
15	Среднее 2021	Числовой	0…3682
16	Среднее 2022	Числовой	0…1713

Так как критерии 1,2 имеют текстовый тип данных, то необходимо категориальное преобразование. Для данного исследования применено фиктивное кодирование, представляющее собой метод, используемый для преобразования категориальных переменных в числовые значения путем создания двоичных столбцов для каждой категории [13]. Критерий 6 вызывает сомнения ввиду максимального количества комнат. Его следует проверить на предмет выбросов данных и удалить ошибочные. Критерии 13-16 необходимо проверить на мультиколлинеарность и удалить

коррелирующие критерии, в противном случае это снизит точность прогноза. Для всех числовых данных в последующем необходимо применить нормализацию из-за большого разброса значений. Всего для моделирования выбраны 4000 точек учета. Там, где это необходимо обучающая и тестовая выборки разделены в соотношении 70 и 30% [8].

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ

В качестве алгоритмов машинного обучения выбраны три популярных и наиболее подходящих к исследуемой задаче. Это метод k- ближайших соседей, случайный лес и линейная регрессия.

1. Метод k – ближайших соседей

Алгоритм использует весь набор данных в качестве обучающей выборки, а не разделяет данные на набор данных для обучения и теста. Когда для нового набора данных требуется определить результат, алгоритм проходит весь набор данных, чтобы найти k-ближайших соседей для нового экземпляра, то есть k экземпляров, наиболее похожих на новую точку, а затем решает, к какой группе эта точка относится. Сходство между экземплярами рассчитывается с использованием таких мер, как евклидово расстояние и расстояние Хемминга [7].

2. Случайный лес

Данный алгоритм может быть использован для задач классификации, регрессии и кластеризации. Он основан на концепции обучения ансамбля, которая представляет собой процесс объединения нескольких классификаторов для решения сложной задачи и повышения производительности модели. Как следует из названия, случайный лес — это классификатор, который содержит несколько деревьев решений в различных подмножествах заданного набора данных и использует среднее значение для повышения точности прогнозирования этого набора данных. Вместо того, чтобы полагаться на одно дерево решений, случайный лес берет прогноз от каждого дерева и основывается на большинстве голосов прогнозов, и далее предсказывает окончательный результат [20].

3. Линейная регрессия

Линейная регрессия — это алгоритм машинного обучения, позволяющий аппроксимировать некую зависимость линейной функцией с использованием метода наименьших квадратов. Несмотря на кажущуюся простоту алгоритма, он является базовым алгоритмом в анализе данных, позволяющим грубо, но достоверно оценить тренды, характер взаимосвязей переменных. Кроме того, алгоритм развивается и обрастает дополнениями, получает новые приложения, так, например нечеткая линейная регрессия или полиномиальная регрессия, построенная на базе линейной, позволяет аппроксимировать нелинейные зависимости [11]. Визуализация работы алгоритма для зависимости двух переменных представлена на Рис. 2. Задача заключается в том, чтобы подобрать такую линейную функцию, которая бы наиболее точно, с минимальной ошибкой описывала существующую зависимость.

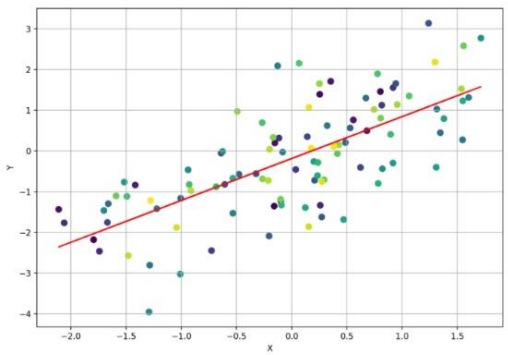


Рис. 2. Линейная регрессия
Fig. 2. Linear regression

Программной средой для реализации вышеуказанных алгоритмов выбраны библиотеки sklearn, NumPy, pandas, seaborn языка программирования Python. Перед реализацией проведены мероприятия по подготовке данных. При помощи тепловой карты (heatmap) выполнен поиск корреляций в исследуемом наборе данных. Представленная на Рис. 3 карта говорит нам о высокой корреляции между критериями Среднее 2019-2022. Так как прогнозируемым параметром будет Среднее 2022, то необходимо удалить из набора данных Среднее за 2019 и 2020 год.

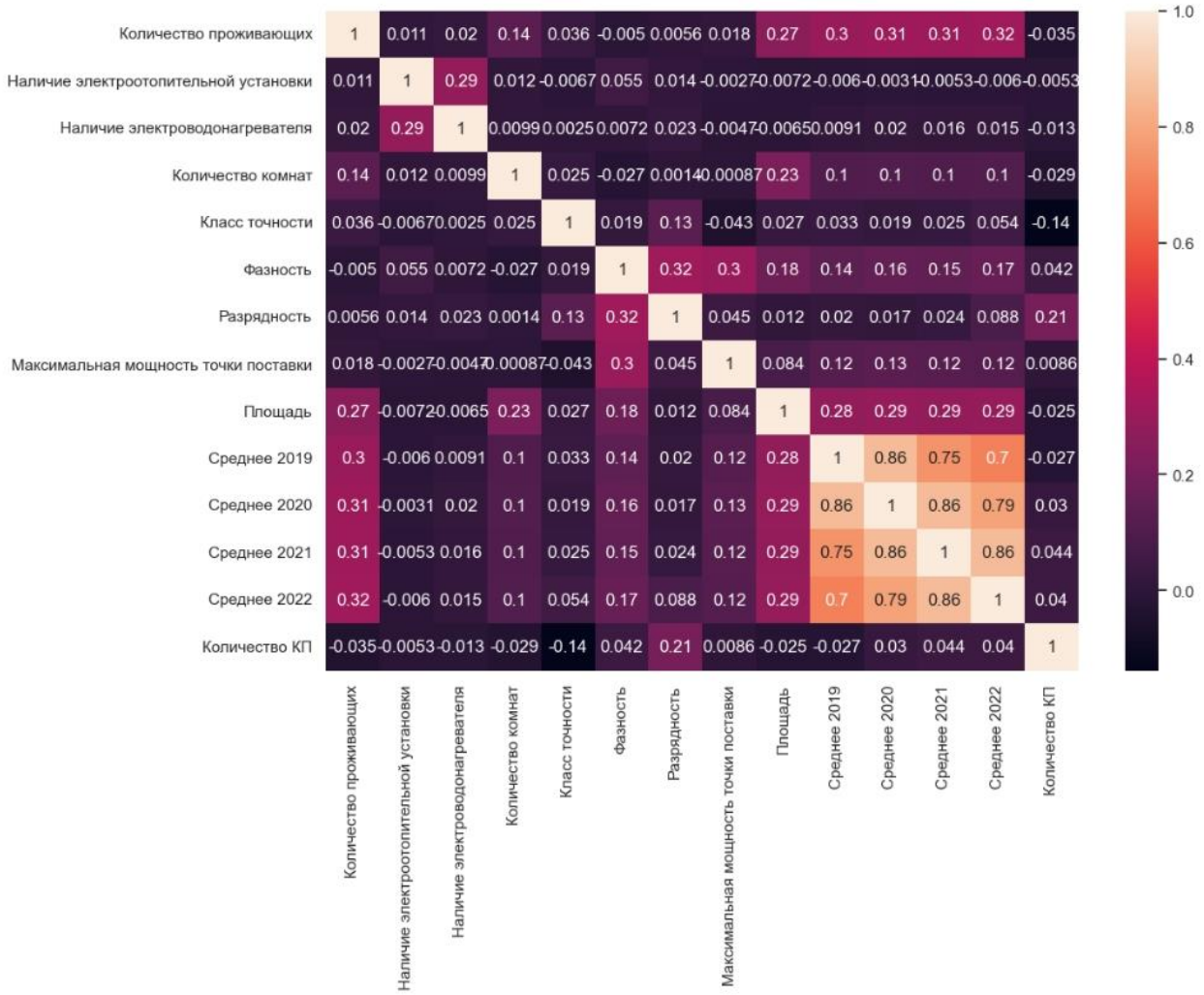


Рис. 3. Тепловая карта
Fig. 3. Heatmap

Категориальные переменные закодированы с помощью добавления фиктивной переменной, пример по критерию “Место прибора” представлен в таблице 2.

Таблица 2

Кодирование категориальных переменных

Table 2

Coding of categorical variables

id	в доме	в хозпостройке	на опоре	на фасаде
0	0	0	1	0
1	0	0	0	1
2	1	0	0	0
3	0	0	1	0
4	**0**	**1**	**0**	**0**

Далее, для “выравнивания” данных выбрана минимакс нормализация – линейное преобразование данных в диапазоне [0...1], где минимальное и максимальное масштабируемые значения соответствуют 0 и 1 соответственно. Формальное представление:

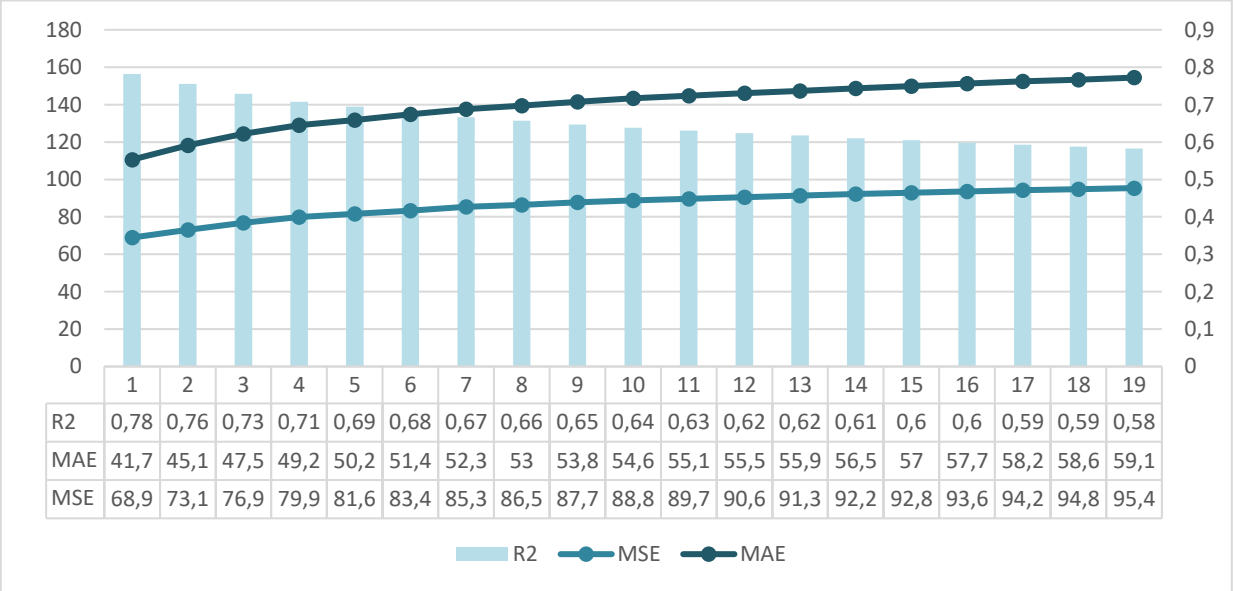
$$X_n = \frac{X - X_{min}}{X_{max} - X_{min}}$$

где, X – текущее значение данных, Xmin – минимальное значение данных выборки, Xmax – максимально значение данных выборки. После проведенных выше мероприятий набор данных подготовлен для моделирования.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

В качестве результатов моделирования представлены кривые показателей MSE,MAE,R2 в зависимости от: числа соседей для метода k-ближайших соседей, числа деревьев в лесу для метода “Случайный лес”, графики частотных зависимостей для всех методов для определения наиболее влияющих критериев, графики сравнения прогнозных-фактических данных для всех методов и итоговая таблица сравнения метрик по каждому методу.

1. ***Метод k – ближайших соседей***



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
R2	0,78	0,76	0,73	0,71	0,69	0,68	0,67	0,66	0,65	0,64	0,63	0,62	0,62	0,61	0,6	0,6	0,59	0,59	0,58
MAE	41,7	45,1	47,5	49,2	50,2	51,4	52,3	53	53,8	54,6	55,1	55,5	55,9	56,5	57	57,7	58,2	58,6	59,1
MSE	68,9	73,1	76,9	79,9	81,6	83,4	85,3	86,5	87,7	88,8	89,7	90,6	91,3	92,2	92,8	93,6	94,2	94,8	95,4

Рис. 4. Метрики качества модели в зависимости от числа соседей
Fig. 4. Model quality metrics depending on the number of neighbors

Итерации производились в диапазоне от 2 до 20 соседей. Как видно из графика на Рис. 4, наибольшие показатели MSE, MAE и R2 достигаются при количестве соседей равном двум. Далее на Рис. 5 представлена степень корреляции между прогнозными и фактическими значениями потребления электроэнергии. Данные коррелируют на 88%.

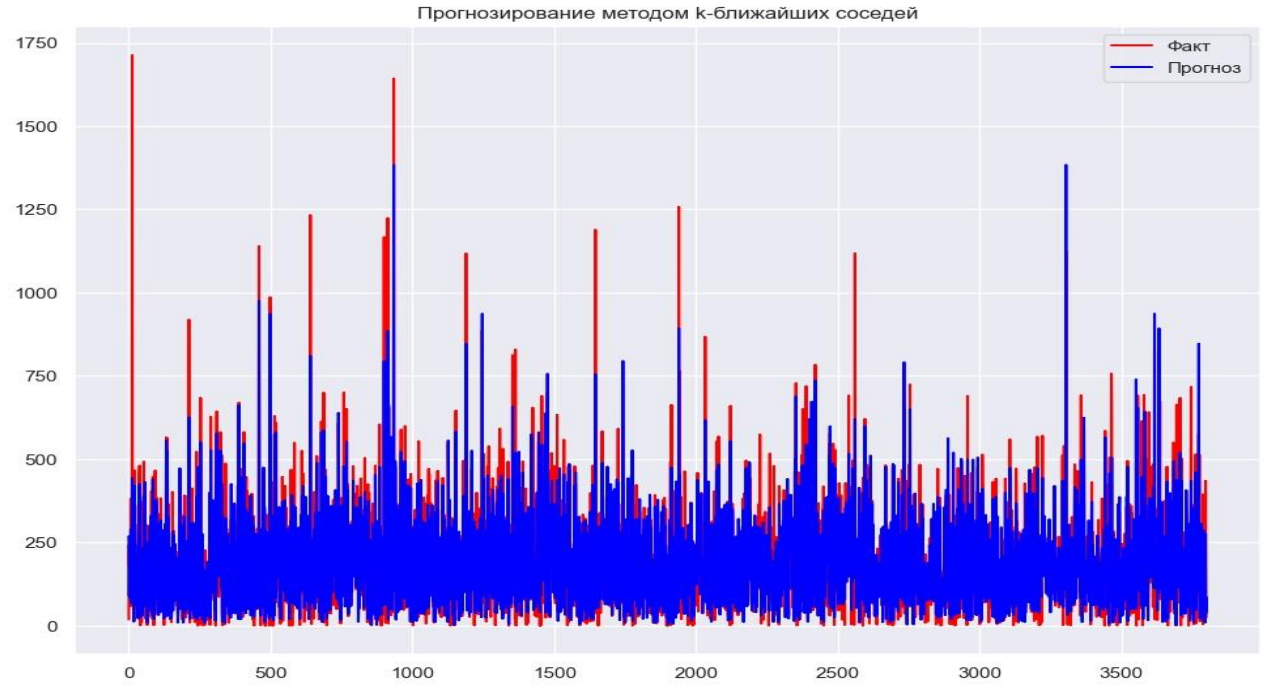
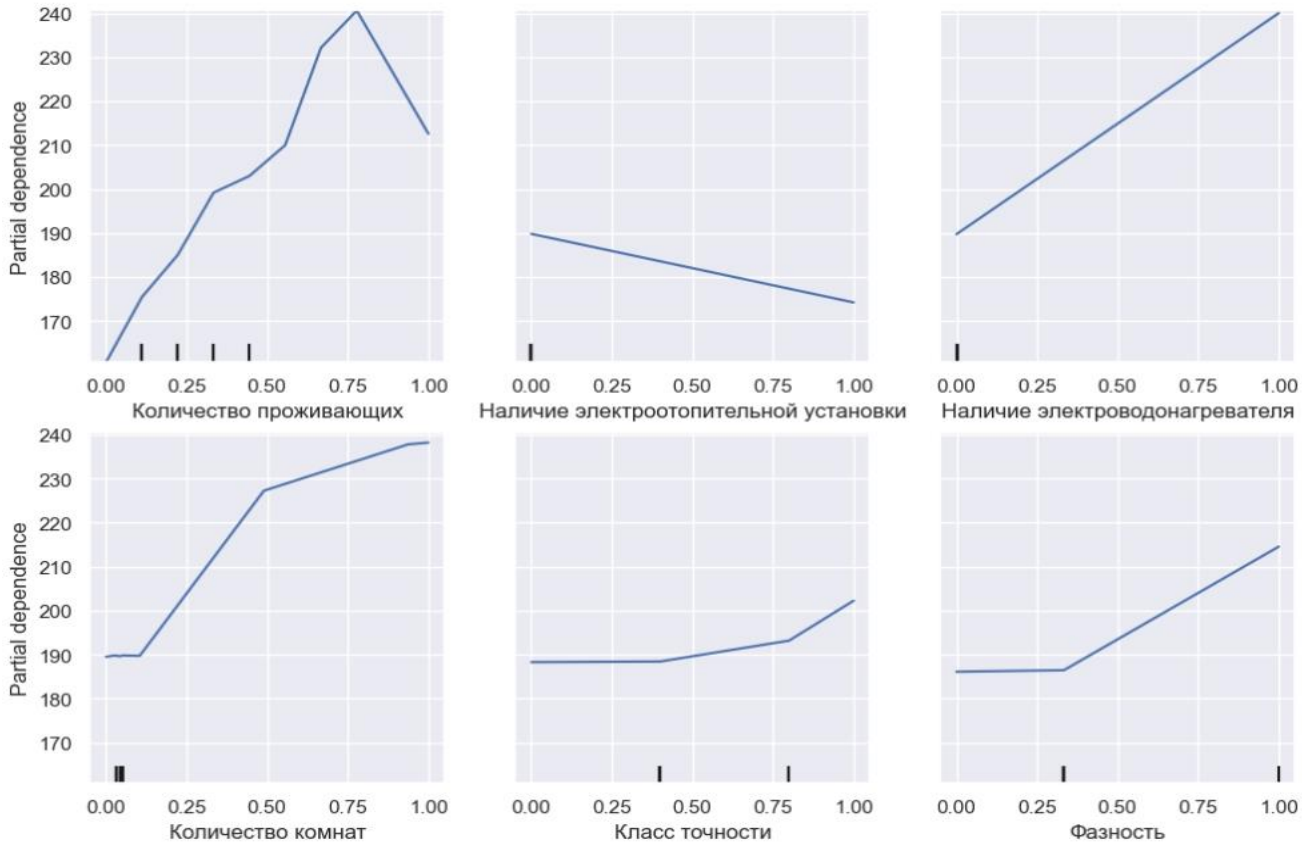


Рис. 5. Корреляция прогнозных и фактических данных
Fig. 5. Correlation of forecast and actual data

Рассмотрим какие критерии из набора данных наиболее влияют на модель. Представлены только первые 12 критериев, так как остальные получены с помощью добавления фиктивной переменной



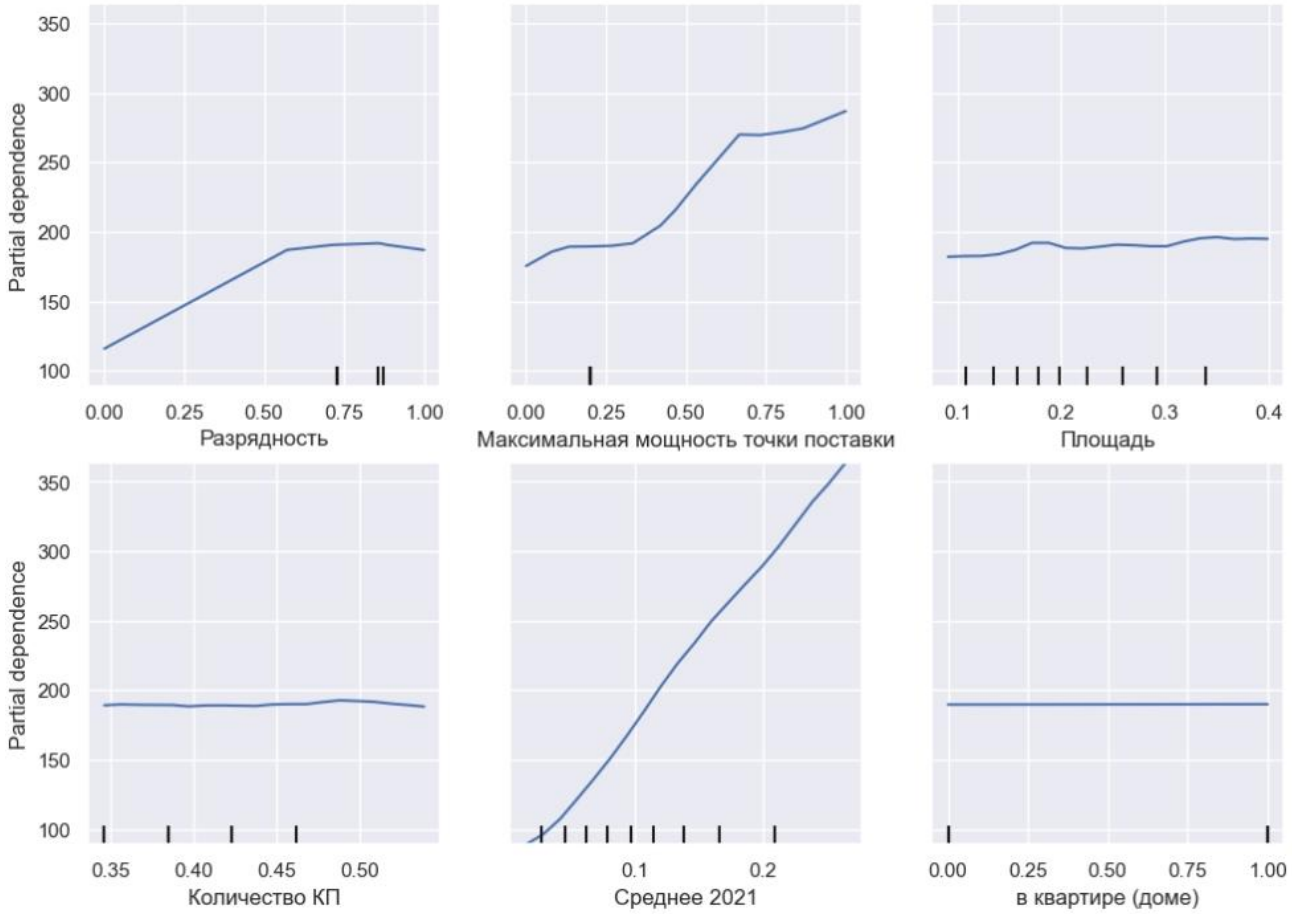


Рис. 6. Степень влияния критериев из набора данных
Fig. 6. The degree of influence of criteria from the data set

Наиболее влияющими критериями, согласно Рис. 6 являются: наличие электроводонагревателя, количество комнат и проживающих, максимальная мощность точки поставки и среднее 2021.

2. Линейная регрессия

Степень корреляции между фактическими и прогнозными значениями составила 87% (Рис.6).

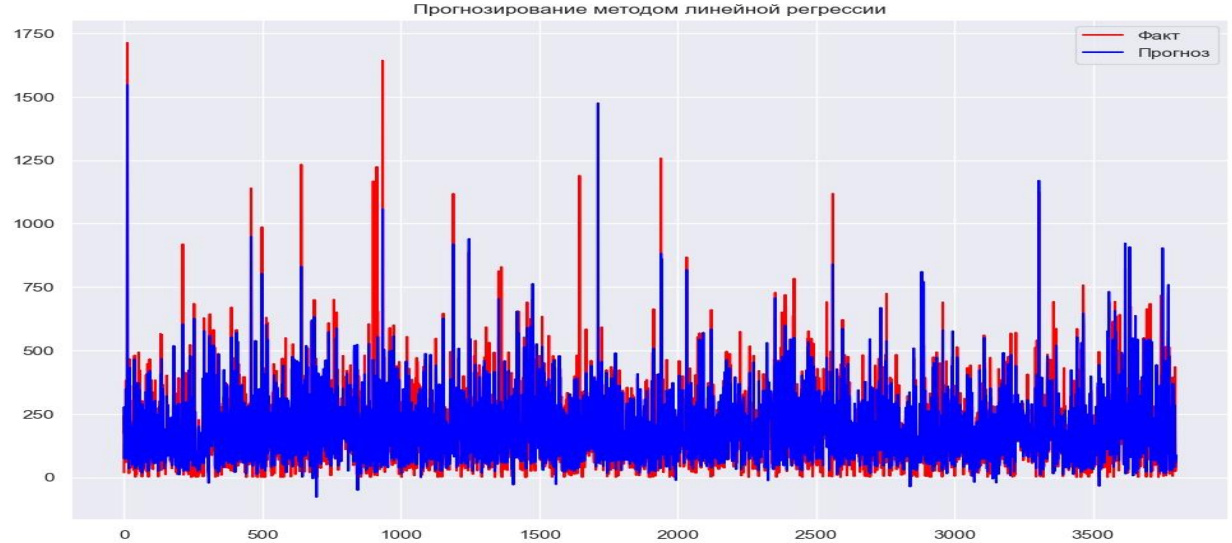


Рис. 7. Корреляция прогнозных и фактических данных
Fig. 7. Correlation of forecast and actual data

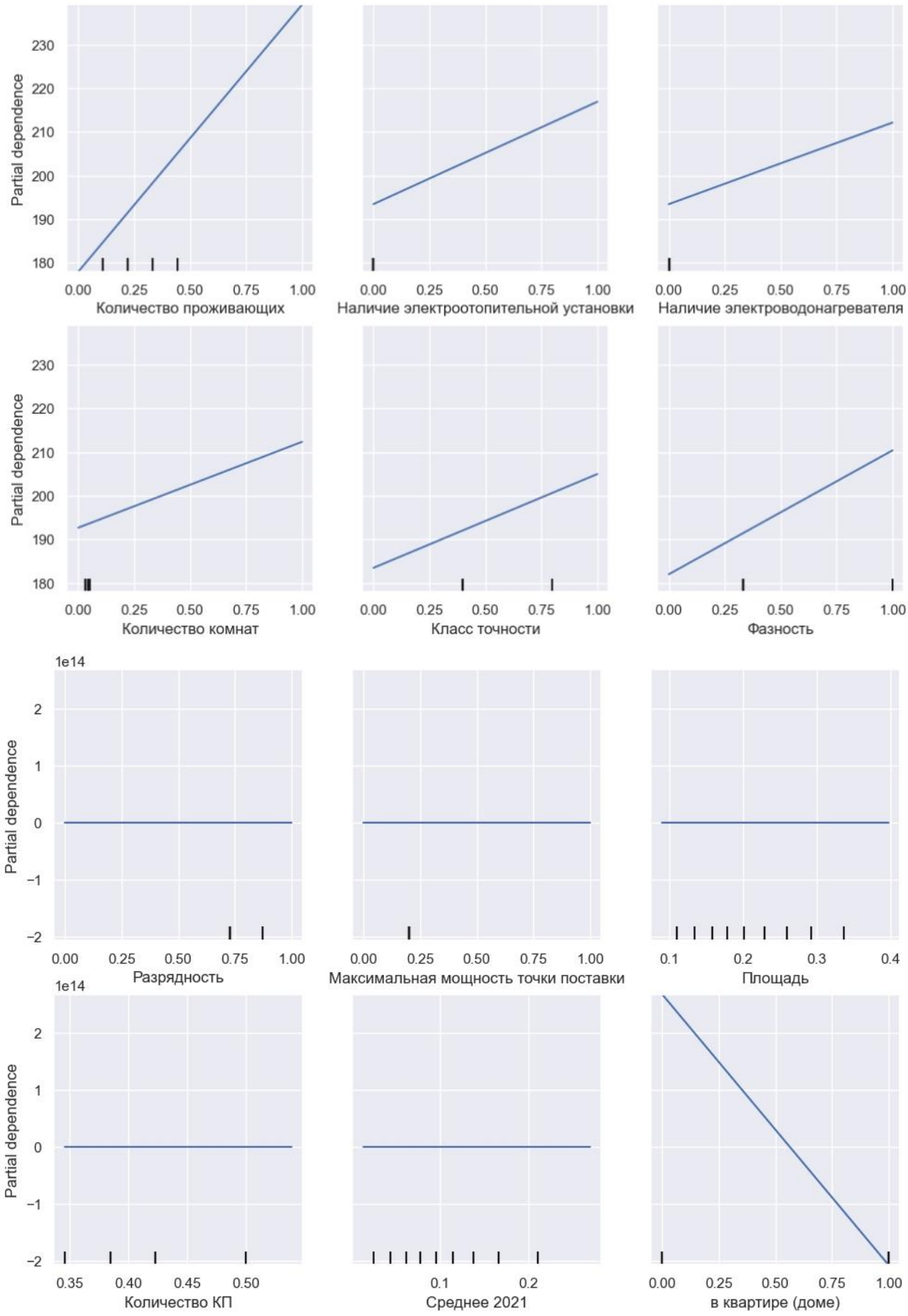


Рис. 8. Степень влияния критериев из набора данных
Fig. 8. The degree of influence of criteria from the data set

Наиболее влияющими критериями, согласно Рис. 9 являются: количество комнат и проживающих, фазность, класс точности, наличие электроотопления и электроводонагрева.

3. Случайный лес

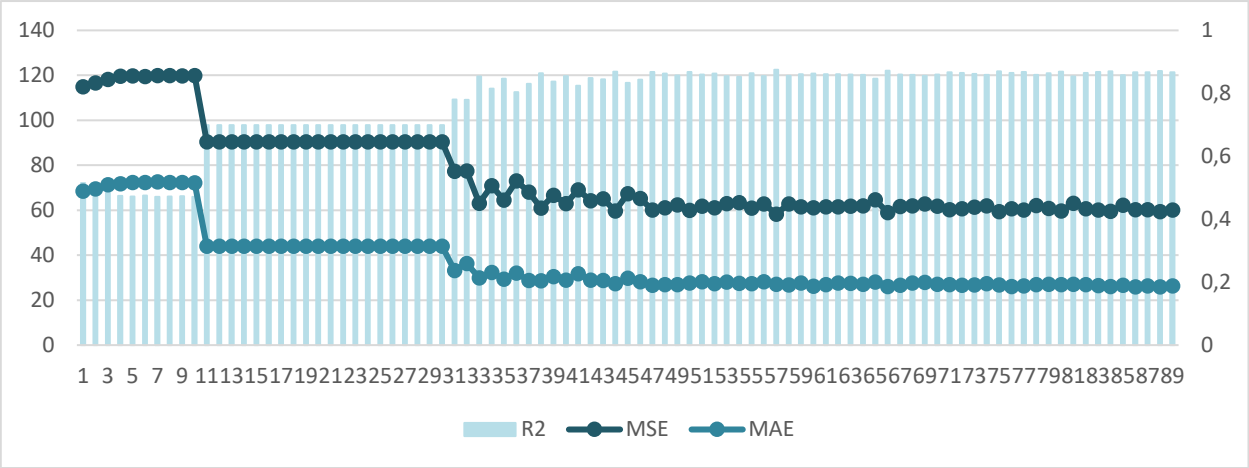


Рис. 9. Метрики качества модели в зависимости от числа деревьев
Fig. 9. Model quality metrics depending on the number of trees

Итерации производились в диапазоне от 10 до 1000 деревьев. На графике из Рис. 9 представлены только первые 89 итераций. Модель демонстрирует наилучшие метрики при 258 деревьях. Степень корреляции 95%. (Рис. 10).

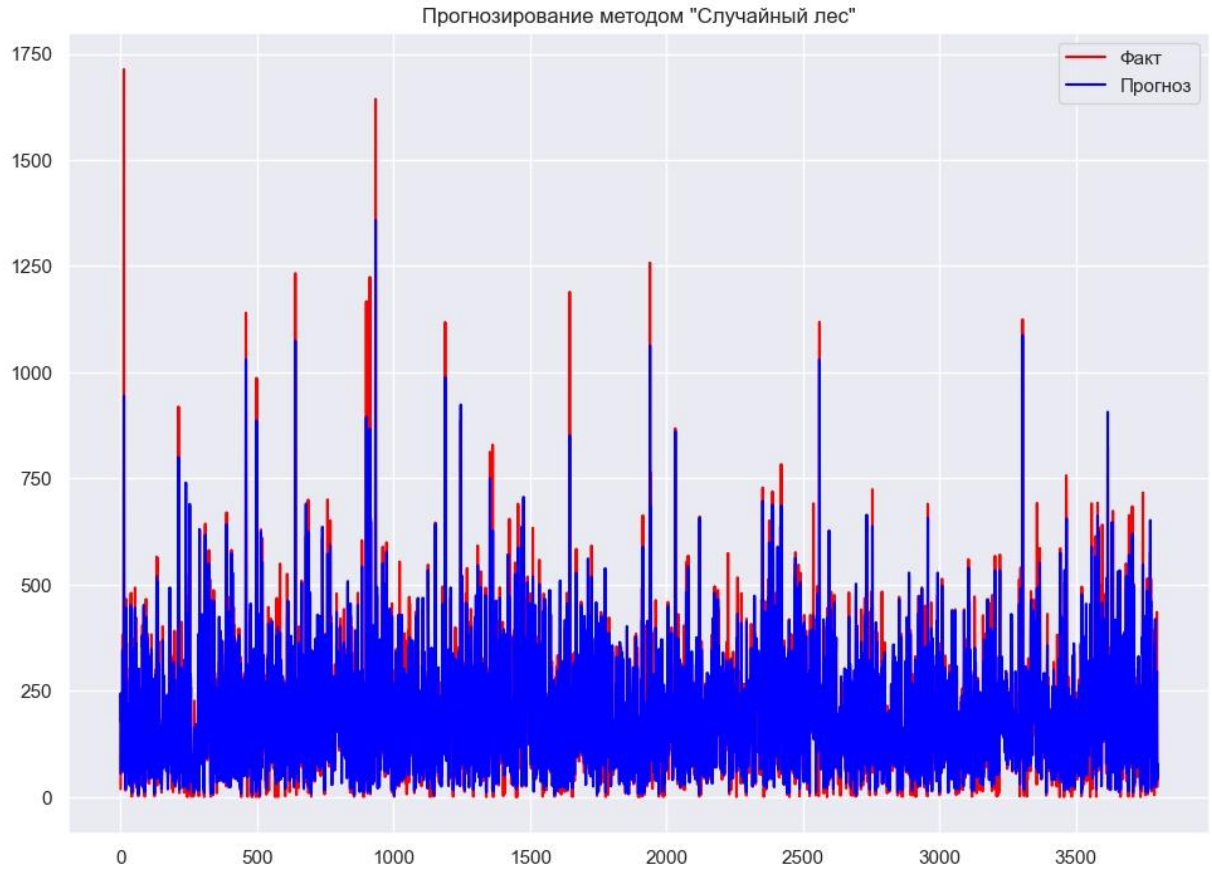


Рис. 10. Корреляция прогнозных и фактических данных
Fig. 10. Correlation of forecast and actual data

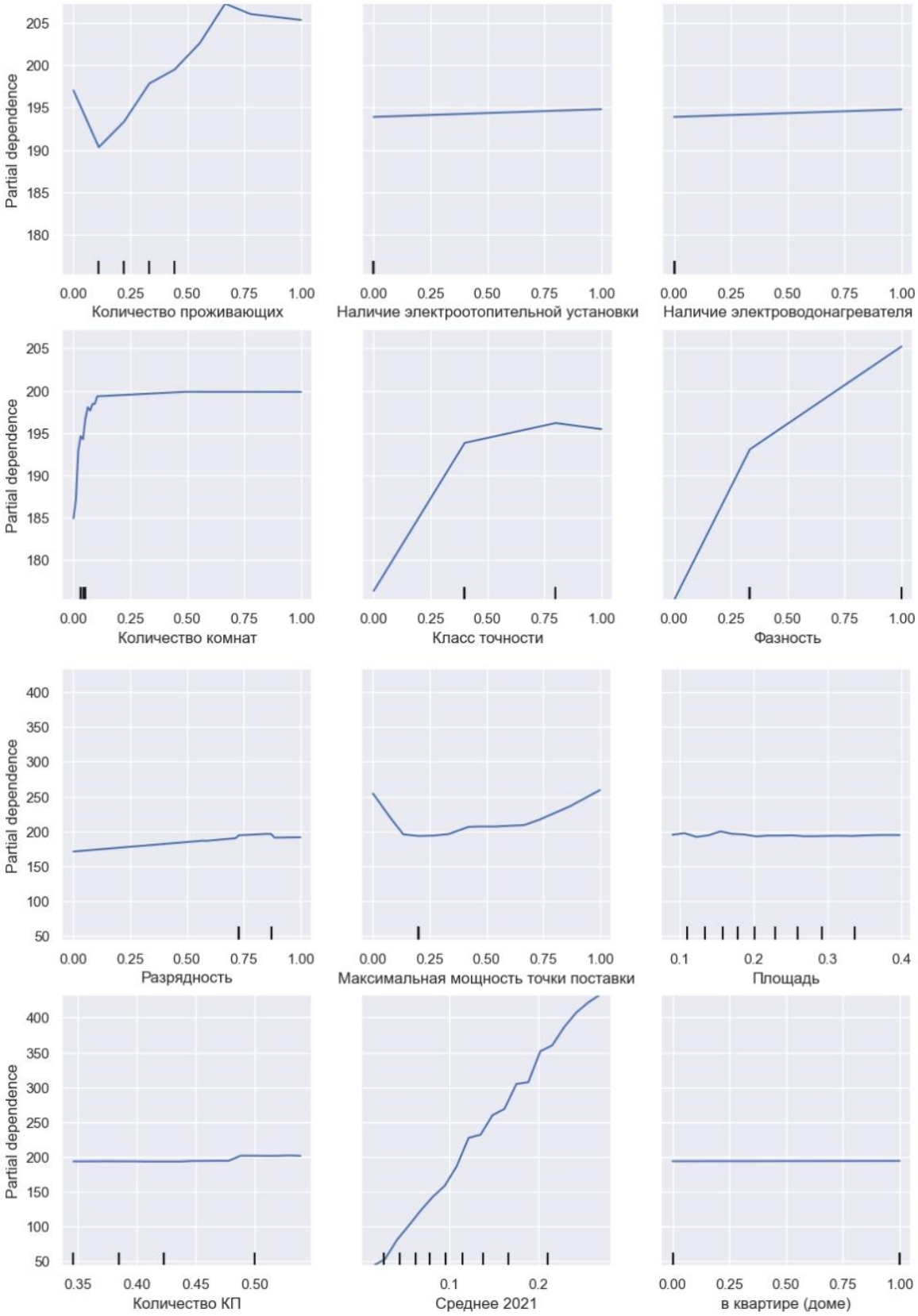


Рис. 11. Степень влияния критериев из набора данных
Fig. 11. The degree of influence of criteria from the data set

Наиболее влияющими критериями, согласно Рис. 10 являются: количество комнат и проживающих, фазность, класс точности, наличие электроотопления и электроводонагрева и среднее 2021. Итоговая таблица сравнения моделей:

Таблица 3

Сравнение метрик качества моделей

Table 3

Comparison of model quality metrics

Метрика	**k-ближайших соседей**	**Линейная регрессия**	**Случайный лес**
MSE	68,921	70,902	42,923
MAE	41,662	37,687	21,586
R2	0,782	0,769	0,915

Таким образом, наилучшие показатели у алгоритма Случайный лес, алгоритмы k-ближайших соседей и Линейной регрессии показали практические одинаковые результаты.

ЗАКЛЮЧЕНИЕ

В представленной работе поднят вопрос о применении алгоритмов машинного обучения к решению проблем поиска потерь электроэнергии. Обучив модель на данных приборов учета, включенных в АИИСКУЭ, можно проверить на отклонения в потреблении контрагентов, не имеющих данные интеллектуальные приборы учета. Для решения этой задачи изучена база данных организации проведена подготовка данных для моделирования. Для моделей использовались три наиболее популярных алгоритма. Наилучшим образом зарекомендовал себя алгоритм “Случайный лес”. Причиной лучшей работы данного алгоритма является отсутствии экстраполяции, то есть выхода за пределы обучающей выборки.

Помимо перечисленных, существует множество других алгоритмов машинного обучения, это ответвление искусственного интеллекта постоянно развивается и разрабатывает все более эффективные методики.

Список литературы

1. Бокс Дж. Анализ временных рядов. Прогноз и управление / Бокс Дж, Дженкинс Г. М.: Мир, Вып.1, 1974. – 406 с.

2. Гаврилова Т.А. Базы знаний интеллектуальных систем. Учебник / Гаврилова Т.А., Хорошевский В.Ф. — СПб.: Питер, 2000. – 384 с.

3. Галушкин А.И. Нейроматематика (проблемы развития) / М.: Радиотехника, 2003.40с.

4. Донской, Д. А. Применение аналитических технологий в системах управления и информатике/ Донской Д.А., Слепцов Н.В., Щербаков М.А.– Пенза, 2005.

5. Железко, Ю.С. Расчет, анализ и нормирование потерь электроэнергии в электрических сетях / Ю.С. Железко. // М.: НУ ЭНАС, 2002. – 280с.

6. Иванов В.Л. Электронный учебник: системы контроля знаний // Информатика и образование. – 2002. – № 1.

7. Казанская А.А. Использование машинного обучения в инвестиционной деятельности / А.А. Казанская, Л.Г. Мишура // Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент. – 2020. – № 2. – С. 23-34. – DOI 10.17586/2310-1172-2020-13-2-23-34. – EDN MUJXYZ.

8. Кафтанников, И.Л. Проблемы формирования обучающей выборки в задачах машинного обучения / И.Л. Кафтанников, А.В. Парасич // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2016. – Т. 16, № 3. – С. 15–24. DOI: 10.14529/ctcr160302

9. Кудашев К., Коммерческие потери электроэнергии без границ, 2017 г. URL: http://www.bigpowernews.ru/interview/document76022.phtml (дата обращения: 23.11.2023)

10. Найти утечку, 2021 г. URL: https://www.kommersant.ru/doc/4877601 (дата обращения: 23.11.2023)

11. Нечеткая линейная регрессия в задачах оценки / Е.В. Вишнякова, Е.В. Иванова, С.М. Камалов [и др.] // Научные записки молодых исследователей. – 2015. – № 5. – С. 14-29.

12. Джонс Т. Программирование искусственного интеллекта в приложениях / Пер. с англ. Осипов А.И. – М.: ДМК Пресс, 2011. – 312 с.

13. Тоуди Т. Преобразование категориальных данных: Практическое руководство по обработке нечисловых переменных для алгоритмов машинного обучения, 2023 г. URL: https://dev-gang.ru/article/preobrazovanie-kategorialnyh-dannyh-prakticzeskoe-rukovodstvo-po-obrabotke-neczislovyh-peremennyh-dlja-algoritmov-mashinnogo-obuczenija-buyh1q4ttt/

14. Трикоз Д.В. Нейронные сети: как это делается? Компьютеры + программы N 4(5). – 1993. – С. 14-20.

15. Флах П. Машинное обучение / П. Флах // М.: ДМК Пресс, 2015. с. 25.

16. Хайкин С. Нейронные сети: полный курс / С. Хайкин. – М.: Диалектика, 2019. – 1104 с.

17. Andrzej C. Neural Networks for Optimization and Signal Processing [Текст] / C. Andrzej, R. Unbehauen, J. Wiley and Sons Ltd, 1993. – 526 с.

18. Hyndman R.J., Koehler A.B. Another look at measures of forecast accuracy // International Journal of Forecasting. –2006. – № 22(4). – P. 679-688.

19. Shcherbakov M.V., Brebels A. Outliers and anomalies detection based on neural networks forecast procedure: Proceedings of the 31st Annual International Symposium on Forecasting (ISF 2011) / Prague: International Institute of Forecasters, 2011. – pp. 21-22. URL: http://www.forecasters.org/isf/pdfs/ISF11_Proceedings.pdf

20. Yu, Chong Ho. Exploratory data analysis in the context of data mining and resampling // International Journal of Psychological Research. 3. 2010.

References

1. Box J. Time series analysis. Forecasting and management / Box J, Jenkins G. M.: Mir, V.1, 1974. – 406 p.

2. Gavrilova T.A. Knowledge bases of intellectual systems. Textbook / Gavrilova T.A., Khoroshevsky V.F. – SPb.: Piter, 2000. – 384 p.

3. Galushkin A.I. Neuromathematics (problems of development) / M.: Radiotekhnika, 2003. 40 p.

4. Donskoy D.A. Application of analytical technologies in control systems and informatics / Donskoy D.A., Sleptsov N.V., Shcherbakov M.A. – Penza, 2005.

5. Zhelezko Yu.S. Calculation, analysis and rationing of the electric power losses in the electric networks / Yu.S. Zhelezko // M.: NU ENAS, 2002. – 280 p.

6. Ivanov V.L. Electronic textbook: knowledge control systems (in Russian) // Informatics and Education. – 2002. – № 1.

7. Kazanskaya A.A. The use of machine learning in investment activity / A.A. Kazanskaya, L.G. Mishura // Scientific Journal of NIU ITMO. Series: Economics and Environmental Management. – 2020. – № 2. – P. 23-34. – DOI: 10.17586/2310-1172-2020-13-2-23-34. – EDN MUJXYZ.

8. Kaftannikov I.L. Problems of training sample formation in machine learning tasks / I.L. Kaftannikov, A.V. Parasich // Vestnik SUSU. Series "Computer technologies, management, radio electronics". – 2016. – T. 16, № 3. – P. 15-24. DOI: 10.14529/ctcr160302

9. Kudashev K. Commercial electricity losses without borders, 2017. URL: http://www.bigpowernews.ru/interview/document76022.phtml (date of reference: 23.11.2023

10. Find Leakage, 2021 URL: https://www.kommersant.ru/doc/4877601 (date access: 23.11.2023)

11. Fuzzy linear regression in estimation problems / E.V. Vishnyakova, E.V. Ivanova, S.M. Kamalov [et al.] // Scientific Notes of Young Researchers. – 2015. – № 5. – P. 14-29.

12. Jones T. Programming of Artificial Intelligence in Applications / Per. from Engl. Osipov A.I. – M.: DMK Press, 2011. – 312 p.

13. Toady T. Transforming categorical data: A practical guide to handling non-numeric variables for machine learning algorithms, 2023 URL: https://dev-gang.ru/article/preobrazovanie-kategorialnyh-dannyh-prakticzeskoe-rukovodstvo-po-obrabotke-neczislovyh-peremennyh-dlja-algoritmov-mashinnogo-obuczenija-buyh1q4ttt/

14. Tricoz D.V. Neural networks: how to do it? Computers + Programs N 4(5). 1993. – 14-20 p.

15. Flach P. Machine learning / P. Flach // M.: DMK Press, 2015. p. 25

16. Haykin S. Neural networks: a complete course / S. Haykin. – M.: Dialectics, 2019. – 1104 p.

17. Andrzej C. Neural Networks for Optimization and Signal Processing [Text] / C. Andrzej, R. Unbehauen, J. Wiley and Sons Ltd, 1993. – 526 p.

18. Hyndman R.J., Koehler A.B. Another look at measures of forecast accuracy // International Journal of Forecasting. –2006. – № 22(4). – P. 679-688.

19. Shcherbakov M.V., Brebels A. Outliers and anomalies detection based on neural networks forecast procedure: Proceedings of the 31st Annual International Symposium on Forecasting (ISF 2011) / Prague: International Institute of Forecasters, 2011. – pp. 21-22. URL: http://www.forecasters.org/isf/pdfs/ISF11_Proceedings.pdf

20. Yu, Chong Ho. Exploratory data analysis in the context of data mining and resampling // International Journal of Psychological Research. 3. 2010.

Коржавых Владислав Валерьевич, заместитель начальника Валуйского района электрических сетей по реализации услуг
Korzhavykh Vladislav Valerievich, Deputy Head of the Valuysky Sistrict of Electric Grids for Sales of Services

УДК 004.032.26 **DOI: 10.18413/2518-1092-2024-9-1-0-8**

Ильинская Е.В.
Голышева Е.Н.
Медведев А.А.
Масалитин Н.С.

ПРИМЕНЕНИЕ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ НЕЙРОСЕТЕЙ ДЛЯ ГЕНЕРАЦИИ ИЗОБРАЖЕНИЙ

Белгородский государственный национальный исследовательский университет,
ул. Победы, 85, г. Белгород, 308015, Россия

e-mail: chmireva@bsu.edu.ru

Аннотация
В данной статье рассматривается тема генерации изображений с использованием генеративно-состязательных нейронных сетей. Благодаря развитию глубокого обучения и искусственного интеллекта, нейросети стали мощным инструментом для создания реалистичных и выразительных изображений. Генерация изображений с помощью нейросетей является одной из наиболее перспективных областей искусственного интеллекта. Нейросети позволяют генерировать изображения, которые не только соответствуют заданным параметрам, но также являются новыми и оригинальными. В этой статье рассматриваются ключевые аспекты использования нейросетей в генерации изображений. Основное внимание уделяется анализу различных архитектур и подходов в области генерации изображений с помощью нейронных сетей. Ключевые аспекты, такие как условная генерация, генеративно-состязательные сети (GAN), исследуются и сравниваются. Также рассматриваются применения нейросетей в различных сферах, включая искусство, дизайн и синтез фотореалистичных изображений. Представлены наиболее известные нейросети, используемые для этой задачи, а также их преимущества и недостатки. Обсуждаются перспективы развития нейросетей для генерации изображений.
Ключевые слова: нейронные сети; генерация изображений; глубокое обучение; условная генерация; генеративно-состязательные сети
Для цитирования: Ильинская Е.В., Голышева Е.Н., Медведев А.А., Масалитин Н.С. Применение генеративно-состязательных нейросетей для генерации изображений // Научный результат. Информационные технологии. – Т.9, №1, 2024. – С. 73-78. DOI: 10.18413/2518-1092-2024-9-1-0-8

Ilyinskaya E.V.
Golysheva E.N.
Medvedev A.A.
Masalitin N.S.

THE USE OF GENERATIVE-ADVERSARIAL NEURAL NETWORKS FOR IMAGE GENERATION

Belgorod State National Research University,
85 Pobedy St., Belgorod, 308015, Russia

e-mail: chmireva@bsu.edu.ru

Abstract
This article discusses the topic of image generation using neural networks. Thanks to the development of deeper learning and artificial intelligence, neural networks have become a powerful tool for creating realistic and expressive images. Image generation using neural networks is one of the most promising areas of artificial intelligence. Neural networks allow you to generate images that not only meet certain requirements, but are also new and original. This article discusses the key aspects of using neural networks in image generation. The main attention is paid to the analysis of various architectures and approaches in the field of image generation using neural networks. Key aspects such as conditional generation, generative-adversarial networks (GAN) are investigated and compared. Applications of neural networks in various fields, including art, design and synthesis of

photorealistic images, are also considered. The most well-known neural networks used to solve this problem are presented, as well as their advantages and disadvantages. The prospects for the development of neural networks for image generation are discussed.
Keywords: neural networks; image generation; deeper learning; conditional generation; generative-adversarial networks
For citation: Ilyinskaya E.V., Golysheva E.N., Medvedev A.A., Masalitin N.S. The use of generative-adversarial neural networks for image generation // Research result. Information technologies. – T.9, №1, 2024. – P. 73-78. DOI: 10.18413/2518-1092-2024-9-1-0-8

ВВЕДЕНИЕ

Использование нейронных сетей в генерации изображений является одной из наиболее сложных задач в области анализа изображений, но также развивающееся направление в области искусственного интеллекта. Традиционные методы создания изображений основаны на использовании алгоритмов, которые уже базируются на правилах. Такие алгоритмы могут генерировать изображения, которые удовлетворяют определенным требованиям, но они не могут создать что-то новое и отличительные фотографии. Нейросети, напротив, могут генерировать уникальные изображения.

ПРИНЦИП РАБОТЫ

Нейронные сети для формирования изображений работают, перенимая информацию из набора данных изображений. Такой набор может иметь в себе фотографии, рисунки, иллюстрации и другие виды изображений. Нейросеть анализирует эти изображения и учится распознавать их особенности, такие как цвет и текстура.

Когда пользователю предоставляется описание при помощи текста или изображение, нейросеть использует свои данные о мире, чтобы сотворить исключительное изображение, которое будет подходить под описание или уже имеющееся фото.

Основные подходы к генерации изображений с помощью нейронных сетей можно разделить на два типа:

1. **На основе текстового описания.** Генерация на основе текстового описания происходит за счет получения на вход нейронной сети словесной характеристики признаков требуемой картинки.
2. **На основе существующих изображений.** Генерация на основе существующих изображений происходит за счет получения на вход нейронной сети существующего изображения, которое необходимо переработать или дополнить.

Рассмотрим более подробно особенности основных подходов к генерации изображений с помощью нейронных сетей.

Популярным подходом к генерации изображений при помощи текстового описания на сегодняшний день является метод, в основу которого положено применение генеративных состязательных сетей (GAN). Указанный метод работает при помощи двух нейронных сетей (генератора и дискриминатора). Словесное описание признаков требуемого изображения получает генератор в текстовом виде и его задачей является воспроизведение полученной информации. Дискриминатор выполняет проверку изображения, определяя действительное ли оно соответствует заданному текстовому описанию. Обучение генератора и дискриминатора происходит одновременно. Генератор формирует изображения, которые будет трудно отличить от подлинника. Генерация изображений проводится до тех пор, пока не будут созданы качественные изображения, максимально соответствующие заданным в текстовом виде признакам.

Ещё одним часто применяемым подходом к генерации изображений на основе текстового описания является подход, основанный на использовании трансформеров. Трансформеры – это нейросети, которые позволяют эффективно обрабатывать последовательности данных.

Применив несколько нейросетей, таких как Catalog.ngc.nvidia и Dezgo, по запросу «собака на пляже с игрушками» мы получили изображения, представленные на рисунке 1.

Рис. 1. Пример генерация изображений на основе текстового описания
Fig. 1. Example generating images based on text description

Распространенным в настоящее время подходом к генерации иллюстраций на основе уже существующих изображений является подход, в основе которого лежит использование циклических генеративных состязательных сетей (CycleGAN). Указанный метод работает при помощи двух нейронных сетей (генератора и дискриминатора). На генератор передается изображение одного типа, которое он стремится преобразовать в изображение другого типа. Дискриминатор используется для проверки сформированного генератором изображения и определяет, реальное ли оно.

Ещё одним известным подходом к генерации изображений на основе существующих изображений является подход, основанный на использовании вариационных автокодировщиков (VAE). VAE – это нейросети, которые позволяют кодировать и декодировать данные. В этом случае нейросеть работает с заданным изображением, которое ей необходимо преобразовать в изображение другого типа, используя VAE.

Сгенерируем уникальные изображения используя нейросеть Imagine.art, на основе иллюстраций из прошлого примера, изменив стиль (рис. 2).

Рис. 2. Пример генерация изображений на основе существующих изображений
Fig. 2. Example of generating images based on existing images

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ НЕЙРОСЕТЕЙ ДЛЯ ГЕНЕРАЦИИ ИЗОБРАЖЕНИЙ

Рассмотрим **преимущества**, которыми обладают нейронные сети, используемые в генерации изображений:

1. Нейронные сети могут формировать изображения, которые определены заданными требованиями, но и будут неповторимыми.
2. Нейронные сети могут создавать изображения, используя разные стили.
3. Нейронные сети могут использовать высокое разрешение при генерации изображений.

Нейронные сети, используемые в генерации изображений, обладают также и **недостатками**:

1. Нейронные сети могут генерировать изображения, которые могут содержать искажения или нарушение.
2. Нейронные сети могут быть подвержены предвзятости данных, на которых они формируются.

ПЕРСПЕКТИВЫ РАЗВИТИЯ

На сегодняшний день нейросети для генерации изображения все еще не идеальны, у них по-прежнему остается множество недостатков и большая область для развития. Так, перспективы развития нейросетей для генерации изображений можно разделить на два основных типа:

1. Улучшение качества генерируемых изображений

Исследователи работают над улучшением качества генерируемых изображений, чтобы они стали как можно более реалистичными, детализированными и не содержали дефектов. Для этого используются различные подходы, такие как:

1) Обучение нейронных сетей с использованием более всевозможных наборов данных.
2) Проектирование архитектур нейросетей для генерации более масштабных иллюстраций.
3) Применение методов анализа данных и методов машинного обучения.

2. Снижение предвзятости нейросетей

Нейросети могут генерировать изображения, которые отражают предубеждения, существующие в данных. Для снижения предвзятости нейросетей используются различные подходы, такие как:

1) Использование более всевозможных наборов данных для обучения нейросетей.
2) Применение инновационных методов обучения нейросетей.

На сегодняшний день генерация изображений при помощи нейронных сетей получает широкое развитие, в то числе генерация изображений в реальном времени, генерация изображений в трехмерном формате.

ОБЛАСТИ ПРИМЕНЕНИЯ

Нейросети для генерации изображений имеют множество сфер применения. Например, они могут быть использованы в области дизайна, моделирования видеоигр, и применяться в научно-исследовательской работе в различных сферах, в том числе и в медицине. Нейросети могут быть использованы для генерирования реалистичных изображений несуществующих объектов или для создания видеороликов с участием вымышленных персонажей. Нейронные сети могут быть использованы для генерации изображений мозга, которые помогут врачам диагностировать заболевания. Также они могут использоваться для создания изображений галактик и других космических объектов, что поможет ученым лучше понять Вселенную. Нейросети могут использоваться для создания персонализированных продуктов и услуг на основе предпочтений клиентов. Например, для онлайн-розничных платформ можно генерировать уникальные дизайны одежды или аксессуаров, которые подходят покупателю. Кроме того, нейронные сети могут быть использованы для генерирования презентаций, где они могут быть особенно ценными в бизнесе и образовании. Нейросети могут использоваться для обучения студентов новым навыкам. Например, нейронные сети могут быть использованы для генерации обучающих материалов или для персонализации обучения в соответствии с потребностями каждого студента.

ЗАКЛЮЧЕНИЕ

С использованием нейронной сети, мы получили сгенерированные изображения как в одном стиле, так и в другом. Помимо этого, использовали методы GAN и CycleGAN, которые отвечают за генерацию изображений по разным принципам: один при помощи текста, другой при помощи существующих изображений. Нейронные сети для генерации изображений представляют собой мощный класс искусственных нейронных сетей, который способен создавать и трансформировать изображения на основе сформированных данных. Эти сети нашли широкое применение в различных сферах, и их способности продолжают расширяться, меняя способы, которыми мы воспринимаем и создаем изображения. Различные типы нейросетей позволяют создавать уникальный и качественный визуальный контент, от портретов и абстрактных композиций до спецэффектов в фильмах и видеоиграх. Эти инструменты становятся все более доступными и могут улучшать процессы в множестве отраслей, от искусства и дизайна, до медицины и медиа. В искусстве они позволяют создавать оригинальные произведения искусства, которые невозможно было создать традиционными методами. В дизайне они позволяют создавать новые дизайны продуктов, одежды и интерьеров. В маркетинге они позволяют создавать рекламные материалы и контент для социальных сетей. В образовании они позволяют создавать новые обучающие материалы и интерактивные игры.

Однако эта технология также связана с потенциальными рисками и этическими проблемами. Например, нейросети могут использоваться для создания поддельных изображений, которые могут использоваться для обмана или манипуляций. Важно учитывать эти аспекты этой технологии, чтобы она использовалась ответственно, и необходимо разработать механизмы, которые помогут предотвратить такое использование нейросетей, проводить дискуссии и разрабатывать эффективные средства проверки и подтверждения подлинности изображений, чтобы избежать негативных последствий.

Нейросети для генерации изображений – это технология, которая развивается постоянно. В ближайшие годы мы можем ожидать появления новых и более совершенных методов генерации изображений. Эти методы будут иметь все более широкий спектр применений, который в большой степени затронет нашу жизнь, однако их использование также подразумевает ответственность и необходимость этического и социального регулирования.

Список литературы

1. Лекун Я. Как учится машина: Революция в области нейронных сетей и глубокого обучения, 2021 г., 370 с.

2. Гудфеллоу Я., Бенджио И., Курвилль А. «Глубокое обучение», 2017 г., 653 с.

3. Безгачев Ф.В. Применение нейросетей в искусственной генерации лиц, 2021 г. URL: https://cyberleninka.ru/article/n/primenenie-neyrosetey-v-iskusstvennoy-generatsii-lits.

4. Сантану Паттанаяк. Генерация изображений с помощью TensorFlow, 2022 г., 698 с.

5. Редько В.Г. Эволюция, нейронные сети, интеллект: Модели и концепции эволюционной кибернетики, М.: Ленанд, 2019 г., 224 с.

6. Cigliano A. Generative adversarial networks, 2018 г. URL: https://www.linkedin.com/pulse/generative-adversarial-networks-andrea-cigliano.

7. Ха Д., Шмидхубер Ю. Модели мира, 2018 г., 21 с.

8. Галушкин А.И. Нейронные сети: основы теории, М.: РиС, 2023 г., 496 с.

9. Андреева О.В. Формирование оптимального алгоритма верификации изображений на основе нейронных сетей, Современные проблемы науки и образования, 2015 г., №1-1, С. 268.

10. Мазуров М.Е. Распознавание сложных объектов избирательными нейронными, Нейрокомпьютеры и их применение: тез. Докл., 2022 г., С. 60-61.

References

1. Lekun Ya. How a machine learns: A revolution in the field of neural networks and deep learning, 2021, 370 p.

2. Goodfellow Ya., Benjio I., Courville A. Deep learning, 2017, 653 p.
3. Bezgachev F.V. Application of neural networks in artificial generation of faces, 2021 URL: https://cyberleninka.ru/article/n/primenenie-neyrosetey-v-iskusstvennoy-generatsii-lits.
4. Santanu Pattanayak. "Image generation using TensorFlow", 2022, 698 p.
5. Redko V.G. Evolution, neural networks, intelligence: Models and concepts of evolutionary cybernetics, M.: Lenand, 2019, 224 p.
6. Cigliano A. Generative adversarial networks, 2018. URL: https://www.linkedin.com/pulse/generative-adversarial-networks-andrea-cigliano
7. Ha D., Schmidhuber Ju. Models of the World, 2018, 21 p.
8. Galushkin A.I. Neural networks: fundamentals of theory, M.: FiG., 2023, 496 p.
9. Andreeva O.V. Formation of an optimal image verification algorithm based on neural networks, Modern problems of science and education, 2015, No.1-1, p. 268.
10. Mazurov M.E. Recognition of complex objects by selective neural networks, Neurocomputers and their applications: tez. Dokl, 2022, pp. 60-61.

Ильинская Елена Владимировна, кандидат экономических наук, доцент кафедры прикладной информатики и информационных технологий
Голышева Елизавета Николаевна, студентка кафедры прикладной информатики и информационных технологий, институт инженерных и цифровых технологий
Медведев Алексей Андреевич, студент кафедры прикладной информатики и информационных технологий, институт инженерных и цифровых технологий
Масалитин Никита Сергеевич, студент кафедры прикладной информатики и информационных технологий, институт инженерных и цифровых технологий

Ilyinskaya Elena Vladimirovna, Candidate of Economic Sciences, associate Professor of the Department of Applied Informatics and Information Technologies
Golysheva Elizaveta Nikolaevna, Bachelor's student, Department of Applied Informatics and Information Technologies, Institute of Engineering and Digital Technologies
Medvedev Alexey Andreevich, Bachelor's student, Department of Applied Informatics and Information Technologies, Institute of Engineering and Digital Technologies
Masalitin Nikita Sergeevich, Bachelor's student, Department of Applied Informatics and Information Technologies, Institute of Engineering and Digital Technologies

УДК 004.855.5 **DOI: 10.18413/2518-1092-2024-9-1-0-9**

Мартон Н.А.[1]
Жихарев А.Г.[2]
Черных В.С.[1]

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ СБОРА ДАННЫХ И МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ РАСПОЗНАВАНИЯ ЛИЦ

[1)]Белгородский государственный национальный исследовательский университет,
ул. Победы, 85, Белгород, 308015, Россия
[2)] Белгородский государственный технологический университет им. В.Г. Шухова,
ул. Костюкова, 46, Белгород, 308012, Россия

e-mail: zhikharev@bsu.edu.ru

Аннотация
В работе представлен комплексный подход к разработке и оптимизации модели нейронной сети для эффективного распознавания лиц в динамичной среде. В частности, рассматривается разработанная авторами нейронная сеть, целью которой является распознавание ограниченного круга лиц. Для обучения нейронной сети была сформирована обучающая выборка.
В работе описывается процесс обучения нейронной сети с использованием библиотеки Keras, включая архитектуру сети, размеры слоев, функции активации и методы оптимизации. Также обсуждаются этапы предварительной обработки и подготовки исходных данных для обучения нейронной сети.
Полученные результаты исследования показывают, что разработанная нейронная сеть обладает высокими производительностью и точностью.
Ключевые слова: нейронная сеть; обучение нейронной сети; модель; слой; эмбеддинг; распознавание лиц
Для цитирования: Мартон Н.А., Жихарев А.Г., Черных В.С. Применение современных технологий сбора данных и методов машинного обучения для распознавания лиц // Научный результат. Информационные технологии. – Т.9, №1, 2024. – С. 79-87. DOI: 10.18413/2518-1092-2024-9-1-0-9

Marton N.A.[1]
Zhikharev A.G.[2]
Chernykh V.S.[1]

APPLICATION OF MODERN DATA COLLECTION TECHNOLOGIES AND MACHINE LEARNING METHODS FOR FACE RECOGNITION

[1)] Belgorod State National Research University,
85 Pobedy Str., Belgorod, 308015, Russia
[2)] Belgorod State Technological University named after V.G. Shukhov,
46 Kostyukova Str., Belgorod, 308012, Russia

e-mail: zhikharev@bsu.edu.ru

Abstract
The article presents a comprehensive approach to the development and optimization of a neural network model for effective face recognition in a dynamic environment. In particular, the neural network developed by the authors is considered, the purpose of which is to recognize a limited number of people. A training sample was formed to train the neural network.
The paper describes the process of training a neural network using the Keras library, including the network architecture, layer sizes, activation functions and optimization methods. The stages of preprocessing and preparation of initial data for training a neural network are also discussed.
The obtained research results show that the developed neural network has high performance and accuracy.
Keywords: neural network; neural network training; model; layer; embedding; face recognition

For citation: Marton N.A., Zhikharev A.G., Chernykh V.S. Application of modern data collection technologies and machine learning methods for face recognition // Research result. Information technologies. – T.9, №1, 2024. – P. 79-87. DOI: 10.18413/2518-1092-2024-9-1-0-9

ВВЕДЕНИЕ

В современном информационном обществе, на фоне стремительно развивающихся технологий, распознавание лиц становится неотъемлемой частью самых различных областей, от повседневного использования до обеспечения безопасности [1]. В данной работе будет рассмотрен процесс создания и оптимизации модели нейронной сети для эффективного распознавания лиц, работу которой мы проверили на обширном наборе данных. Помимо этого, будет рассмотрен процесс формирования обучающей выборки, а также описаны шаги предварительной обработки и подготовки исходных данных.

НАЧАЛЬНЫЕ УСЛОВИЯ

Для каждого пользователя, которого будет необходимо распознавать модели нейронной сети, необходимо подготовить набор данных, основанный на различных фото, с разными выражениями и положениями лица. Это необходимо для того, чтобы показать модели как можно больше вариантов одного и того же лица, чтобы распознать человека было возможно даже во время активного движения головой или речи.

В качестве обучающих данных были выбраны фотографии 9 человек. Для каждого человека была создана некоторая базовая коллекция изображений, которые затем подверглись аугментации, включая клонирование и деформацию. Этот процесс искусственно увеличил объем данных и их разнообразие, что поспособствовало более эффективному обучению модели. Для эксперимента для разных людей было взято разное количество фото. Это было сделано с целью проверить, насколько отличаться точность определения при различном количестве данных. Так же, для увеличения точности распознавания, на некоторых фото были использованы различные аксессуары/помехи, вроде очков или причёски.

В ходе экспериментов было выявлено, что помимо данных девяти человек, так же было необходимо определить класс “неизвестный”, который будет отвечать за неизвестных людей. Данный класс должен включать как можно больше разнообразных видов персон, разных полов, рас, возрастов и выражений лиц. Всё это необходимо для того, чтобы составить максимально расплывчатый класс, который может подойти любому человеку, не входящему в число девяти распознаваемых классов. В рамках данной работы, для класса “неизвестный” было выбрано 47 изображений людей различных полов, рас, возрастов и т.д.

Каждый набор изображений был обработан, в результате чего для каждого класса были получены различные наборы эмбеддингов, записанных в формате “.npy”, каждый из которых хранится в соответствующих папках.

ОБРАБОТКА ДАННЫХ

Получение данных для обучения нейронной сети и распознавания происходит следующим образом:

1. Получение изображения, содержащее лицо – на данном этапе над обрабатываемым фото ведётся работа по выявлению на нём лиц. Обработка статичных фото и видео реализуется с помощью функций библиотеки OpenCV, а также каскадов Хаара, импортируемых с помощью класса CascadeClassifier [3]. Функция данного класса detectMultiScale используется для поиска лица на фото, после чего найденное изображения лица записывается в специальный файл, с которым мы будем работать в следующих пунктах.

2. Получение эмбеддинга лица – на данном этапе из фото, полученного в пункте 1, получаются специальные метрики лица, которые в дальнейшем будут использоваться для

распознавания и обучения модели. Получение эмбеддингов происходят благодаря функции face_encodings, библиотеки face_recognition. Сам эмбеддинг представляет из себя массив, размером 128 элементов, в котором каждый элемент является значением от -1 до 1 [4].

3. Сохранение полученных данных: на последнем этапе обработки данные, с помощью функции np.save сохраняются в файл в формате ".npy". Далее, при необходимости, их можно будет извлечь из файлом данного формата с помощью функции np.load.

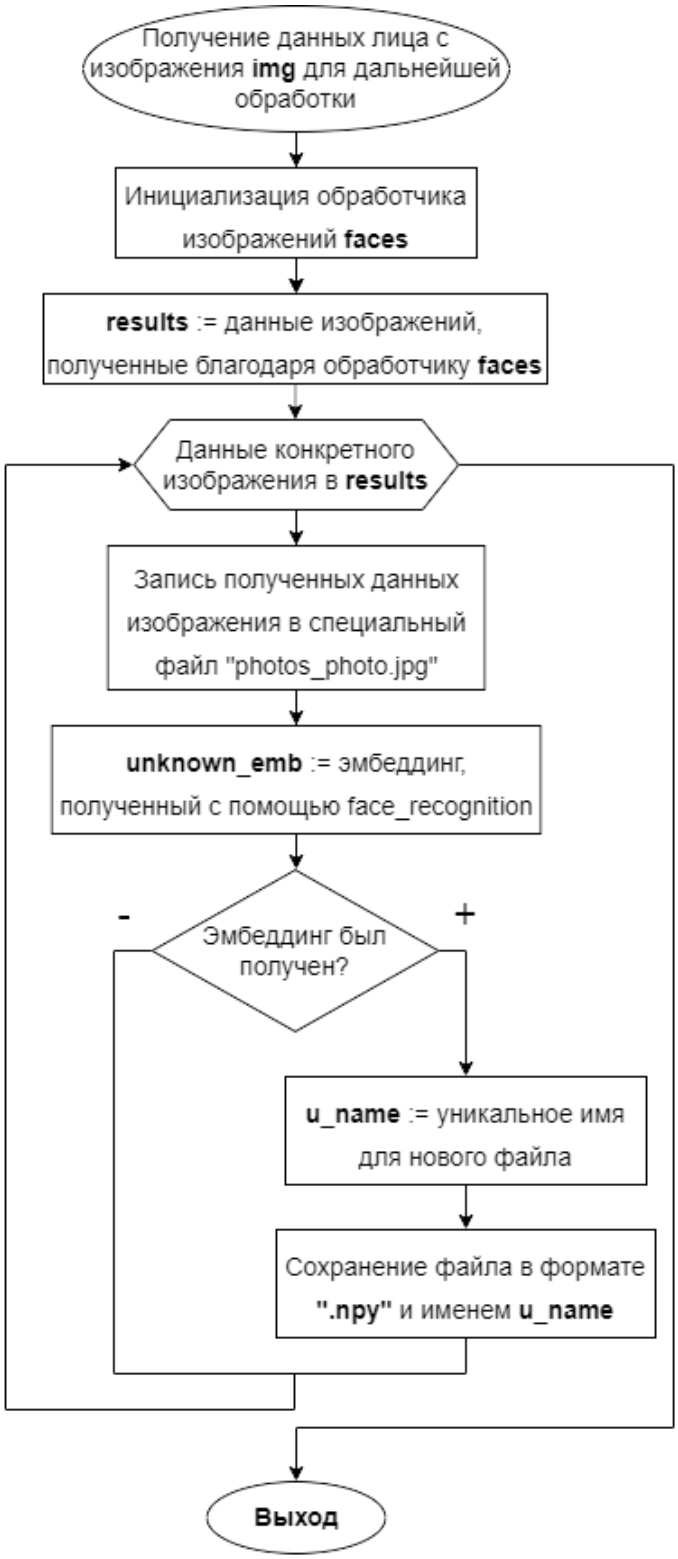


Рис. 1. Получение данных лица с изображения img
Fig. 1. Getting face data from img image

МОДЕЛЬ НЕЙРОННОЙ СЕТИ

В данной модели нейронной сети были использованы следующие слои:

BatchNormalization – данный слой нормализует входные данные путём стандартизации их по среднему значению и дисперсии. Это помогает улучшить стабильность и скорость обучения модели.

Dropout – данный слой используется для предотвращения переобучения модели путем случайного обнуления некоторых элементов выходных данных во время обучения. Это помогает улучшить обобщающую способность модели и предотвратить переобучение. На вход данному слою передаётся доля элементов, которые будет необходимо обнулить.

Dense – данные полносвязные слои применяются для классификации. Они содержат определённое количество нейронов, которые соединены со всеми нейронами предыдущего слоя. [2] На вход в данном слое подаётся количество нейронов данного слоя, функция активации нейронов, а также регулятор веса слоя, который отвечает за добавление штрафа к функции потерь, что так же способствует предотвращению переобучения модели.

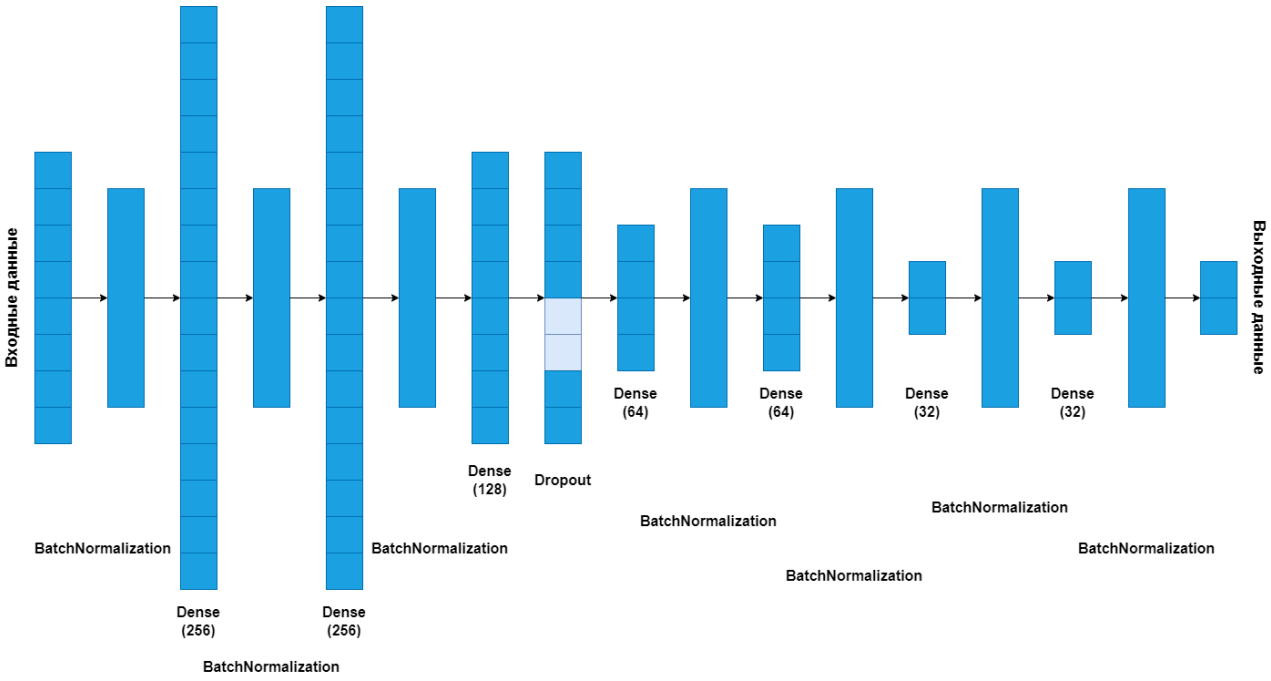


Рис. 2. Структура модели нейронной сети
Fig. 2. Structure of the neural network model

Первым слоем является BatchNormalization.

Вторым слоем является Dense с 256 нейронами, указанием формы входных данных для этого слоя в виде первого элемента в обучающем наборе данных, функцией активации tanh и L2-регулятором веса слоя со значением 0.0001. Далее во всех слоях Dense будут повторяться значения функции активации и L2-регулятора.

Третьим слоем является BatchNormalization.

Четвёртым слоем так же является Dense с 256 нейронами.

Пятым слоем является BatchNormalization.

Шестым слоем является Dense с 128 нейронами.

Седьмым слоем является Dropout со значением 0.2.

Восьмым слоем является Dense с 64 нейронами.

Девятым слоем является BatchNormalization.

Десятым слоем является Dense с 64 нейронами.

Одиннадцатым слоем является BatchNormalization.

Двенадцатым слоем является Dense с 32 нейронами.

Тринадцатым слоем является BatchNormalization.

Четырнадцатым слоем является Dense с 32 нейронами.

Пятнадцатым слоем является BatchNormalization.

Выходным слоем является Dense с количеством нейронов, равным количеству распознаваемых классов, а также функцией активации softmax.

Для разработанной модели используется функция потерь categorical_crossentropy, т.к. с помощью данной модели мы планируем решать задачу многоклассовой классификации. В то же время оптимизатор adam выбран, так как он эффективно обновляет веса модели в процессе обучения, а также обеспечивает быструю сходимость.

В ходе экспериментов во время работы над проектом были испробованы различные варианты архитектуры модели нейронной сети для распознавания лиц, и именно описанный выше вариант показал наиболее перспективные результаты, как на обучающих и тестовых данных, так и во время тестирования обученной модели на неизвестных ранее фотографиях и видео.

Так как данная модель нейронной сети предназначена для распознавания лиц людей, стоит реализовать возможность добавления новых классов к уже существующей модели, а также удаление старых. Данную возможность необходимо обеспечить, так как в организациях, в которых данная модель может быть использована, часто может меняться состав людей, которых модели необходимо опознавать. К примеру, в рамках использования внутри высшего учебного заведения, студенты добавляются и уходят в больших количествах каждый год, а значит обеспечить безопасное добавление и удаление новых классов для распознавания просто необходимо.

Добавление нового класса для распознавания реализовано следующим образом:

1. **Копируем веса и смещения последнего слоя** – на данном этапе происходит копирование весов и смещения последнего слоя модели нейронной сети, которые мы будем использовать в дальнейшем.
2. **Удаление последнего слоя –** на данном этапе мы удаляем ранее скопированный последний слой из модели нейронной сети.
3. **Создание нового слоя –** на этом этапе мы создаём новый слой модели нейронной сети, но на один нейрон больше скопированного последнего слоя. Размещение нового нейрона зависит от условий решаемой задачи.
4. **Копируем веса прошлого последнего слоя обратно –** на данном этапе происходит копирование весов предыдущего последнего слоя в новый.
5. **Инициализация веса для нового класса –** на данном этапе инициализируем веса нового класса, для чего используем средний вес.
6. **Тренировка новой модели –** на этом этапе происходит тренировка изменённой модели.

Удаление класса, в целом, похоже на добавление, и происходит следующим образом:

1. **Копируем веса и смещения последнего слоя** – на данном этапе происходит копирование весов и смещения последнего слоя модели нейронной сети, которые мы будем использовать в дальнейшем.
2. **Удаление последнего слоя –** на данном этапе мы удаляем ранее скопированный последний слой из модели нейронной сети.
3. **Создание нового слоя –** на этом этапе мы создаём новый слой модели нейронной сети, но размером на один нейрон меньше скопированного последнего слоя.
4. **Копируем веса прошлого последнего слоя обратно –** на данном этапе происходит копирование весов предыдущего последнего слоя в новый, исключая веса и смещения того класса, который нам необходимо удалить.
5. **Тренировка новой модели –** на этом этапе происходит тренировка изменённой модели.

РЕЗУЛЬТАТЫ РАБОТЫ

Исходные данные были разделены на обучающие и тестовые. Для обучения было выделено 70% исходных данных, в то время как для тестов использовались оставшиеся 30%. Само распределение данных по классам выглядело следующим образом:

Рис. 3. Распределение данных между классами
Fig. 3. Distribution of data between classes

В результате обучения спроектированной модели нейронной сети мы получили высокие показатели точности распознавания. При анализе графиков точности и потерь на этапах обучения и проверки, можно заметить, что ещё на начальных эпохах точность модели достигает высоких показателей, а потери стремятся к нулю, что свидетельствует об успешном обучении и классификации, как на обучающих, так и новых данных. Так же было выяснено, что лучшие показатели были достигнуты на 278-й эпохе обучения. Точность модели достигла до **94.83%**, в то время как потери на данном этапе составили **0.1944**.

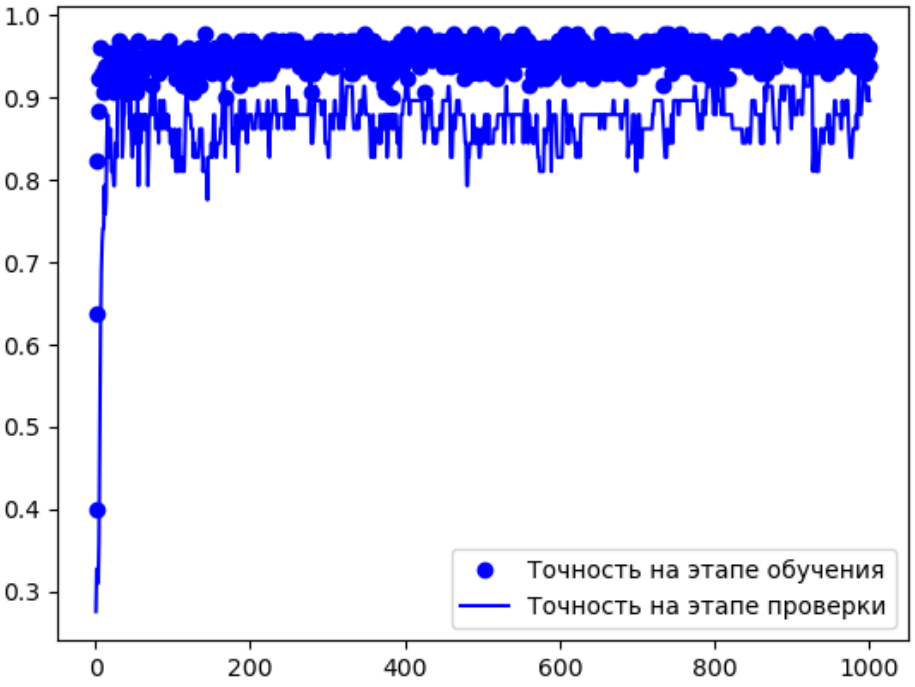


Рис. 4. Точность на этапах обучения и проверки
Fig. 4. Accuracy at the stages of training and verification

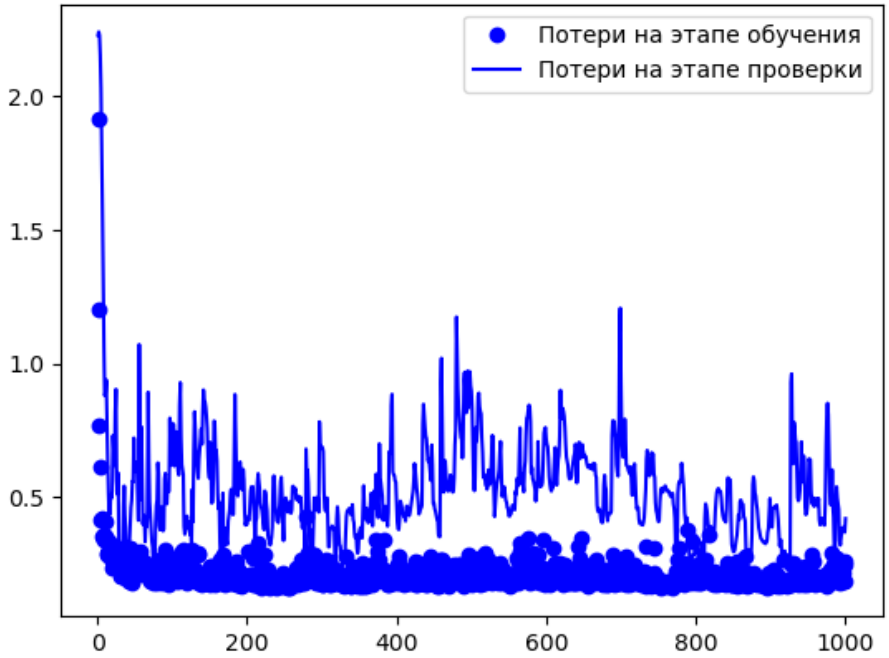


Рис. 5. Потери на этапах обучения и проверки
Fig. 5. Losses at the stages of training and verification

После обучения модель была протестирована с фотографиями, не входящими ни в набор обучающих, ни в набор тестовых данных. Так же провелось несколько тестов с использованием видеокамеры. В тестировании принимали участие, как персоны, распознавать которых модель была обучена, так и ранее неизвестные ей лица.

Таблица 1

Тестирование обученной модели

Table 1

Testing the trained model

	Тест фото 1	Тест фото 2	Тест фото 3	Тест камера 1	Тест камеры 2
Известный 1	99.94%	99.92%	98.37%	99.97%	99.54%
Известный 2	99.99%	99.98%	94.03%	99.77%	99.98%
Неизвестный 1	74.59%	96.66%	89.24%	73.77%	83.87%
Неизвестный 2	46.38%	92.4%	93.01%	81.95%	61.17%

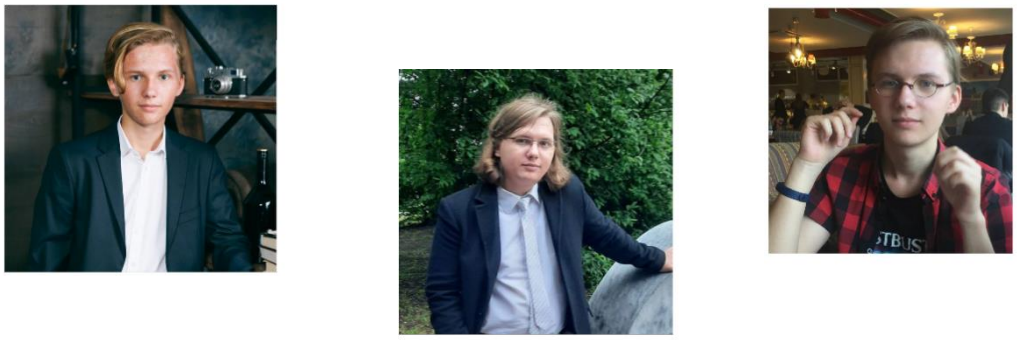


Рис. 6. Примеры фото обучающего набора Мужчины 8
Fig. 6. Examples of photos of the training set Men 8

Рис. 7. Успешно распознанное фото Мужчины 8, не входящее в обучающий набор
Fig. 7. Successfully recognized photo of Man 8, not included in the training set

В результате тестирования можно прийти к выводам, что получившаяся модель отлично распознаёт тех людей, которых была обучена распознавать, а также в большей степени хорошо распознаёт, если человек ей неизвестен.

ЗАКЛЮЧАНИЕ

Благодаря библиотекам Keras и face-recognition нами была разработана модель нейронной сети, показавшая высокую точность распознавания и довольно низкие потери. Графики точности и потерь подтверждают успешность обучения модели, которая достигла наилучших показателей на 278-й эпохе обучения с точностью в 94.83% и потерями в 0.1944.

Дальнейшее улучшение получившейся модели можно реализовать благодаря увеличению размера обучающего набора данных, особенно отмечая увеличение класса “неизвестный”, что улучшит большую обобщающую способность модели.

Список литературы

1. Шолле Ф. Глубокое обучение на Python. 2-е межд. издание / Ф. Шолле; – СПб.: Питер, 2023. – 576 с. – ISBN 978-5-4461-1909-7

2. Жихарев А.Г., Черных В.С. Классификация речевых данных по эмоциональному фону // Научный результат. Информационные технологии. – Т.8, №3, 2023. – С. 34-44. DOI: 10.18413/2518-1092-2022-8-3-0-5

3. Визуализация каскадов Хаара. [Электронный ресурс] – Электрон, дан., 2020. – URL: https://habr.com/ru/articles/504288/

4. Техническая документация библиотеки face-recognition. [Электронный ресурс] — Электрон, дан., 2020. – URL: https://libraries.io/pypi/face-recognition

References

1. Chollet F. Deep Learning with Python. 2nd interd. edition / F. Chollet; – Spb.: St. Petersburg, —2023. – 576 p. – ISBN 978-5-4461-1909-7

2. Zhikharev A.G., Chernykh V.S. Classification of speech data by emotional background // Research result. Information technologies. – T.8, №3, 2023. – P. 34-44 DOI: 10.18413/2518-1092-2022-8-3-0-5

3. Visualization of Haar cascades. [Electronic resource] – Electronic data, 2020. – URL: https://habr.com/ru/articles/504288/

4. Technical documentation of the face-recognition library. [Electronic resource] – Electronic data, 2020. – URL: https://libraries.io/pypi/face-recognition

Мартон Никита Андреевич, студент 1 курса магистратуры, кафедры прикладной информатики и информационных технологий, институт инженерных и цифровых технологий
Жихарев Александр Геннадиевич, доктор технических наук, доцент, доцент кафедры программного обеспечения вычислительной техники и автоматизированных систем
Черных Владимир Сергеевич, студент 1 курса магистратуры кафедры информационных и робототехнических систем, институт инженерных и цифровых технологий

Marton Nikita Andreevich, 1st year Master's student, Department of Applied Informatics and Information Technologies, Institute of Engineering and Digital Technologies
Zhikharev Alexander Gennadievich, Doctor of Technical Sciences, Associate Professor, Associate Professor of the Department of Software for Computer Engineering and Automated Systems
Chernykh Vladimir Sergeevich, 1st year Master's student, Department of Information and Robotic Systems, Institute of Engineering and Digital Technologies