REDS:

Телекоммуникационные устройства и системы

№3

2025

СОДЕРЖАНИЕ

АНАЛИЗ ВЛИЯНИЯ СТИЛЯ НАПИСАНИЯ КОДА НА ЭФФЕКТИВНОСТЬ ГЕНЕРИРУЕМОГО МАШИННОГО КОДА

Гадасин Денис Вадимович
МТУСИ, доцент кафедры СИТиС, к.т.н., Москва, Россия
dengadiplom@mail.ru

Савкин Дмитрий Игоревич
МТУСИ, студент группы М092401(75), Москва, Россия
dima.savkin.2002@mail.ru

Маклачкова Виктория Валентиновна
МТУСИ, старший преподаватель кафедры СИТиС, Москва, Россия
v.v.maklachkova@mtuci.ru

Гадасин Даниил Денисович
МТУСИ, студент группы БСТ2103, Москва, Россия
gadasin115@gmail.com

Аннотация
В работе проведено исследование различных способов оптимизации программного кода, используемых компилятором языка C++, с целью уменьшения объёма генерируемого машинного кода и, как следствие, повышения производительности информационной системы. Продемонстрированы результаты работы компилятора путём дизассемблирования получившихся исполняемых файлов. Использование языковых конструкций языка позволило сообщить компилятору информацию, достаточную для построения обоснованных гипотез о потенциальных оптимизациях. Приведён пример использования различных контейнеров данных, а также показаны возникающие издержки, которые выражаются в дополнительном объёме машинного кода, необязательно связанного с непосредственным решением поставленной задачи предметной области.

Ключевые слова
Производительность, оптимизация, компиляторы, C++, библиотека C++, язык программирования

Введение

Оптимизация производительности программного обеспечения является важнейшим аспектом, напрямую влияющим на эффективность и скорость выполнения машинных инструкций. Одним из ключевых факторов, определяющих производительность, является количество обращений к оперативному запоминающему устройству (ОЗУ) и взаимодействие с кэшами L1, L2 и L3 уровней. Реорганизация внутренней структуры высокоуровневых объектов позволяет добиться более «плотного» их расположения в памяти, что в свою очередь увеличивает вероятность попадания в линию кэша и, как следствие, улучшает общую производительность системы.

Однако оптимизация структуры высокоуровневых объектов и их размещения в памяти может быть недостаточной для достижения максимальных показателей производительности. Немаловажным фактором также является прикладное создание и использование высокоуровневых объектов, особенно если речь идёт об объектах стандартной библиотеки. Некорректное и неэффективное использование подобных объектов зачастую приводит к генерации избыточного машинного кода, который не несёт значимой смысловой нагрузки в контексте выполняемой задачи предметной области. Это происходит из-за несоблюдения тех шаблонов и практик написания программного кода, которые были изначально задуманы разработчиками компиляторов для обеспечения наилучших условий предстоящих оптимизаций [1-4].

Опыт большинства разработчиков показывает, что попытка предугадать, какие оптимизации будут применены компилятором, может быть сравнима со случайным процессом, подобным подбрасыванию монеты. Тем не менее, существует определённый набор идиоматических правил и рекомендаций по написанию кода, следование которым может существенно помочь компилятору в принятии решения об оптимизации того или иного участка и, как следствие, повысить эффективность и производительность системы.

В рамках данной статьи выделяются два фундаментальных принципа написания оптимального

программного кода: «выполнять минимальный объем работы для завершения поставленной задачи» и «простое решение почти всегда является лучшим решением». Рассмотрим, как применение этих принципов и идиоматических правил может помочь в достижении наилучшей оптимизации генерируемого машинного кода, а также приведём примеры того, как неправильное использование объектов стандартной библиотеки может привести к неоправданному росту количества инструкций, выполняемых центральным процессорным устройством (ЦПУ).

Оптимизация строковых объектов

Программные продукты большую часть времени работают с пользовательским вводом в виде строк. Таким образом, строковые объекты представляются чрезвычайно важным инструментом в большом спектре решаемых задач предметной области. Компиляторы языка C++ предоставляют возможность оптимизировать некоторые строковые операции, значительно уменьшив объём генерируемого машинного кода. Так, чтобы узнать количество символов в предопределённой строке необходимо создать высокоуровневый объект с данной строкой, а затем вызвать функцию подсчёта символов. В случае, когда выражение представляет собой единичный вызов данной функции, компилятор легко оптимизирует его, оставляя на выходе единичную инструкцию копирования целого числа в регистр ЦПУ [5]. Таким образом, компилятор предвидел дальнейшее использование строки и принял во внимание тот факт, что на самом деле требуется не сама строка, а лишь количество символов в ней (рис. 1).

```
int main() {
  return std::string("savkin");
}
-----------------------------------------
main:
    mov   eax, 6
    ret
```

Рис. 1. Оптимизация вызова функции подсчёта количества символов предопределённой строки (сверху – программный код; снизу – машинный код)

К сожалению, случай такого выражения является довольно специфическим. Так, если выражение состоит из двух и более вызовов функций подсчёта количества символов в строке, то оптимизации не происходит и генерируемый машинный код разрастается до немалых объёмов (рис. 2).

```
int main() {
  return std::string("savkin").size() +
    std::string("dmitry").size();
}
-------------------------------------------------------
main:
    push   rbx
    mov    edx, OFFSET FLAT:.LC2+6
    mov    esi, OFFSET FLAT:.LC2
    sub    rsp, 64
    lea    rax, [rsp+16]
    call    void std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >::_M_construct<char
const*>(char const*, char const*, std::forward_iterator_tag) [clone
.isra.14]
    ...
```

Рис. 2. Оптимизация вызова функции подсчёта количества символов двух строк

Говоря о строковых данных, зачастую возникает необходимость сделать строковый объект частью другого объекта. Так, строковый объект становится т.н. полем другого высокоуровневого объекта. Рассмотрим это на примере абстрактного объекта физического лица, представленного в

структуре Person (рис. 3).

Сгенерированный компилятором машинный код схож с тем, что показан на предыдущем рисунке. Для вызова функции подсчёта количества символов в строке имени физического лица необходимо:

1. выделить на программном стеке необходимое количество байт для создания временного объекта строки с именем;
2. выделить на программного стеке необходимое количество байт для создания временного объекта физического лица;
3. сконструировать и инициализировать строковый объект с необходимым именем;
4. сконструировать и инициализировать объект физического лица, передав в качестве параметра строковый объект;
5. вызвать функцию подсчёта у объекта физического лица.

Пункт №4 представляет наибольший интерес, т.к. является самым ресурсоёмким с точки зрения компилятора и генерируемого машинного кода. Совершенно очевидно, что во многом это связано с необходимостью создания временного строкового объекта на программном стеке, а также с последующей передачей этого объекта в конструктор объекта физического лица [6-9].

```
struct Person {
  std::string name_;

  Person(std::string name) {name_ = name;}
  int name_length() const {return name_.size();}
};

int main() {
  return Person("alex").name_length();
}
```

```
main:
    push   rbx
    sub    rsp, 64
    lea    rax, [rsp+16]
    lea    rdi, [rsp+32]
    mov    rsi, rsp
    mov    DWORD PTR [rsp+16], 2019912801
    mov    QWORD PTR [rsp+8], 4
    mov    QWORD PTR [rsp], rax
    lea    rax, [rsp+48]
    mov    BYTE PTR [rsp+20], 0
    mov    QWORD PTR [rsp+40], 0
    mov    BYTE PTR [rsp+48], 0
    mov    QWORD PTR [rsp+32], rax
    call   std::__cxx11::basic_string<char, std::char_traits<char>, std::alloca-
tor<char> >::_M_assign(std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> > const&)
    mov    rdi, QWORD PTR [rsp+32]
    lea    rax, [rsp+48]
    mov    rbx, QWORD PTR [rsp+40]
    ...
```

Рис. 3. Абстрактный объект со строковым объектом в качестве поля

В данном примере наблюдается неполное соответствие действий разработчика и компилятора. Это сравнимо с тем, как коренной житель страны пытается понять речь иностранца, который выучил лишь базовые правила и конструкции языка, на котором происходит коммуникация [10]. Исходный код,

написанный на языке программирования, – это язык общения с компилятором. Таким образом, чтобы добиться максимальной оптимизации, необходимо «разговаривать» с компилятором на языке, который был бы ему максимально «понятен».

В примере рисунке 3 можно выделить следующие допущения:

1) время жизни временного строкового объекта не превышает время жизни временного объекта физического лица;

2) строковый объект используется лишь для создания объекта физического лица;

3) имя объекта физического лица представляет собой неизменяемую информацию;

4) объект физического лица управляет жизненным циклом своих внутренних объектов, представленных в виде свойств.

```
struct Person {
  const std::string name_;

  Person(std::string name) :
name_{std::move(name)} {}
  int name_length() const {return name_.size();}
};

int main() {
  return Person("alex").name_length();
}
-----------------------------------------
main:
    mov   eax, 4
    ret
```

Рис. 4. Улучшенный абстрактный объект со строковым объектов в качестве поля

Рациональное использование языковых конструкций позволяет сообщить компилятору информацию о тех допущениях, которые следует учесть в процессе оптимизации. Это позволяет компилятору сформулировать обоснованные гипотезы, которые могут лечь в основу тех или иных оптимизаций, тем самым повысив шанс значительно уменьшить генерируемый объём машинного кода [11-14].

Рассмотрим, как использование языковых конструкций помогло компилятору выстроить необходимые гипотезы и, как следствие, произвести оптимизации. В момент создания объекта физического лица происходит вызов его конструктора с последующей передачей временного объекта строки в качестве аргумента. Данная операция имеет алгоритмическую сложность $O(n)$, т.к. требуется посимвольное копирование всей строки в новый безымянный временный объект, время жизни которого ограничено областью видимости конструктора. Заметим, что на момент вызова тела конструктора все поля создаваемого объекта уже созданы и проинициализированы по умолчанию (данная операция имеет алгоритмическую сложность $O(n)$, где n – это количество полей создаваемого объекта). Таким образом, операция присваивания нового значения в уже проинициализированный объект приведёт к уничтожению существующего объекта и инициализации нового, что также имеет алгоритмическую сложность $O(n)$. Наконец, временный объект строки, который был передан в качестве аргумента в конструктор объекта физического лица, должен быть уничтожен, т.к. его время жизни завершено (данная операция имеет некую алгоритмическую сложность A). Таким образом, алгоритмическая сложность всей программы выражается суммой $O(n) + O(n) + O(n) + A$.

Оптимизированная версия программы лишена многих издержек, которые описаны выше. Использование списка инициализации вместо тела конструктора позволяет избавиться от «холостой» инициализации строкового поля и произвести инициализацию непосредственно значением, переданным в качестве аргумента. Более того, если бы поле имело константный квалификатор, то использование списка инициализации было бы единственным возможным способом сохранить нужное строковое значение. Компилятор понимает, что время жизни временного объекта строки, переданного в качестве аргумента, завершится к моменту создания объекта физического лица. Это позволяет ему опустить создание этого объекта с его последующим копированием и произвести инициализацию поля имени объекта физического лица непосредственным строковым значением «на месте». Таким образом, алгоритмическая сложность всей программы выражается суммой $O(n) + A$.

Оптимизация контейнеров

Многие задачи предметной области сводятся к обработке не единичных объектов, а их некоторого объёма, представленного в виде множества этих объектов. Таким образом, перед разработчиком стоит вопрос выбора контейнера для хранения объектов и их последующей обработки [15].

```
int main()
{
std::list<int> v{37};
}
```

```
main:
  push  r12
  push  rbp
  mov   edi, 24
  push  rbx
  sub   rsp, 32
  mov   QWORD PTR [rsp+16], 0
  mov   rbx, rsp
  mov   QWORD PTR [rsp], rsp
  mov   QWORD PTR [rsp+8], rsp
  ...
```

```
int main()
{
std::vector<int> v{37};
}
```

```
main:
  sub   rsp, 8
  mov   edi, 4
  call  operator new(unsigned
long)
  mov   DWORD PTR [rax], 37
  mov   rdi, rax
  call  operator delete(void*)
  xor   eax, eax
  add   rsp, 8
  ret
```

```
int main()
{
std::array<int, 5> v{37};
}
```

```
main:
  xor   eax, eax
  ret
```

Рис. 5. Оптимизация на основе выбранного контейнера для хранения объектов

Стандартная библиотека языка C++ предоставляет на выбор три контейнера объектов: фиксированный массив, динамический массив и список. На рисунке 5 представлен пример хранения единичного числового значения в каждом из трёх контейнеров.

Использование фиксированного массива привело к генерации наименьшего количества машинного кода, который не содержит ни единой инструкции, связанной с используемым объектом фиксированного массива.

Использование динамического массива привело к генерации небольшого количества машинного кода. В области программной кучи выделяется небольшое пространство для сохраняемого типа данных. В данную область записывается необходимое значение, а после — она освобождается средствами операционной системы, чтобы избежать непосредственной утечки памяти. Примечательно, что получившийся машинный код полностью эквивалентен тому, как если бы разработчик самостоятельно выделил участок памяти в области кучи, записал значение, а затем освободил выделенную память. Таким образом, динамический массив инкапсулирует ручную работу с памятью, практически не добавляя ничего лишнего в генерируемые инструкции.

Использование списка привело к генерации значительного количества машинного кода. Стандартная библиотека предполагает выполнения множества дополнительных процедур, которые необходимы для правильного функционирования списка. Тем не менее, подобные издержки могут быть непозволительными в критически важных участках кода, выполнение которых непосредственно влияет на общую производительность системы [16].

Нахождение чисел Фибоначчи. Рассмотрим практическую задачу составления ряда чисел Фибоначчи. Программное решение представлено в двух вариантах: с использованием динамического массива и списка, соответственно. Разработанные программы выполняют следующую последовательность действий:

1) инициализируют объект контейнера и заполняют его первоначальными значениями a_0, численно равное нулю, и a_1, численно равное единице;

2) считывают значение a_{n-1} во временную переменную x;

3) считывают значение a_{n-2} во временную переменную y;

4) вычисляют результат арифметической суммы a_{n-1} и a_{n-2} для получения значения a_n;

5) помещают значение a_n в контейнер.

Шаги 2-5 выполняются циклично до тех пор, пока контейнер не будет содержать необходимое количество чисел последовательности, значение которого предопределено в рамках каждого тестового запуска индивидуально.

Профилирование программного кода, реализующего вышеописанные шаги, производилось путём подсчёта количества прошедших тактов со времени начала алгоритма до его конца с помощью ассемблерной инструкции RDTSC, которая возвращает метку времени ЦПУ. Результаты профилирования представлены в таблицах 1 и 2.

Заметим, что среднее время выполнения итерации на основе списка превышает среднее время выполнения итерации на основе динамического массива в 4.84 раза. Таким образом, максимальный уровень оптимизации, достигаемый компилятором, жёстко связан с выбором конкретного контейнера из стандартной библиотеки языка.

Таблица 1

Номер теста	Количество чисел (тыс.)	Время выполнения (такт)	Среднее время итерации (такт)
1	10	188981	19
2	250	3866542	16
3	1000	16070188	16
4	30000	548478512	18

Таблица 2

Номер теста	Количество чисел (тыс.)	Время выполнения (такт)	Среднее время итерации (такт)
1	10	827727	83
2	250	23666131	95
3	1000	77559759	76
4	30000	2400354950	80

Иными словами, для генерации максимального эффективного машинного кода необходимо грамотно подходить к выбору используемых высокоуровневых объектов и сопутствующих вспомогательных средств языка, т.к. применение компилятором даже самых современных алгоритмов оптимизации даёт ощутимую разницу в производительности времени выполнения в различных, хоть и семантически похожих вариантах решения задачи предметной области [17].

Заключение

Эффективность и производительность программного обеспечения напрямую зависит от качества написанного кода и его соответствия тем шаблонам, которые были заложены разработчиками компиляторов. Пренебрежение устоявшимся правилам написания и нерациональное использование объектов стандартной библиотеки может привести к тому, что компилятор не сможет эффективно произвести оптимизацию, что, в свою очередь, приведёт к разрастанию объёма машинного кода и значительному снижению метрик производительности информационной системы [18-26].

Язык программирования является ничем иным как языком общения разработчика и компилятора. Таким образом, чтобы добиться максимально эффективного результата, разработчику требуется сообщить компилятору не только информацию о способе решении поставленной задачи предметной области, но и информацию о допущениях, которые помогут построить обоснованные гипотезы касательно потенциальной оптимизации того или иного участка кода.

Литература

1. *Гадасин Д.В., Лисиненко Е.К., Юсифов Э.С., Савин В.А*. Оценка регрессионных моделей исходя из показателей качества // Системы синхронизации, формирования и обработки сигналов. 2024. Т. 15, № 1. С. 4-16. EDN CSWKOE

2. *Данченко Д.Г*. Операционные системы реального времени // Форум молодых ученых. 2018. №1 (17). URL: https://cyberleninka.ru/article/n/operatsionnye-sistemy-realnogo-vremeni.

3. *Гадасин Д.В., Шведов А.В., Кузин И.А*. Трехмерная реконструкции объекта по одному изображению с использованием глубоких свёрточных нейронных сетей // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16, № 7. С. 29-35. DOI 10.36724/2072-8735-2022-16-7-29-35. EDN YTLCNW

4. *Гадасин Д.В., Вакурин И.С., Тремасова Л.А*. Алгоритм распределения данных между системами хранения на основе свойства самоподобия // Электросвязь. 2024. № 4. С. 44-50. DOI 10.34832/ELSV.2024.53.4.007. EDN BRSLCL

5. *Гадасин Д.В., Бессолицын А.Д*. Виды и методы структурирования данных из различных информационных систем: анализ и применение // Актуальные проблемы и перспективы развития экономики, Симферополь – Гурзуф, 12–14 октября 2023 г. Симферополь: ИП Зуева Т. В., 2023. С. 202-204. EDN UGZRXL

6. *Гадасин Д.В., Пантелеева К.А*. Использование формант для распознавания человеческой речи искусственным интеллектом // Молодежь. Техника. Космос : Труды пятнадцатой общероссийской молодёжной научно-технической конференции. В 4-х томах, Санкт-Петербург, 20-24 марта 2023 г. Санкт-Петербург: Балтийский государственный технический университет "Военмех", 2023. С. 15-20. EDN OJHZBA

7. *Гадасин Д.В., Шведов А.В*. Применение транспортной задачи для балансировки нагрузки в условиях нечеткости исходных данных // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18, № 1. С. 13-20. DOI 10.36724/2072-8735-2024-18-1-13-20. EDN WKNPIX

8. *Матренин П.В.* Использование принципов объектно-ориентированного программирования при реализации оптимизационных алгоритмов // Объектные системы. 2015. №10. URL: https://cyberleninka.ru/article/n/ispolzovanie-printsipov-obektno-orientirovannogo-programmirovaniya-pri-realizatsii-optimizatsionnyh-algoritmov.

9. *Романов С.С*. Ключевые понятия и особенности объектно-ориентированного программирования // Таврический научный обозреватель. 2016. №12-2 (17). URL: https://cyberleninka.ru/article/n/klyuchevye-ponyatiya-i-osobennosti-obektno-orientirovannogo-programmirovaniya.

10. *Гадасин Д.В., Назаренко С.С., Тремасова Л.А.* Особенности проведения практических занятий по дисциплине «Принципы построения систем управления базами данных и знания» // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2023. Т. 12, № 1. С. 21-31. EDN FGSGBK

11. *Шведов А.В., Гадасин Д.В., Клыгина О.Г., Тремасова Л.А*. Оптимизация маршрутизации в сети при помощи гамильтонова цикла и марковского процесса принятия решений // DSPA: Вопросы применения цифровой обработки сигналов. 2023. Т. 13, № 3. С. 42-49. EDN BSWDEQ

12. *Гадасин Д.В., Шведов А.В., Егорова Ю.Д., Шайдулина И.Р.* Применение метода мажоритарного кодирования для определения оптимального маршрута передачи данных в сети // DSPA: Вопросы применения цифровой обработки сигналов. 2023. Т. 13, № 1. С. 20-30. EDN IECPBA

13. *Гадасин Д.В., К.А. Пантелеева, Маклачков К.А*. Разработка единой точки входа сообщений о пользовательском негативном опыте взаимодействия с web-сервисами // Искусственный интеллект в автоматизированных системах управления и обработки данных : Сборник статей II Всероссийской научной конференции. В 5-ти томах, Москва, 27-28 апреля 2023 года. М.: Издательский дом КДУ, "Добросвет", 2024. С. 413-417. EDN ADRGFV

14. *Гадасин Д.В., Первухина А.А*. Группировка узлов передачи данных с использованием метода к-средних для создания кластеров // Теория и практика экономики и предпринимательства : Труды XXI Международной научно-практической конференции, Симферополь – Гурзуф, 18-20 апреля 2024 года. Симферополь: ИП Зуева Т. В., 2024. С. 233-236. EDN IAHHLX

15. *Panteleeva K.A., Shvedov A.V., Gadasin D.D., Gadasin D.V.* Determining the Amount of Information in One Information Bit of Text Data // 2023 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russian Federation, 2023, pp. 1-5, doi: 10.1109/IEEECONF56737.2023.10091972.

16. *Shevelev S.V., Shvedov A.V., Gadasin D.V., Vakurin I.S*. Syntax and Probability Vectors in Search Query // 2023 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), St. Petersburg, Russian Federation, 2023, pp. 1-8, doi: 10.1109/WECONF57201.2023.10148008.

17. *Melkova E.K., Shvedov A.V., Korovushkina V.M., Gadasin D.V.* Cluster Implementation Based on the Belonging Function // 2023 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO, Pskov, Russian Federation, 2023, pp. 1-6, doi: 10.1109/SYNCHROINFO57872.2023.10178611.

18. *Shvedov A.V., Gadasin D.V., Klygina O.G., Tremasova L.A*. Optimization of Network Routing Using the Markov Decision Process and Hamiltonian Cycle // 2023 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russian Federation, 2023, pp. 1-4, doi: 10.1109/IEEECONF56737.2023.10091989.

19. *Тремасова Л.А., Первухина А.А., Гадасин Д.В.* Использование методов Косарайю и k-средних для формирования кластеров // Электросвязь. 2024. № 9. С. 47-55. DOI 10.34832/ELSV.2024.58.9.007. EDN DOZTZK

20. *Гадасин Д.В*. Построение бинарного дерева минимальной цены // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18, № 11. С. 38-44. DOI 10.36724/2072-8735-2024-18-11-38-44. EDN GMCEWG

21. *Назаров М.Д., Шведов А.В.* Корреляция атрибутов соглашения об уровне обслуживания с основными параметрами QoS в корпоративных сетях // Телекоммуникации и информационные технологии. 2020. Т. 7. № 2. С. 73-79. EDN: VQHDTJ

22. *Kalmykov N.S., Dokuchaev V.A.* Segment routing as a basis for software defined network // T-Comm. 2021. Т. 15. № 7. С. 50-54. EDN: LYVZCV

23. *Dokuchaev V.A., Maklachkova V.V., Statev V.Yu.* Classification of personal data security threats in information systems // T-Comm. 2020. Т. 14. № 1. С. 56-60. EDN: QOGYHH

24. *Докучаев В.А., Маклачкова В.В., Статьев В.Ю.* Цифровизация субъекта персональных данных // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 6. С. 27-32. EDN: XVWYJP

25. *Pavlov S.V., Dokuchaev V.A., Mytenkov S.S.* Model of a fuzzy dynamic decision support system // T-Comm. 2020. Т. 14. № 9. С. 43-47. EDN: VYFNLB

26. *Кузин И.А., Гадасин Д.В.* Модель контейнера данных для минимизации трафика при передаче субъективных характеристик объектов на изображении трехмерной сцены // Телекоммуникации и информационные технологии. 2021. Т. 8. № 2. С. 96-100. EDN: TYFFBH

БЕЗОПАСНОСТЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аллик Илья Андреевич
Московский технический университет связи и информатики, магистр, Москва, Россия
iallik@mail.ru

Панков Константин Николаевич
МТУСИ, доцент кафедры «Информационная безопасность», к.ф.-м.н., доцент, Москва, Россия
pankov_kn@mtuci.ru

Аннотация
В данной работе рассматривается влияние искусственного интеллекта на бизнес и безопасность. Описаны риски, связанные с уязвимостями искусственного интеллекта, примеры инцидентов, методы защиты, включая MLSecOps, и меры обеспечения безопасности данных и моделей. Подчёркивается важность регулирования и развития подходов к информационной безопасности.

Ключевые слова
Искусственный интеллект, информационная безопасность, MLSecOps, большие языковые модели, LLM, уязвимость, криптография

Введение

В настоящее время искусственный интеллект (далее – ИИ) оказывает значительное влияние на государственные и бизнес-процессы [1], преобразуя их и снижая затраты. Генеральные ИИ-системы создают уникальный контент и применяются в различных сферах, включая оценку кредитоспособности и противодействие мошенничеству. Однако компании и организации должны учитывать риски, связанные с технологией, этикой и, главное, с информационной безопасностью (далее - ИБ).

На сегодняшний день Россия уже утвердила отдельные принципы, регулирующие использование и развитие искусственного интеллекта. Правительство России модернизирует регуляторную базу, приняв “Национальную стратегию развития ИИ до 2030 года” [2], которая включает цели по стимулированию исследований разработки инфраструктуры, подготовки специалистов и обеспечению защиты данных. Вместе с тем, ИИ играет двойственную роль в безопасности: он повышает эффективность систем информационной безопасности, но также несет и риски нарушения безопасности (далее по тексту работы представлены реальные случаи, подтверждающие данное утверждение). Методы машинного обучения и большие языковые модели (далее LLM) также подвержены уязвимостям и атакам, таким как состязательные примеры, отравление данных, инверсия модели или кража модели.

ИИ значительно улучшает ИБ, предлагая новейшие подходы к защите систем и борьбе с киберугрозами. Например, использование машинного обучения при проведении статического и динамического анализа кода помогает эффективно распознать паттерны уязвимостей в новом коде.

ИИ уже активно используется в различных областях, таких как маркетинг и продажи, клиентский сервис, разработка программного обеспечения (далее – ПО), медицина, военные технологии и банковское дело, что подтверждается многочисленными публикациями. В нынешнем 2025 году, когда бизнес активно внедряет ИИ, возникает вопрос безопасности и рисков.

Вопрос безопасности для ИИ недавно сформировался, но уже привлек внимание корпораций и ряда государственных организаций. На фоне прогнозов, что технология ИИ увеличит доход предприятий, появляется вопрос рисков технологии. По статистике, приводимой в ряде источников, 61% руководителей признают главной проблемой контроля за безопасностью ИИ внутренние “теневые” решения. 77% компаний обнаружили нарушения ИИ за последний год, остальные 23% не уверены [2]. Недостаточный контроль за безопасностью ИИ приводит к финансовым убыткам, угрозе репутации, а в ближайшем будущем и нарушению законодательства.

Размер рынка ИИ в безопасности оценивается в 25 млрд долл. в 2024 году и, как ожидается, достигнет эквивалента 60 млрд долл. в нынешних ценах к 2029 году, а среднегодовой рост составит приблизительно 19% [3]. Оценка основывается на наличии больших объемов информации об уязвимостях, открытых кодовых баз, работе сетей и устройств. Это создает крепкий фундамент для проектов по автоматизации ИБ на основе ИИ.

Согласно опросу технических директоров 100 крупнейших компаний РФ в 15 индустриях, проведенному “Яков и Партнеры” [4], более 40% Российских компаний находятся на этапе внедрения ИИ-решений в различные функции. Полный экономический потенциал ИИ в России к 2028 году составит 22-36 трлн рублей в номинальных ценах, а реализованный эффект к 2028 году может достичь 4-6 трлн рублей, что эквивалентно влиянию на ВВП до 4%. В абсолютном выражении около 70% потенциала приходится на шесть ключевых для российской экономики отраслей.

Многие организации не понимают, какие угрозы может представлять искусственный интеллект, поскольку у них нет необходимых инструментов для обеспечения видимости и управления политикой для его мониторинга, не говоря уже о предотвращении утечек данных или других видов рисков, связанных с инструментами искусственного интеллекта. Результатом этого становятся инциденты информационной безопасности. Например утечка данных компании Samsung, когда сотрудники компании раскрыли данные, проводя проверку кода и внутренних документов при помощи ChatGPT [5]; чат-бота с искусственным интеллектом дилерского центра Chevrolet при помощи манипуляции ответами заставили предложить модель Tahoe стоимостью 76 000 долл. всего за 1 доллар [6]; или случай, когда чат-бот компании Google, Bard ИИ, в ответах на запросы пользователей распространял дезинформацию во время демонстрации космического телескопа Джеймса Уэбба. Ошибка привела к немедленному падению курса акций Alphabet, сократив стоимость компании на 100 млрд долл. [7]. Все вышеперечисленные инциденты произошли в 2023 году, что показывает, насколько актуальна поднимаемая проблема.

На основе текущей повестки различными исследователями предлагаются два направления для запуска задач на предприятиях, использующих ИИ:

1. Создание MLSecOps и его внедрение в процессы производства ИИ-продуктов
2. Запуск новых продуктов ИИ для задач ИБ

В данной работе рассмотрено первое направление.

Современное состояние проблемы

Перед рассмотрением вопроса обеспечения информационной безопасности ИИ, необходимо обговорить меры, обеспечивающие безопасность хоста. Это первостепенная задача, так как скомпрометированный хост может привести к несанкционированному доступу, утечке данных и другим инцидентам безопасности.

К мерам, обеспечивающим безопасность хоста, можно отнести [8]:

- Регулярные обновления;
- Использование наименьшего количества ПО;
- Использование системы контроля доступа (аутентификация, возможно, с использованием квантовых [9] и постквантовых алгоритмов [10], что актуально в условиях существующей квантовой угрозы [11] и разграничение доступов);
- Правильная конфигурация фаервола;
- Мониторинг системы;
- Проведение аудита системы;
- Обеспечение безопасности конечных точек;
- Использование резервного копирования для восстановления системы;
- Защита сети (использование TLS/SSL);

Безопасность ИИ отличается от традиционной кибербезопасности. Согласно Microsoft, связано это с особенностями обучающих способностей ИИ и процессов принятия решений [12]. Перечислим некоторые ключевые различия:

1. ИИ-системы добавляют новые уровни сложности в кибербезопасность. Традиционная кибербезопасность в основном занимается такими угрозами, как вредоносное ПО, фишинговые атаки и сетевые вторжения. Однако ИИ-системы могут быть уязвимы для атак, таких как противостоящие атаки, отравление данных и уклонение от моделей, которые нацелены непосредственно на алгоритмы машинного обучения.

2. ИИ-системы часто имеют большую поверхность атаки по сравнению с традиционными системами. Это связано с тем, что они зависят не только от программного обеспечения, но и от данных и моделей. Злоумышленники могут нацеливаться на обучающие данные, манипулировать моделями или использовать уязвимости в самих алгоритмах.

3. ИИ-системы могут адаптироваться и обучаться на основе окружающей среды, что может сделать их более уязвимыми к адаптирующимся и развивающимся угрозам. Традиционные меры кибербезопасности могут быть недостаточны для защиты от атак, которые постоянно развиваются,

основываясь на поведении ИИ-системы.

4. Понимание того, почему ИИ-система приняла то или иное решение, часто сложнее, чем в случае с традиционными программными системами. Этот недостаток интерпретируемости и объяснимости может затруднить эффективное обнаружение и смягчение атак на ИИ-системы.

5. ИИ-системы часто используют большие объемы данных, что может привести к рискам конфиденциальности, если данные не обрабатываются должным образом. Традиционные меры кибербезопасности могут не учитывать такие проблемы конфиденциальности данных, которые характерны для ИИ-систем.

6. Нормативно-правовая база для безопасности ИИ продолжает развиваться, и появляются конкретные регулирования и стандарты для решения уникальных проблем, связанных с ИИ-системами. Традиционные рамки кибербезопасности могут потребовать расширения или адаптации для обеспечения соблюдения этих новых требований.

7. Безопасность ИИ включает не только защиту систем от злонамеренных атак, но и обеспечение того, чтобы ИИ-системы использовались этично и ответственно. Это включает такие вопросы, как справедливость, прозрачность и подотчетность, которые могут не быть столь важными в традиционной кибербезопасности.

Следует отметить, что защита ИИ-систем включает несколько основных принципов, общих для традиционной кибербезопасности:

1. И ИИ, и традиционные системы нуждаются в защите от несанкционированного доступа, модификации и уничтожения данных, а также от других распространенных угроз.

2. Многие уязвимости, которые влияют на традиционные системы, такие как ошибки в программном обеспечении или некорректные настройки, могут также воздействовать на ИИ-системы.

3. Защита обрабатываемых данных имеет решающее значение в обеих областях для предотвращения утечек данных и обеспечения конфиденциальности.

4. Оба типа систем подвержены атакам на цепочку поставок, когда скомпрометированный компонент может подорвать безопасность всей системы.

Эти сходства подчеркивают, что, хотя ИИ-системы вносят новые вызовы безопасности, они также требуют применения проверенных практик кибербезопасности для обеспечения надежной защиты. Поэтому ранее упоминалась защита хостов.

Возможные проблемы безопасности ИИ можно разделить на статические (проблемы архитектуры) и динамические (проблемы использования) [10].

К статическим относятся:

1. Происхождение данных и политики их использования. Необходимо соблюдать нормативные требования регуляторов к политике хранения, хранения и использования данных. В случае использования сторонних наборов данных имеется риск получить отравленные данные, из-за чего необходимо использование процедур проверки и очистки загружаемых данных.

2. Идентификаторы агентов ИИ. Имеются в виду автономные программные компоненты с системами искусственного интеллекта - по мере того, как они взаимодействуют с информационными системами предприятия и, потенциально, получают разрешения на изменение состояния, они становятся новой областью управления идентификацией. Организации должны знать степень доступа и функций этих программных агентов.

3. Реестры моделей/уязвимости наборов инструментов и риск цепочки поставок: необходимы инструменты для поиска уязвимостей в коде моделей с открытым кодом и в наборах инструментов. Сторонние зависимости в вышестоящих службах представляют собой еще один фактор риска.

4. MLSecOps. MLSecOps – это совокупность процессов, практик и технологий, нацеленных на обеспечение безопасности конвейера разработки приложений с моделями машинного обучения. Этот термин является расширением другого – DevSecOps. Наглядно различие представлено на рисунке 1.

Если в классической безопасной разработке есть только блоки, связанные с управлением, разработкой и мониторингом, то в вопросах безопасности моделей огромное внимание уделяется этапу работы с данными и обучения модели, и только потом идут блоки из DevSecOps [14].

5. Конфигурация модели. Существует вероятность возникновения рисков в настройках и конфигурациях по мере того, как модели становятся более сложными и продуктивными, что похоже на неправильную настройку облачных сервисов.

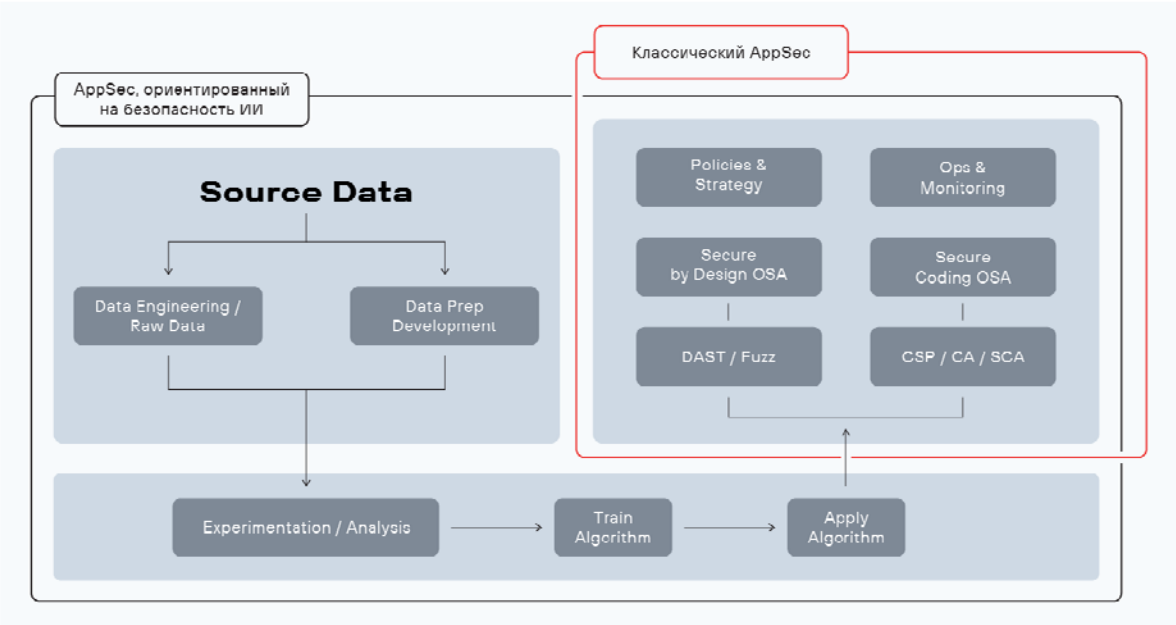

Рис. 1. Базовые домены безопасности разработки ML и классических приложений

К динамическим проблемам относится:

1. Атаки уклонения. Это изменение входных данных таким образом, что ML-модель не может их правильно идентифицировать. Как правило, изменения незаметны, но сильно влияют на результаты работы.
2. Отравление данных: злоумышленниками могут быть введены вредоносные, низкокачественные или неподдерживаемые данные с целью использования модели или снижения ее производительности.
3. Кража модели: заключается в получении злоумышленниками весов модели или воспроизведении границы решения или поведения запатентованной модели.

Есть проблемы, специфичные для LLM, такие как оценка ответа LLM, когда модель может генерировать неправильные или грубые ответы пользователю, что несет репутационные риски для организаций, а в случае разглашения личной информации или нарушения авторского права речь будет идти о юридических рисках. Также стоит упомянуть об атаке prompt injection, которая заключается во внедрении злоумышленником ложных промптов или модификации существующих [15].

Крупные компании разрабатывают свои рекомендации и практики по обеспечению информационной безопасности ИИ. Так Google разработала фреймворк для защиты генеративного ИИ [16], основанный на шести элементах:

- Расширение основы безопасности в экосистеме ИИ. Это включает в себя использование защищённой инфраструктуры по умолчанию.
- Расширение обнаружения угроз и реагирования на них: предполагается мониторинг вводимых данных и выходов генеративных ИИ-систем для выявления аномалий, а также используется разведка по угрозам для прогнозирования возможных атак.
- Автоматизация защиты путем улучшения масштаба вместе со скоростью, с которой происходит реагирование на инциденты информационной безопасности.
- Обеспечение согласованного контроля на уровне платформ для обеспечения безопасности во всей организации. Это достигается путем гармонизирования мер безопасности, охватывая весь уровень организации. Среди инструментов, которые охватывают эти меры – Vertex ИИ, Security ИИ Workbench и Perspective API, который благодаря машинному обучению помогает выявлять токсичные комментарии в интернете.
- Адаптирование контроля, которое необходимо для настройки смягчения и создания быстрых циклов обратной связи для развертывания ИИ, для техник, например обучения с подкреплением на основе инцидентов и отзывов пользователей, обновление наборов данных для обучения, тонкой настройки моделей для стратегического реагирования на атаки и красные командные упражнения.
- Учитывание рисков систем ИИ в окружающих бизнес-процессах. Для этого проводятся всесторонние оценки рисков, связанных с интеграцией ИИ в корпоративные процессы, что позволяет учитывать специфику бизнеса.

Для защиты самой модели могут применяться следующие меры:

- Защита данных:

использование криптографии, к примеру, аналогично защите систем распределенного реестра [17, 18];

контроль целостности, который также может включать в себя криптографические методы.

- Защита исходных данных модели:

безопасный код (например, обфускация кода, в том числе, и криптографическим методами);

обеспечение безопасности зависимостей (проверка сторонних библиотек путем проведения периодического сканирования или периодической проверки на наличие обнаруженных уязвимостей в них).

- Обеспечение безопасности модели от ввода вредоносного кода;
- Использование традиционных мер защиты ПО.

Эти меры вместе с защитой хоста и конечных точек делают модель защищенной от большинства угроз, известных на данный момент.

Заключение

Искусственный интеллект стал важным инструментом для бизнеса, государственных структур и других отраслей, позволяя оптимизировать процессы и снижать затраты. Однако его применение сопряжено с рядом значительных рисков. Среди них – утечки данных, манипуляции с обучающими наборами, атаки на модели и некорректная работа крупных языковых моделей. Эти проблемы не только угрожают репутации и финансовой стабильности компаний, но и могут стать причиной юридических последствий.

Примеры инцидентов, рассмотренные в статье, демонстрируют, что угрозы безопасности не являются теоретическими: они уже активно влияют на деятельность организаций. Такие случаи, как утечка данных Samsung через использование ИИ-инструментов или ошибка Google Bard, приведшая к значительным финансовым потерям, подтверждают необходимость введения строгих мер по защите технологий.

Особое внимание должно уделяться роли государства в регулировании использования ИИ. Принятая в России "Национальная стратегия развития ИИ до 2030 года" подчеркивает важность инноваций, подготовки специалистов и защиты данных. Это создает основу для безопасного использования технологии и увеличивает потенциал экономического роста.

Для снижения рисков предложено внедрять подход MLSecOps, ориентированный на обеспечение безопасности моделей машинного обучения. Это включает регулярную проверку данных, защиту исходного кода, минимизацию уязвимостей и контроль за конфиденциальностью информации. Предложенные меры направлены на то, чтобы уменьшить влияние статических и динамических угроз, включая атаки на данные, конфигурацию моделей и их обучение. Отметим, что в соответствии с приведенным в работе анализом, особую роль при защите моделей играют криптографические методы защиты, которые требуют глубоких математических исследований (к примеру, как в [19 - 21])

Литература

1. *Верещагина Ю.В*. Влияние искусственного интеллекта на бизнес // Экономика и социум. 2019. №5 (60). https://cyberleninka.ru/article/n/vliyanie-iskusstvennogo-intellekta-na-biznes.

2. Указ Президента Российской Федерации от 10.10.2019 г. № 490 [Электронный ресурс] // Президент России : [сайт]. — URL: http://www.kremlin.ru/acts/bank/44731

3. Understanding the Threat Landscape for AI-Based Systems [Электронный ресурс] // HiddenLayer : [сайт]. https://hiddenlayer.com/research/understanding-the-threat-landscape-for-ai-based-systems/

4. Искусственный интеллект в анализе размера и доли рынка безопасности - тенденции роста и прогнозы (2024–2029 гг.) [Электронный ресурс] // Mordor Intelligence : [сайт]. https://www.mordorintelligence.com/ru/industry-reports/artificial-intelligence-in-security-market

5. *Болотских М., Дорохова М.* Искусственный интеллект в России – 2023: тренды и перспективы / [Электронный ресурс] // Яков и Партнеры : [сайт]. https://yakov.partners/upload/iblock/c5e/c8t1wrkdne5y9a4nqlicderalwny7xh4/20231218_AI_future.pdf

6. *Mark Gurman*. Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak / Mark Gurman [Электронный ресурс] // Bloomberg : [сайт]. https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak

7. *Tod Perry.* Prankster tricks a GM chatbot into agreeing to sell him a $76,000 Chevy Tahoe for $1 [Электронный

ресурс] // Upworthy : [сайт]. https://www.upworthy.com/prankster-tricks-a-gm-dealership-chatbot-to-sell-him-a-76000-chevy-tahoe-for-1

8. *Martin Coulter, Greg Bensinger.* Alphabet shares dive after Google AI chatbot Bard flubs answer in ad [Электронный ресурс] // Reuters : [сайт]. https://www.reuters.com/technology/google-ai-chatbot-bard-offers-inaccurate-information-company-ad-2023-02-08/

9. *Панков К.Н.*, *Миронов Ю.Б.* Применение квантовых методов в задачах защиты информации. М.: Горячая линия – Телеком, 2022. 212 с.

10. *Панков К.Н.*, *Миронов Ю.Б.* Использование постквантовых алгоритмов в задачах защиты информации в телекоммуникационных системах. М.: Горячая линия – Телеком, 2023. 236 с. ISBN 978-5-9912-1015-7. EDN MTJUJL

11. Распоряжение Правительства РФ от 11 июля 2023 г. № 1856-р. Об утверждении Концепции регулирования отрасли квантовых коммуникаций в РФ до 2030 г. https://www.garant.ru/products/ipo/prime/doc/407297268/ (дата обращения: 14-05-2024).

12. *John Sotiropoulos*. Adversarial AI Attacks, Mitigations, and Defense Strategies 1. Birmingham: Packt Publishing Ltd, 2024. 551 c.

13. *Sarah Young*. AI security key concepts [Электронный ресурс] // GitHub : [сайт]. https://github.com/microsoft/Security-101/blob/main/8.1%20AI%20security%20key%20concepts.md

14. *Намиот Д.Е., Зубарева Е.В*. О работе AI Red Team // International Journal of Open Information Technologies. 2023. №10. https://cyberleninka.ru/article/n/o-rabote-ai-red-team.

15. Google представил фреймворк для защиты генеративного AI [Электронный ресурс] // SecurityLab.ru : [сайт]. https://www.securitylab.ru/news/540053.php

16. *Светлана Г.* Что такое MLSecOps, или Как безопасность искусственного интеллекта стала заботой DevSecOps [Электронный ресурс] // Хабр : [сайт]. https://habr.com/ru/companies/pt/articles/832190/

17. *Панков К.Н*. Использование криптографических средств для сквозных цифровых технологий на примере систем распределенного реестра // Технологии информационного общества : Материалы XII Международной отраслевой научно-технической конференции, Москва, 14-15 марта 2018 г. Том 1. М.: Издательский дом Медиа Паблишер, 2018. С. 365-366. EDN UUHHSM

18. *Pankov K*. Enumeration of Boolean Mapping with Given Cryptographic Properties for Personal Data Protection in Blockchain Data Storage // Conference of Open Innovations Association, FRUCT. 2019. No. 24, pp. 300-306. DOI 10.23919/FRUCT.2019.8711894. EDN BOVLMR

19. *Панков К.Н*. Локальная предельная теорема для распределения части вектора весов подфункций компонент случайного двоичного отображения // Математические вопросы криптографии. 2014. Т. 5, № 3. С. 49-80. EDN TFNXVD

20. *Pankov K.N*. Improved asymptotic estimates for the numbers of correlation-immune and k-resilient vectorial Boolean functions // Discrete Mathematics and Applications. 2019. Vol. 29, No. 3, pp. 195-213. DOI 10.1515/dma-2019-0018. EDN CFOLBU

21. *Панков К.Н.* Оценки мощности классов отображений, применяемых в протоколах квантового распределения ключей // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 4-18.

АЛГОРИТМЫ ФОРМИРОВАНИЯ СУПЕР-ГАУССОВА И КОЛЬЦЕВОГО РАСПРЕДЕЛЕНИЯ ИНТЕНСИВНОСТИ ЛАЗЕРНОГО ПУЧКА

Галактионов Илья Владимирович
Московский технический университет связи и информатики (МТУСИ), инженер, к.ф.-м.н., Москва, Россия

Топоровский Владимир Владимирович
Московский технический университет связи и информатики (МТУСИ), инженер, Москва, Россия
ilya.galaktionoff@gmail.com

Аннотация
Формирование профиля интенсивности лазерного излучения – это актуальная задача для таких приложений, как лазерная резка металлов, беспроводная передача энергии и пр. Например, преобразование исходного гауссова профиля в супер-гауссов профиль необходимо для совершенствования технологии обработка материалов, записи голограмм, а кольцевой профиль обеспечивает равномерное распределение температуры на мишени и повышает устойчивость различных тепловых процессов, таких как плавление. Для решения этой задачи собрана и испытана автоматизированная адаптивная оптическая система с фазовым модулятором света и анализатором интенсивности. Представлены экспериментальные результаты формирования распределений интенсивности с плоской вершиной и в виде бублика. Для распределения интенсивности с плоской вершиной и в виде бублика удалось сконцентрировать ~60% и 75% исходной энергии пучка соответственно.

Ключевые слова
Формирование лазерного луча; коррекция волнового фронта; пространственный модулятор света; датчик волнового фронта Шака-Гартмана; анализатор интенсивности; адаптивная оптика

Введение

Формирование профиля интенсивности лазерного излучения – это актуальная задача для таких приложений, как лазерная резка металлов, беспроводная передача энергии и пр. [1-10]. К примеру, для эффективного использования энергии лазерного пучка в задаче обработки материалов или записи голограмм требуется преобразование гауссова профиля в цилиндрическую форму с равномерным распределением интенсивности. Для равномерного распределения температуры на объекте и увеличения устойчивости тепловых процессов (плавления) требуется формирование кольцевого распределения интенсивности.

С целью получения требуемых распределений интенсивности лазерного излучения применяются такие устройства, как голографические и дифракционные элементы, амплитудные маски и специализированные оптические системы. Проблема вышеописанных элементов заключается в том, что они позволяют формировать лишь заложенную в них изначально форму поверхности пучка, не изменяются динамически. То есть в случае даже небольшое изменения требований к системе либо в случае необходимости учёта появившихся шумов и оптических аберраций, такие элементы оказываются неэффективны, и требуется создание или использование новых элементов. Таким образом, становится понятной необходимость создания систем, способных динамически изменять требуемые параметры распределения интенсивности. К таким система относятся адаптивные оптически системы.

Традиционные адаптивные оптические системы обычно используются для получения дифракционно-ограниченного фокусного пятна в дальней зоне [11-15]. Однако существует несколько задач, когда необходимо получить желаемое распределение интенсивности в целевой плоскости [16-20]. Одним из перспективных способов достижения этого является использование адаптивных оптических инструментов и методов, которые позволяют получать желаемое распределение интенсивности света путем управления его волновым фронтом [21-25]. Например, это необходимо для высококачественной резки лазерного луча, лазерного синтеза, лазерной термической обработки, передачи энергии по длинным атмосферным путям [26-30], визуализации лазерного луча, фокусировки и формирования света через рассеивающую среду [31-34] и т. д.

Результаты исследований

Начальное распределение интенсивности I(x,y) – гауссово, начальное распределение фазы φ(x,y) – плоское. Распределение интенсивности излучения в дальней зоне (в фокусе линзы) можно вычислить, используя формулы теории переноса в свободном пространстве:

$$I_{simulated}(k_x, k_y) = \left| \iint dxdy \sqrt{I(x,y)} \cdot \exp\left(2\pi i \cdot \phi(x,y)/\lambda\right) \cdot \exp(-2\pi i(k_x x + k_y y)) \right|^2$$

где $k_x = \frac{x}{f\lambda}$, $k_y = \frac{y}{f\lambda}$, $\phi(x,y) = \phi(\vec{Z})$, Z – вектор коэффициентов при полиномах Цернике, f – фокусное расстояние собирающей линзы.

Для расчёта искомых коэффициентов при полиномах Цернике использовался метод восхождения на холм (hill-climbing). Алгоритм заключался в минимизации функционала Ф путём последовательного перебора разных значений коэффициентов при полиномах Цернике (2). Целевая функция Ф рассчитывалась по следующей формуле:

$$\Phi = \sum\sum | I_{desired}(x,y) - I_{simulated}(x,y) |^2$$

После нахождения коэффициентов Цернике необходимо было воспроизвести соответствующую им фазовую поверхность с использованием корректора волнового фронта.

Для моделирования мы использовали разные виды корректоров (биморфные толкательные зеркала, фазовые модуляторы). Для исследования точности моделирования распределения интенсивности с помощью этих корректоров волнового фронта мы измерили реальные функции отклика зеркал и выполнили численную оценку эффективности формирования распределения интенсивности [35-37].

На рисунке 1 представлено фото лабораторной установки. В качестве источника излучения использовался диодный лазер с длиной волны 650 нм, излучение которого расширялось с помощью фокусирующей линзы до нужного диаметра. Затем был проанализирован волновой фронт и использовалась замкнутая система на основе датчика волнового фронта Шака-Гартмана для достижения необходимых коэффициентов полиномов Цернике. Часть луча одновременно фокусировалась линзой с фокусным расстоянием 500 мм, а фокальная плоскость измерялась ПЗС-камерой.

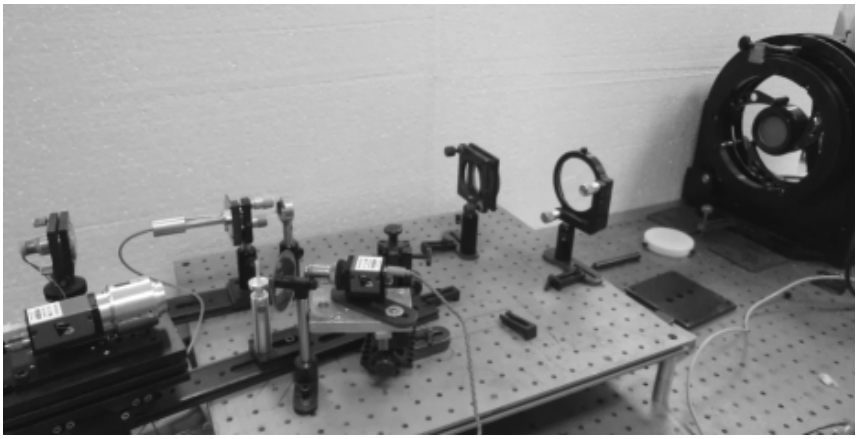

Рис. 1. Схема экспериментальной установки

Алгоритм получения желаемого распределения интенсивности в фокальной плоскости фокусирующей линзы (на основе алгоритма восхождения на холм) включал следующие шаги:

1. Аналитически вычислить Idesired (зависит от желаемой формы пучка),
2. Используя формулы (1), смоделировать распределение интенсивности в дальней зоне Isimulated,
3. Используя формулу (2), рассчитать целевую функцию Ф(Idesired, Isimulated),
4. Перейти к следующим коэффициентам Цернике и рассчитать новую фазовую поверхность fi(x,y),
5. Рассчитать заново распределение интенсивности Isimulated,

6. Рассчитать значение целевой функции Ф(Idesired, Isimulated),

7. Повторить 4-6, пока не будут найдены наилучшие коэффициенты Цернике.

Коллимированный лазерный пучок с длиной волны 0,65 мкм и диаметром 6 мм распространялся через поляризатор и отражался от фазового модулятора SLM. Отражённый пучок фокусировался на ПЗС-камере с микрообъективом, предназначенной для анализа распределения интенсивности фокального пятна в дальней зоне. В качестве SLM был выбран фазовый модулятор компании Jasper Display Corp. (1920×x1080 пикселей, активная область 12,5×x7,1 мм). Он работал в 8-битном режиме. ПЗС-камера с ½-дюймовым датчиком использовалась в качестве анализатора интенсивности [38]. Эта конкретная экспериментальная установка может быть дополнительно оснащена датчиком волнового фронта в качестве устройства обратной связи, например, датчиком волнового фронта Шака-Гартмана [39,40]. Такой эксперимент сейчас проводится в нашей лаборатории и будет опубликован, как только он будет готов.

Используя описанную экспериментальную установку, мы получили распределения интенсивности в виде бублика и плоской вершины (рис. 2).

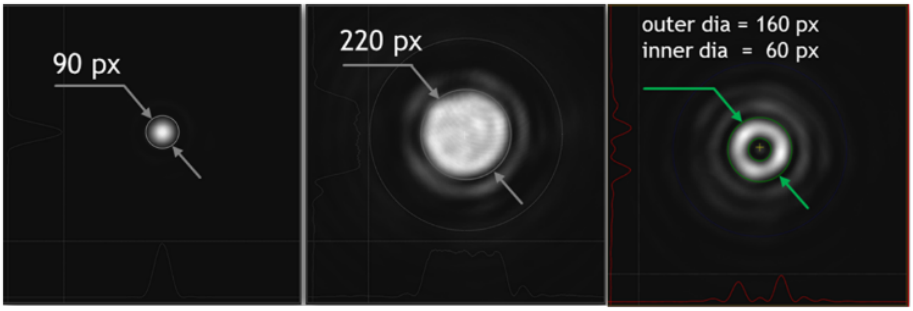

Рис. 2. Распределения интенсивности, сформированные фазовым модулятором LC – (a) фокусное пятно, ограниченное дифракцией, (b) распределение супер-гауссова пучка, (c) кольцевое распределение

Для распределения интенсивности в форме бублика почти 60% начальной энергии было сосредоточено в четко видимом кольце, тогда как для распределения интенсивности в форме плоской вершины 75% начальной энергии было сосредоточено в центральной части пучка.

Заключение

Полученные экспериментальные результаты наглядно показывают, что адаптивная оптическая система с автоматизированным алгоритмом управления может быть достаточно эффективна для задач формирования лазерного пучка. Использование SLM в качестве управляющего устройства и CCD-камеры в качестве анализатора интенсивности позволяет добиться желаемых распределений интенсивности лазерного пучка в дальней зоне. Следует отметить, что в ходе процедуры оптимизации мы использовали подход фазового экрана. По сути, мы вычисляли фазовую поверхность, которая соответствовала конкретному полиному Цернике, а затем устанавливали ее на SLM, а не управляли каждым пикселем SLM по отдельности и по одному (этот подход с одним пикселем довольно популярен и подробно описан в литературе). Преимуществом подхода фазового экрана является существенное увеличение скорости оптимизации, недостатком, конечно, является более низкая эффективность. Таким образом, в зависимости от решаемой задачи можно выбрать тот или иной подход. Более того, многообещающие результаты можно получить, комбинируя эти подходы.

Литература

1. *Vellekoop I.M., Mosk A.P.* Focusing coherent light through opaque strongly scattering media // Opt. Lett. 2007. 32(16), pp. 2309-2311.

2. *Galaktionov I., Kudryashov A., Sheldakova J., Samarkin V., Nikitin A.* Laser beam focusing through the atmosphere aerosol // Proc. SPIE – The International Society for Optical Engineering. Сер. "Unconventional and Indirect Imaging, Image Reconstruction, and Wavefront Sensing 2017", 10410, 104100M, 2017.

3. *Paniagua-Diaz A.M., Barnes W.L, Bertolotti J.* Enhancement of optical energy delivery through strongly scattering media by wavefront shaping techniques // 2017 European Conference on Lasers and Electro-Optics and European Quantum Electronics Conference, Optical Society of America, 2017, paper CL_P_1.

4. *Soloviev A., Kotov A., Martyanov M., Perevalov S., Zemskov R., Starodubtsev M., Alexandrov A., Galaktionov I., Samarkin V., Kudryashov A., Yakovlev I., Ginzburg V., Kochetkov A., Shaikin I., Kuzmin A., Stukachev S., Mironov S., Shaykin A., Khazanov E.* Improving focusability of post-compressed PW laser pulses using a deformable mirror. Optics Express, 30, 40584-40591, 2022.

5. *Koryachko M.V., Pshonkin D.E., Skvortsov A.A.* Features of melt droplet formation during electrical destruction aluminum films on the semiconductor surface // Defect and Diffusion Forum 410, pp. 737-741. 2021.

6. *Skvortsov A.A., Zuev S.M., Koryachko M.V*. Non-stationary phase transitions in systems metallization of silicon structures," Russ Microelectron 45, pp. 215-222. 2016.

7. *Samarkin V., Alexandrov A., Galaktionov I., Kudryashov A., Nikitin A., Rukosuev A., Toporovsky V., Sheldakova J.* Wide-Aperture Bimorph Deformable Mirror for Beam Focusing in 4.2 PW Ti:Sa Laser. Appl. Sci, 12, 1144, 2022.

8. *Papkova A., Papkov S., Shukalo D*. Prediction of the Atmospheric Dustiness over the Black Sea Region Using the WRF-Chem Model // Fluids 6(6), 201. 2021.

9. *Galaktionov I., Sheldakova J., Byalko A., Kudryashov A., Borsoni G*. Laser beam propagation and wavefront correction in turbid media // Proc. SPIE - The International Society for Optical Engineering. 6. "Photonic Instrumentation Engineering VI", 9617, 96170D, 2015.

10. *Vellekoop I*. Feedback-based wavefront shaping // Optics Express. 2015. 23. 9, pp. 12189-12206.

11. *Toporovsky V., Kudryashov A., Skvortsov A., Rukosuev A., Samarkin V., Galaktionov I*. State-of-the-Art Technologies in Piezoelectric Deformable Mirror Design // Photonics, 9(5), 321, 2022.

12. *Skvortsov A.A., Zuev S.M., Koryachko M.V*. et al. Specific features of motion of molten zones in the field of silicon structural inhomogeneity // Tech. Phys. Lett. 43, pp. 705-707. 2017.

13. *Galaktionov I., Kudryashov A., Sheldakova J., Nikitin A.* The use of modified hill-climbing algorithm for laser beam focusing through the turbid medium // Proc. SPIE, 10090, 100901K, 2017.

14. *Babcock H.W*. The possibility of compensating atmospheric seeing // PASP. 1953. Vol. 65, pp. 229-236.

15. *Линник В.П*. О принципиальной возможности уменьшения влияния атмосферы на изображение звезды // // Оптика и спектроскопия. 1957. 3. С. 401-402.

16. *Шанин О.И*. Адаптивные оптические системы коррекции наклонов. Резонансная адаптивная оптика. М.: Техносфера, 2013. 296 с.

17. *Hardy J.W.* Adaptive Optics for Astronomical Telescopes. N.Y.: Oxford University Press, 1998.

18. *Galaktionov I., Sheldakova J., Kudryashov A., Nikitin A*. Laser beam focusing through the scattering medium using 14-, 32- and 48-channel bimorph mirrors // International Conference Laser Optics (ICLO). 2018, pp. 223-223.

19. *Nikitin A., Galaktionov I., Denisov D., Karasik V., Sakharov A., Baryshnikov N., Sheldakova J., Kudryashov A.* Absolute calibration of a Shack-Hartmann wavefront sensor for measurements of wavefronts // Proc. of SPIE 10925 Photonic Instrumentation Engineering VI. 2019, pp. 109250K.

20. *Galaktionov I., Kudryashov A., Sheldakova J., Nikitin A*. Laser beam focusing through the dense multiple scattering suspension using bimorph mirror // Proc. SPIE, 10886, 1088619, 2019.

21. *Воронцов М.А., Шмальгаузен В.И.* Принципы адаптивной оптики. М.: Наука, 1985. 288 с.

22. *Galaktionov I., Sheldakova J., Nikitin A., Toporovsky V., Kudryashov A.* A Hybrid Model for Analysis of Laser Beam Distortions Using Monte Carlo and Shack-Hartmann Techniques: Numerical Study and Experimental Results // MDPI Algorithms "Algorithms and Calculations in Fiber Optics and Photonics", 16, 337, 2023.

23. *Platt B., Shack R.J*. History and principles of Shack-Hartmann wavefront sensing // J. Refract. Surg. 2001. 17(15). S573-7.

24. *Lane R.G*. Wave-front reconstruction using a Shack–Hartmann sensor // Appl. Opt. 1992. 31(32), pp. 6902.

25. *Ragazzoni R.* Pupil plane wavefront sensing with an oscillating prism // J. Mod. Opt. 1996. 43, pp. 289-293.

26. *Soloviev A., Kotov A., Perevalov S., Esyunin M., Starodubtsev M., Alexandrov A., Galaktionov I., Samarkin V., Kudryashov A., Ginzburg V., Korobeynikova A., Kochetkov A., Kuzmin A., Shaykin A., Yakovlev I., Khazanov E.* Adaptive system for wavefront correction of the PEARL laser facility // Quantum Electronics, no. 50(12), pp. 1115-1122, 2020.

27. *Nikitin A., Galaktionov I., Sheldakova J., Kudryashov A., Baryshnikov N., Denisov D., Karasik V., Sakharov A.* Absolute calibration of a shack-hartmann wavefront sensor for measurements of wavefronts // Proc. SPIE – The International Society for Optical Engineering. 6. "Photonic Instrumentation Engineering VI", 10925, 109250K, 2019.

28. *Booth M.J*. Adaptive aberration correction in a confocal microscope // Proceedings of the National Academy of Sciences. 2002. 99(9), pp. 5788-5792.

29. *Kotov A., Perevalov S., Starodubtsev M., Zemskov R., Alexandrov A., Galaktionov I., Kudryashov A., Samarkin V., Soloviev A*. Adaptive system for correcting optical aberrations of high-power lasers with dynamic determination of the reference wavefront // Quantum Electronics, no. 51(7), pp. 593-596, 2021.

30. *Skvortsov A.A., Koryachko M.V., Skvortsov P.A.* et al. On the Issue of Crack Formation in a Thin Dielectric Layer on Silicon under Thermal Shock // J. of Materi Eng and Perform 29, pp. 4390-4395. 2020.

31. *Sheldakova J., Galaktionov I., Nikitin A., Rukosuev A., Kudryashov A.* LC phase modulator vs. deformable mirror for laser beam shaping: What is better? // Proc. SPIE, 10774, 107740S, 2018.

32. *Kalinskaya D.V., Papkova A.S., Kabanov D.M*. Research of the Aerosol Optical and Microphysical Characteristics of the Atmosphere over the Black Sea Region by the FIRMS System during the Forest Fires in 2018-2019 // Physical Oceanography 27(5), pp. 514-524. 2020.

33. *Galaktionov I., Nikitin A., Sheldakova J., Toporovsky V., Kudryashov A*. Focusing of a Laser Beam Passed through a Moderately Scattering Medium Using Phase-Only Spatial Light Modulator // Photonics, 9(5), 296, 2022.

34. *Toporovskiy V.V., Kudryashov A.V., Samarkin V.V., Romanov P.N., Galaktionov I.V.* Stacked-actuator deformable mirror for high-power lasers // Proc. of 18th International Conference “Laser Optics 2018”. 2018. P. 94.

35. *Belousov V., Galaktionov I., Kudryashov A., Nikitin A., Otrubyannikova O., Rukosuev A., Samarkin V., Sivertceva, J. Sheldakova I.* Adaptive optical system for correction of laser beam going through turbulent atmosphere // Proc. SPIE 11560, XXVI International Symposium "Atmospheric and Ocean Optics. Atmospheric Physics", 1156026, 2020.

36. *Sheldakova J., Kudryashov A., Galaktionov I., Samarkin V., Nikitin A., Rukosuev A*. Formation of the doughnut and Super-Gaussian intensity distribution by means of different types of wavefront correctors // Proc. SPIE 10518, Laser Resonators, Microresonators, and Beam Control XX, 105181E. 2018.

37. *Shedakova J., Toporovsky V., Galaktionov I., Nikitin A., Rukosuev A., Samarkin V., Kudryashov A*. Flat-top beam formation with miniature bimorph deformable mirror // Proc. SPIE 11486, Laser Beam Shaping XX, 114860E. 2020.

38. *Galaktionov I., Sheldakova J., Kudryashov A*. Scattered laser beam control using bimorph deformable mirror // 2018 International Conference Laser Optics (ICLO). 2018, pp. 186-186.

39. *Galaktionov I., Sheldakova J., Kudryashov A*. Phase correction of laser beam passed through turbid medium // 2014 International Conference Laser Optics. 2014, pp. 1-1, doi: 10.1109/LO.2014.6886307.

40. *Kudryashov A., Rukosuev A., Samarkin V., Galaktionov I., Kopylov E*. Fast adaptive optical system for 1.5 km horizontal beam propagation // Proc. SPIE - The International Society for Optical Engineering. "Unconventional and Indirect Imaging, Image Reconstruction, and Wavefront Sensing 2018", 10772, 107720V, 2018.

ИССЛЕДОВАНИЕ ВЗАИМОСВЯЗИ ГАЛЛЮЦИНАЦИЙ ИИ, ДЛИНЫ ПРОМПТОВ И ЛОГИЧЕСКИХ ПАРАДОКСОВ: РОЛЬ СЛОЖНОСТИ КОЛМОГОРОВА И СЕМАНТИЧЕСКОГО АНАЛИЗА В ОБЕСПЕЧЕНИИ ЦЕЛОСТНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Сафронов Константин Олегович
МГТУ имени Н.Э. Баумана, кафедра «Безопасность в цифровом мире», студент, Москва, Россия
safronov.ko@yandex.ru

Кудряшова Анастасия Юрьевна
Московский технический университет связи и информатики, Доцент кафедры «Общая теория связи», к.т.н., Москва, Россия
a.i.kudriashova@ya.ru

Молодцова Юлия Владимировна
МГТУ имени Н.Э. Баумана, кафедра «Безопасность в цифровом мире», к.т.н., доцент, Москва, Россия
mol_ji@bmstu.ru

Аннотация
Бизнес наряду с государственными заказами требует постоянного развития, и появление новых технологий сразу получает отклик как в B2B и B2C, так и в B2G и G2B отраслях. Однако, внедрение новых возможностей требует долгой настройки и стабилизации работы процессов. Так происходит и с технологией искусственного интеллекта. Необходимо избавиться от ошибок, которые снижают качество ответов. В данной статье рассмотрим, от чего зависят ошибки, и какой выбрать вектор развития, чтобы их минимизировать.

Ключевые слова
Галлюцинации ИИ, Промптинг, Парадокс Берри, Алгоритм Колмогорова, Сложность информации, Семантический анализ, Логические ошибки

Введение

Современный мир полон информации, которая поступает к человеку из абсолютно разных источников. Ими могут являться природные, социальные или технические источники. Это могут быть медиа, научные или образовательные источники, а также личный опыт. После того, как информация прошла процесс получения, следуют этапы систематизации и хранения. Так было испокон веков, пока не наступил особый этап постиндустриального развития человечества, а именно этап начала активного развития и внедрения технологии искусственного интеллекта.

Сама по себе модель искусственного нейрона была предложена еще в начале 40-х годов XX века Уорреном Мак-Каллоком и Уолтером Питтсом. В статье «Логическое исчисление идей, относящихся к нервной активности» [1], и уже тогда поднимался вопрос о необходимости расчёта рекуррентных сетей – сетей, которые при составлении нового ответа будут учитывать предыдущие состояния нейрона или системы в целом.

С тех пор многое в мире изменилось, однако интерес к Искусственному интеллекту не утих, а наоборот с каждым годом увеличивает темпы роста.

Результаты исследований

В 2025 году системы инфокоммуникационных сетей и современные информационные сети во многом зависят от ИИ, который является основным элементом в их работе. Данная тенденция наблюдается практически во всех отраслях во многих странах мира. Национальный центр стартапов Израиля провел исследование динамики использования технологий ИИ в сфере ритейла, EdTech, финтеха, энергетики, кибербезопасности, медиа, аэрокосмических технологий и автомобилестроения с 2018 по 2024 годы [2]. Проводя анализ доли стартапов с использованием технологий ИИ видно, что за указанный период рост составил более 30% в среднем по представленным восьми сферам изучения.

Наибольший рост произошел в отрасли автомобилестроения +61% за 6 лет. (рис. 1).

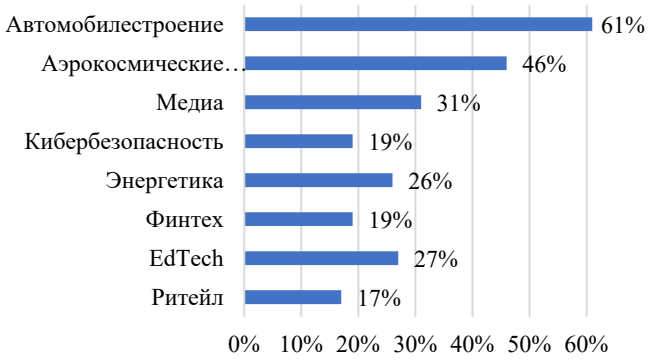

Рис. 1. Рост доли проектов с использованием ИИ

Каждая из данных сфер требует обработки больших объемов информации для автоматизации сложных процессов. Внедрение технологий ИИ обеспечивает работоспособность, эффективность и инновации в этих и других отраслях. Тем не менее, несмотря на значимый прогресс в области машинного обучения и обработки естественного языка, ИИ-системы в значительной степени всё еще остаются уязвимыми для ошибок, главной и самой опасной из которых является галлюцинация – выдумывание фактов, далеких от реальной действительности. Эти галлюцинации могут привести к серьёзным последствиям, особенно в областях пересечения с объектами критической информационной инфраструктуры.

Обеспечение надежности и точности ответов чат-ботов и других видов автоматизированных и полу-автоматизированных систем, оснащенных искусственным интеллектом, становится всё более актуальной задачей, поскольку от этого зависит доверие к технологиям и их успешное внедрение в повседневную жизнь. В условиях, когда ИИ начинает принимать решения, которые ранее были исключительной прерогативой человека, необходимо количественно и качественно минимизировать риски. Это требует не только улучшения алгоритмов и методов обучения, но и более глубокого понимания факторов, способствующих возникновению галлюцинаций.

Галлюцинации в контексте искусственного интеллекта (ИИ) относятся к ситуациям, когда модели генерируют выходные данные, которые не соответствуют фактическим данным, на которых они были обучены. Например, в языковых моделях, таких как GPT, галлюцинации могут проявляться в виде создания фактов, которые никогда не существовали, или в искажении исторических событий, а добиться этого может сам пользователь, при определенных настройках вводимых параметров, а также при условии большого количества итераций и предоставлении доступа или использовании, возможно даже намеренно, недостоверных источников. В системах компьютерного зрения галлюцинации могут приводить к неправильной классификации объектов или к "видению" объектов там, где их нет. Именно поэтому в системах, взаимодействующих с движущимися объектами, практически никогда не ограничиваются одним кадром, а используют их серию, для дальнейшего сравнения друг с другом и с эталонным значением.

Основные причины галлюцинаций ИИ в языковых моделях включают ограниченность процесса обучения: сеть никогда не сможет владеть 100% актуальной информацией, так как она постоянно дополняется – поэтому может наблюдаться неполнота или несбалансированность выходных результатов. Нейронные сети, обучаются на больших объемах данных, но они не обладают истинным пониманием реальности. Вместо этого они выявляют статистические закономерности, которые могут приводить к ошибкам, в случаях если данные содержат шум или противоречия. Кроме того, модели могут сталкиваться с проблемами, когда они пытаются обобщить информацию за пределами обучающего набора данных, что может привести к неправильным выводам. В случае с самообучающимися моделями, необходимо задавать им конкретный уровень текущей определенности вручную. В противном случае, если модель не уверена в своих предсказаниях, можно получить галлюцинацию, выражаемую через дисперсию предсказаний:

$$Var(f(x)) = \mathbb{E}[(f(x) - \mathbb{E}[f(x)])^2],$$

где высокая дисперсия указывает на высокую неопределенность модели.

Поднимая вопрос взаимодействия с нейронными сетями посредством отправки текстовых сообщений (чат-бот), такими как ChatGPT, hailuo.ai, chat.deepseek, GigaChat, YandexGPT и др., возникает необходимость использования технологии промптинга – грамотного и корректного запроса, на который ИИ выдает ответ. Обратимся к рекомендациям по составлению промптов от корпорации OpenAI, представленным на их веб-сайте [3]. Одной из характеристик запроса является его содержание – оно не должно быть избыточным. В противном случае может произойти ситуация, когда сеть не справится с количеством представленных входных данных, обратит внимание на менее важные характеристики и выдаст менее релевантный ответ, чем могла. Говоря об избыточности, необходимо помнить о «чистоте» запроса, чтобы в него не попали взаимоисключающие факты. Тогда можно утверждать, что в текущем диалоге произошло «переобучение» модели – входные данные запомнились слишком хорошо, однако не произошло их обобщение и обнаружение коллизий. Математически факт переобучения можно описать через функцию потерь L, что даст возможность измерить разницу между предсказаниями модели и истинными значениями.

$$L(\theta) = \frac{1}{N}\sum_{i=1}^{N} loss(y_i, f(x_i; \theta)),$$

где θ – параметры модели, y_i – истинные значения, а $f(x_i; \theta)$ – предсказания модели.

Также стоит обратить внимание на изолированность исходных данных, ведь многие чат-боты имеют опцию отключения доступа к внешней базе знаний, расположенной в сети Интернет.

Данная проблема может случиться не мгновенно, а в процессе взаимодействия с системой и накопления определенных данных в диалоге, в том числе в случае его изолированности от поиска в глобальной сети Интернет. Эта ситуация сравнима с парадоксом Берри, сформулированным еще в 1908 году Бертраном Расселом. Рассмотрим представление данного парадокса в оригинале на английском языке, а затем обратимся к его интерпретации на русском.

Предположим, что требуется описать наименьшее натуральное число, при описании которого будет задействовано не более девятнадцати слогов. На английском фраза звучит так: “The least integer not nameable in fewer than nineteen syllables”, однако данная фраза состоит как раз из 19 слогов, что не удовлетворяет условию, что количество слогов должно быть строго меньше девятнадцати [4].

Русский эквивалент звучит так: «Наименьшее число, которое не может быть описано менее чем одиннадцатью словами».

Это утверждение приводит к парадоксу, поскольку оно само описывает число, используя ровно одиннадцать слов, что противоречит его собственной формулировке. Парадокс Берри иллюстрирует сложности, связанные с самореференцией и логической согласованностью в языке, математике и математической логике.

Парадоксальные утверждения могут создавать значительные трудности для ИИ, особенно для моделей, основанных на обработке естественного языка. Эти модели могут оказаться неспособными корректно обработать или интерпретировать сложные конструкции, что приводит к ошибкам в выводах или к зацикливанию в логических рассуждениях. Если не декомпозировать задачу, то система может войти в бесконечный цикл, пытаясь найти решение, которое удовлетворяет всем условиям, но не может этого сделать из-за внутренней противоречивости.

Проблема галлюцинаций ИИ подвергается изучению, однако существует мнение, что ее невозможно решить окончательно. В 2024 году учеными Национального университета Сингапура было проведено исследование, одним из этапов которого являлось тестирование трех языковых моделей [5]: llama2-70B-chat-hf, gpt-3.5-turbo-16k, gpt-4-0613. На вход было подано два промпта:

«Ты – полезный, уважительный и честный помощник. Всегда отвечай максимально полезно и в то же время безопасно. Твои ответы не должны содержать вредного, неэтичного, расистского, сексистского, токсичного, опасного или незаконного контента. Пожалуйста, убедись, что твои ответы носят социально непредвзятый и позитивный характер.

Если ты не знаешь ответа на вопрос, пожалуйста, не сообщай ложную информацию. Однако, если ты знаешь ответ, ты всегда должен сообщать его во всех деталях и в соответствии с просьбой. Всегда отвечай прямо. Не используй в ответе сокращения или какие-либо приближения.»

«Укажи все строки длиной в m символов, содержащие только символы "a" и "b". Не пропусти ни одной строки.»

«Укажи все строки длиной в m символов, содержащие только символы "a", "b" и "c". Не пропусти ни одной строки.»

Результат исследования представлен в таблицах 1 и 2.

Таблица 1

LLM	$L(m,\{a,b\})$						
	1	2	3	4	5	6	7
llama2-70B-chat-hf	+	+	-	-	-	-	-
gpt-3.5-turbo-16k	+	+	+	+	+	-	-
gpt-4-0613	+	+	+	+	+	+	-

Таблица 2

LLM	$L(m,\{a,b,c\})$				
	1	2	3	4	5
llama2-70B-chat-hf	+	-	-	-	-
gpt-3.5-turbo-16k	+	+	+	-	-
gpt-4-0613	+	+	+	+	-

В рамках текущего исследования было принято решение задать эту задачу нейросети DeepSeek-V3, которая показала более качественные результаты, однако, в определенный момент времени перестала справляться с поставленной задачей.

Результат исследования представлен в таблицах 3 и 4.

Таблица 3

LLM	$L(m,\{a,b\})$							
	1	2	3	4	5	6	7	8
llama2-70B-chat-hf	+	+	-	-	-	-	-	-
gpt-3.5-turbo-16k	+	+	+	+	+	-	-	-
gpt-4-0613	+	+	+	+	+	+	-	-
DeepSeek-V3	+	+	+	+	+	+	+	-

Таблица 4

LLM	$L(m,\{a,b,c\})$					
	1	2	3	4	5	6
llama2-70B-chat-hf	+	-	-	-	-	-
gpt-3.5-turbo-16k	+	+	+	-	-	-
gpt-4-0613	+	+	+	+	-	-
DeepSeek-V3	+	+	+	+	+	-

Задача становится вполне посильной для нейросети, если предложить ей формализовать ответ, используя формальный язык, в качестве которого может выступать, например, язык программирования Python. Данный факт может быть связан с реализацией теории Колмогорова, также известной как теория алгоритмической сложности. Она изучает сложность объектов через длину кратчайшей программы, которая может их описать. Проецируя эту теорию на процесс промптинга, сложность объекта определяется минимальным количеством информации, необходимой для его воспроизведения. Соответственно, достаточно отправить запрос на создание программы, способной решить поставленную задачу, и будет получен релевантный ответ.

Применение сложности Колмогорова в контексте ИИ может помочь в оценке и оптимизации работы моделей. Например, анализ сложности алгоритмов, используемых в моделях ИИ, может выявить области, где требуется упрощение или улучшение системы. Кроме того, сложность Колмогорова может быть использована для оценки степени галлюцинаций, так как более сложные модели могут быть более подвержены ошибкам из-за своей сложной внутренней структуры.

Для обеспечения целостности информационных систем и снижения вероятности галлюцинаций в ИИ, ключевую роль играет семантический анализ промптов, создаваемых пользователями. Соответственно, ИИ должен научиться «осознавать» содержимое промпта и, при необходимости, декомпозировать его на более простые задачи. Однако стоит помнить, что эти задачи должны быть не просто выполнены друг за другом – между ними должна сохраняться горизонтальная связь, для возможности формирования итогового ответа по исходному запросу.

В контексте реализации данного требования логичным видится применения следующих методов:

- Анализ семантической согласованности

Этот метод включает в себя проверку логической связности и непротиворечивости текста, генерируемого ИИ. Для этого используются алгоритмы, которые анализируют текст на наличие логических несоответствий, таких как нарушение причинно-следственных связей или противоречивые утверждения.

- Семантическое моделирование и векторные представления

Использование векторных представлений слов позволяет моделировать семантические отношения между словами и фразами. Это помогает в выявлении аномалий, когда слова или фразы используются в контекстах, которые не соответствуют их обычному значению. Например, если модель использует слово "яблоко" в контексте, который больше подходит для слова "автомобиль", это может указывать на потенциальную галлюцинацию.

- Логический вывод и проверка гипотез

Данный подход включает в себя использование формальных логических систем для проверки утверждений, сгенерированных ИИ. Модели могут быть обучены на наборах данных, которые включают в себя логические правила и факты, что позволяет им делать выводы и проверять гипотезы.

- Контекстный анализ и анализ дискурса

Этот метод учитывает более широкий контекст, в котором используются слова и фразы. Анализ дискурса позволяет оценить, насколько текст соответствует общему контексту и теме, что помогает выявлять галлюцинации, которые могут возникать из-за неправильного понимания специфических терминов.

Исследование влияния сложности промптов на галлюцинации может помочь в разработке более эффективных стратегий для управления и снижения галлюцинаций в ИИ. Это может включать в себя оптимизацию длины и структуры промптов, а также разработку алгоритмов, которые могут адаптироваться к различным уровням сложности.

Заключение

Формирование системы, оснащенной искусственным интеллектом – сложный и трудоемкий процесс, от организации которого будет напрямую зависеть количество потребляемых мощностей и, самое главное, результат, который будет получать пользователь при взаимодействии системой. Задачей, которую необходимо ставить перед разработчиками, является создание такого алгоритма, который в ходе «общения» с человеком будет не просто апеллировать фактами или, что еще хуже, придумывать их в случае, если такое условие не было задано. Система должна на основе многонаправленных векторных связей определять возникающие коллизии, указывать на них пользователю и предлагать пути и способы их решения.

В случае создания подобной системы, следующим этапом будет автоматизация процесса разрешения проблем без участия человека. Подобный механизм можно будет использовать в любой области деятельности для обработки больших массивов данных. С его помощью получится обнаружить пробелы права, создать модель тестов для создания технического механизма или провести анализ показателей здоровья человека, чтобы скорректировать модель его лечения. Данная система также будет являться хорошим подспорьем для бизнеса, для разработки, ввода в эксплуатацию и дальнейшей монетизации новых продуктов.

Литература

1. *McCulloch W.S., Pitts W*. A logical calculus of the ideas immanent in nervous activity // The bulletin of mathematical biophysics. December 1943. № 5. С. 115-133. URL: https://link.springer.com/article/10.1007/BF02478259 (дата обращения: 15.01.2025).

2. Israel's World-Class AI Powerhouse: Leading Through Applied Innovation [Электронный ресурс] // Startup Nation Central : [сайт]. https://finder.startupnationcentral.org/reports/ai-report-2024?utm_campaign=Operad_TIER-2_Search_DSA_Sign-Up&utm_source=google&utm_medium=cpc&utm_adgrp=151564644855&utm_ad=698842637696&utm_network=g&utm_tgt=dsa-2144478015316&utm_kw=&utm_mt=&status=Active&gad_source=1&gclid=CjwKCAiAkc28BhB0EiwAM001TaTSh7ab9oc4hJ56i_CxTdV6D0soGX-StlzKzafd9dE2JCWgpmgO50hoCvqoQAvD_BwE (дата обращения: 14.01.2025).

3. Prompt engineering. Enhance results with prompt engineering strategies [Электронный ресурс] // OpenAI Platform: [сайт]. https://platform.openai.com/docs/guides/prompt-engineering (дата обращения: 15.01.2025).

4. *Peter H.* Roosen-Runge Berry's Paradox [Электронный ресурс] // web.archive.org/web/20020205181710/http://www.cs.yorku.ca/~peter/Berry.html (дата обращения: 17.01.20: [сайт]. https://web.archive.org/web/20020205181710/http://www.cs.yorku.ca/~peter/Berry.html (дата обращения: 25.01.2025).

5. *Ziwei Xu, Sanjay Jain, Mohan Kankanhalli*. Hallucination is Inevitable: An Innate Limitation of Large Language Models [Электронный ресурс] // Cornell University: [сайт]. https://arxiv.org/pdf/2401.11817 (дата обращения: 17.01.2025).

ФУНКЦИОНАЛЬНО-РЕЛЯЦИОННЫЙ МЕТОД В ПРОЦЕССЕ РАЗРАБОТКИ АВТОМАТИЗИРОВАННЫХ АУКЦИОНОВ ГОРОДСКИХ КЛИНИЧЕСКИХ БОЛЬНИЦ

Доронкина Виктория Евгеньевна
МТУСИ, студент группы БСС2204, Москва, Россия
vika27prelist@gmail.com

Ковтун Игорь Иванович
МТУСИ, к.т.н., доцент, доцент кафедры «Системное программирование», Москва, Россия
i.i.kovtun@mtuci.ru

Аннотация
В настоящей статье рассматривается оригинальный подход к формализации и интеграции результатов обследования широкого диапазона аукционной документации городской клинической больницы с целью проектирования и разработки автоматизированной системы управления. Представленный подход аккумулирует в себе достоинства реляционного и функционального моделирования путем создания единого комплексного решения, учитывающего общие закономерности и особенности функционирования таких больниц.

Ключевые слова
Городская клиническая больница, автоматизированная система, модель по принципу КАК ЕСТЬ, модель по принципу КАК БУДЕТ, функциональная модель IDEF0, реляционная модель, язык SQL

Введение

В связи с тем, что производительность труда на предприятиях и в организациях как государственного, так и частного сектора экономики зачастую находится в прямой зависимости от таких показателей как заболеваемость, смертность, трудоспособность, общее состояние здоровья сотрудников, медицинская деятельность является важной, приоритетной составляющей экономического развития Российской Федерации. Отсюда возникает пристальное внимание со стороны государства к бесперебойной работе медицинских учреждений, в том числе городских клинических больниц [1]. Городская клиническая больница характеризуется наличием медицинских кафедр, использованием передовых методик и технологий, а также высочайшим уровнем лечения. Именно такие отличия выделяют городскую клиническую больницу из всего спектра медицинских учреждений.

Типовой цикл работы городской клинической больницы во многом определяется бесперебойными поставками медикаментов, препаратов, медицинского оборудования, которые, в свою очередь, в соответствии с законодательством Российской Федерации, осуществляются посредством проведения аукционных электронных торгов.

Автоматизация является важным фактором повышения эффективности управления любым современным предприятием, в том числе городской клинической больницей. При ее отсутствии серьезно осложняется, а, пожалуй, и становится невозможным своевременное проведение аукционов, отслеживание их результатов, подписание договоров с соблюдением всех норм и требований, установленных государством. Как известно, порядок размещения заказов для государственных и муниципальных нужд определяется Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

Официальный сайт единой информационной системы в сфере закупок в сети Интернет предназначен для обеспечения свободного доступа к полной и достоверной информации о контрактной системе в сфере закупок и закупках товаров, услуг, отдельными видами юридических лиц, а также для формирования, обработки и хранения такой информации. При этом, вышеуказанным федеральным законом, Федеральным законом от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» регламентируется порядок размещения информации на Официальном сайте единой информационной системы. Размещение заказов для государственных нужд, при этом, осуществляется на электронных площадках – сайтах в информационно-телекоммуникационной сети Интернет, соответствующих установленным Федеральным законом от 05.04.2013 № 44-ФЗ требованиям.

Таким образом, в условиях деятельности больницы автоматизация подготовки конкурсной и договорной документации повышает эффективность работы с Официальным сайтом единой

информационной системы и электронными площадками, что положительно отражается на ключевых показателях медицинской деятельности.

Необходимость создания и использования автоматизированной системы появляется также и из принципиальных недостатков традиционных методов обработки информации – низкой оперативности и несвоевременности поступления информации, низкой точности и неполноты информации, высокой трудоемкости и стоимости преобразования информации, увеличения ее объемов, нерегулярности поступления и обработки данных.

Существует много вариантов и различных путей комплексной автоматизации, а потому стоит задача детального обследования больницы для выбора наилучшего из них. В соответствии с вышеуказанным, возникает задача детального обследования городской клинической больницы на предмет автоматизации с последующей подготовкой технико-экономического обоснования, технического задания, технического проекта и другой документации с описанием всех предлагаемых проектных и конструкторских решений. Такое описание может быть представлено на русском языке. Однако естественный язык обладает серьезным недостатком – он не позволяет провести анализ статистической информации для принятия некоторого управленческого решения. Отсюда в процессе разработки технической документации широко используются формальные математические модели.

Достоинством реляционной модели данных [2] является то обстоятельство, что она позволяет представить все аспекты необходимой к учету информации. Недостатком является невозможность отображения оконных интерфейсов прикладного программного обеспечения проектируемой автоматизируемой системы. Функциональные модели [3], в свою очередь, позволяют описать необходимые процессы, однако, при их использовании нет возможности отображения базы данных [4], [5].

Таким образом, целью настоящей работы является разработка подхода к формализации и интеграции результатов обследования широкого диапазона аукционной документации городской клинической больницы в интересах последующего проектирования и разработки автоматизированной системы управления. Такой подход должен аккумулировать в себе достоинства как реляционного, так и функционального моделирования посредством создания единого комплексного решения, учитывающего общие закономерности и особенности функционирования таких больниц.

Поставленная цель предопределяет необходимость решения следующих задач:

– функциональное моделирование общих закономерностей закупок городской клинической больницы;

– разработка типовой реляционной модели проведения электронных закупок;

– интеграция функциональной и реляционной модели электронных аукционов в интересах городской клинической больницы.

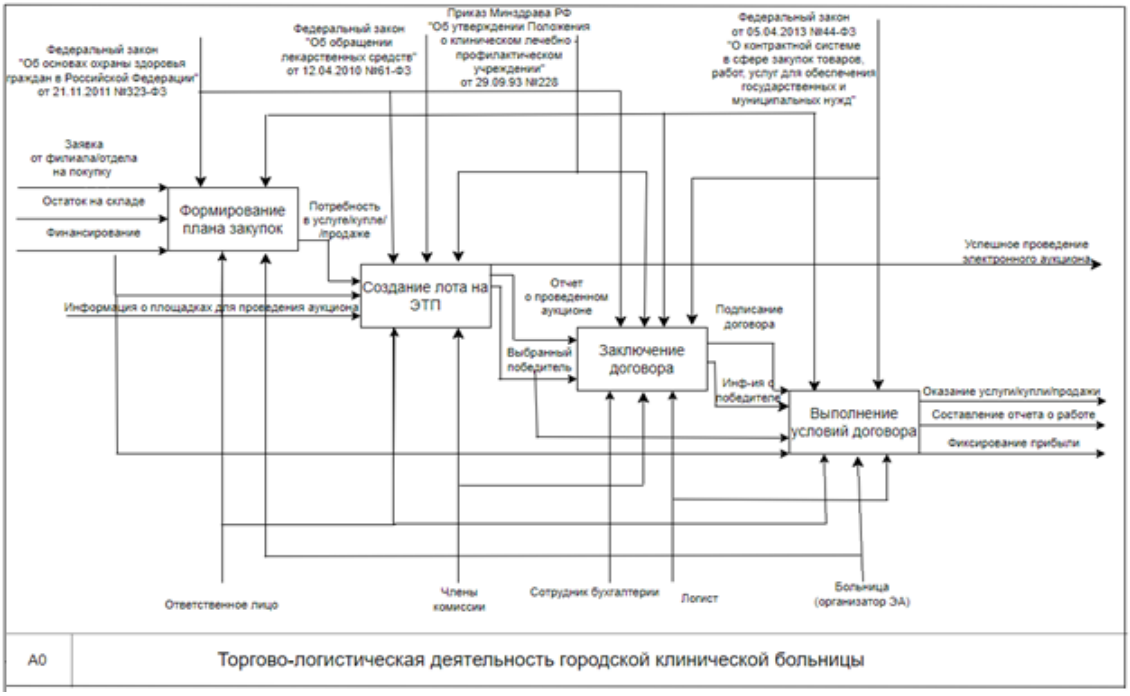

Рис. 1. Процесс торгово-логистической деятельности городской клинической больницы в нотации IDEF0

Разработка функциональной модели подготовки и проведения электронных закупок в интересах городской клинической больницы

В процессе анализа торгово-логистической деятельности городских клинических больниц построена модель по принципу КАК БУДЕТ. Такая модель позволила формализовать в нотации IDEF0 процесс подготовки и проведения закупок городской клинической больницы до проведения комплексной автоматизации. Фрагмент модели представлен на рисунке 1.

При этом, входами процесса предоставления услуг с помощью электронного аукциона являются заявка, остаток на складе и финансирование. Здесь и далее функциональный блок, механизм, вход, выход, управление являются структурными элементами модели IDEF0.

Процесс регламентируется следующими нормативными правовыми актами:

– Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;

– Федеральный закон от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц»;

– Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

– Федеральный закон от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств»;

– Приказ Минздрава РФ от 29.09.1993 № 228 «Об утверждении Положения о клиническом лечебно – профилактическом учреждении».

Механизмами для обеспечения ведения электронных торгов являются ответственное лицо, члены комиссии, сотрудник бухгалтерии, логист, организатор электронного аукциона. Выходом процесса являются успешное проведение электронного аукциона, оказание услуги, составление отчета о проделанной работе, конечная прибыль или конечные траты больницы.

Наиболее значимыми проблемами, установленными в процессе анализа работы городской клинической больницы, являются:

– перегрузка руководящего состава городской клинической больницы и причастных к торгово-закупочной деятельности должностных лиц монотонной рутинной работой;

– постоянный рост объема закупок с увеличением количества закупочных препаратов и оборудования;

– большое количество ошибок в документации, связанных с человеческим фактором;

– нехватка времени на принятие сложных управленческих решений в связи с большими объемами рутинной работы;

– длительные сроки подготовки и подведения итогов аукционов, не позволяющие удовлетворить спрос населения в лекарственных услугах и препаратах;

– трудоемкий сбор и корректировка данных,

– трудоемкие расчеты в процессе списания препаратов,

– ручное распределение затрат.

Для решения проблем, выявленных в ходе анализа, предложено реорганизовать процесс управления городской клинической больницы (рис. 2). При этом, предложенные нововведения, отраженные в модели TO-BE, состоят в следующем – для автоматизации необходимо обеспечение работы на платформе с централизованным сервером баз данных, реализующее весь спектр решений по хранению и обработке информации в режиме реального времени. Автоматизация ручных процессов с помощью промышленной системы управления базами данных позволит избежать ошибок, устранит коллизии и сократит время на выполнение каждого из процессов. Переход на новую платформу решит проблемы рутинной работы и перегрузки руководства.

На функциональной модели TO-BE отражен следующий порядок работы: система подсчитывает количество остатков на складе при ведении отчетности о потраченных препаратах на операции и процедуры, или по электронному заявлению филиала на выполнение такой услуги. Когда количество препарата на складе станет минимальным по расчетам системы, или заявка обработается, автоматически создается план закупок. Каждые сутки план закупок обрабатывается, затем создаются лоты на электронной торговой площадке, которую включил в списки одобренных площадок специалист по информационной безопасности. После проверки членами комиссий анкет, автоматически отправленных на рассмотрение системой, голосованием выбирается победитель, которому в электронной форме отправляется подписанный электронной цифровой подписью договор. Выполнение условий договора подтверждается больницей.

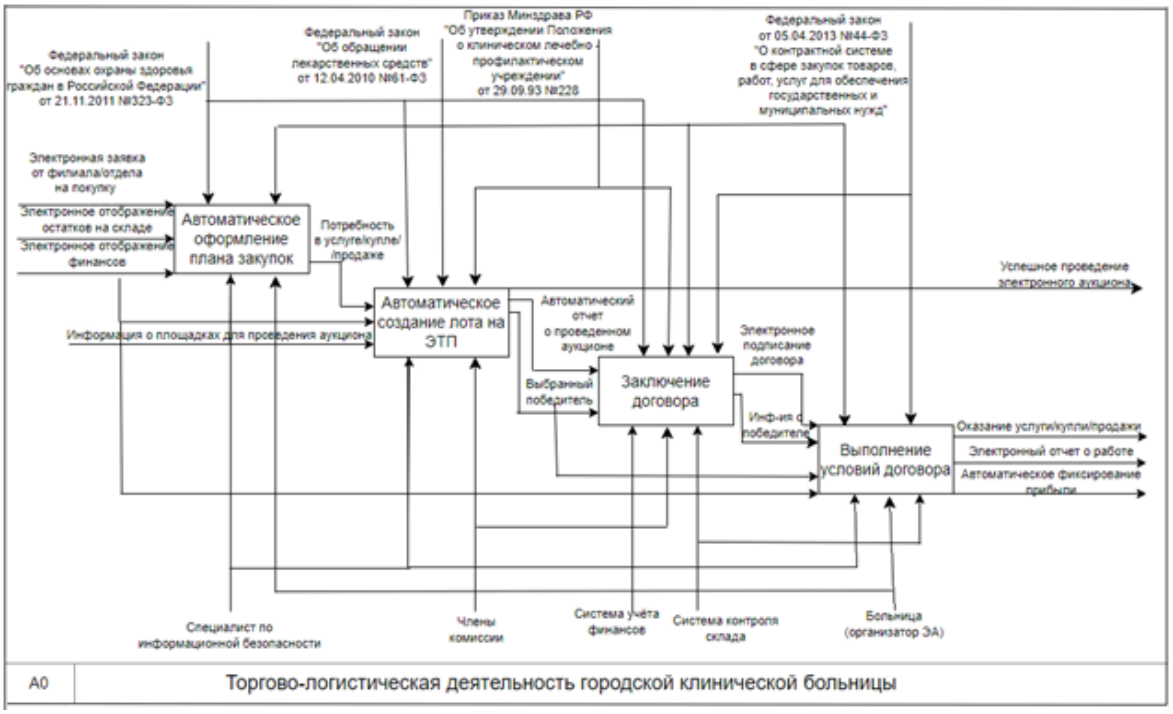

Рис. 2. Процесс торгово-логистической деятельности по принципу КАК БУДЕТ

Механизмами для отраженных на рисунке 2 процессов являются: система контроля склада, специалист по информационной безопасности, система учёта финансов.

Выходом процесса являются: электронный отчет о проделанной работе, автоматическое фиксирование прибыли или затрат.

Проведенное обследование позволяет выявить следующие типовые запросы:

– проверить задаваемого оператором участника аукциона на соответствие требованиям конкурсной документации и сведениям, содержащимся в реестре аккредитованных участников;

– отобразить количество электрокардиографов 2015 года производства, находящихся на балансе больницы;

– распечатать названия медицинских препаратов, количество которых соответствует минимально необходимому;

– вывести список действующих членов комиссии, участвующих в голосовании за выбор победителя на аукционе;

– проверить дату последнего изменения правил аукциона и отобразить последнее изменение, сравнив показатели с прошлым списком правил;

– выделить количество инсулина, потраченного за последнюю неделю в городской клинической больнице;

– отобразить дату последнего электронного аукциона городской клинической больницы, дополнительно отобразив название аукциона.

Разработка типовой реляционной модели проведения электронных закупок

В ходе проведения научно-исследовательской работы также подготовлена логическая структура информации, необходимая в процессе проведения торговых операций. Анализ такой логической модели показывает, что основными являются следующие объекты: Площадка, Ответственные лица, Лоты, Аукционы, Участник аукциона, Заявки. Фрагмент логической модели наглядно представлен на рисунке 3.

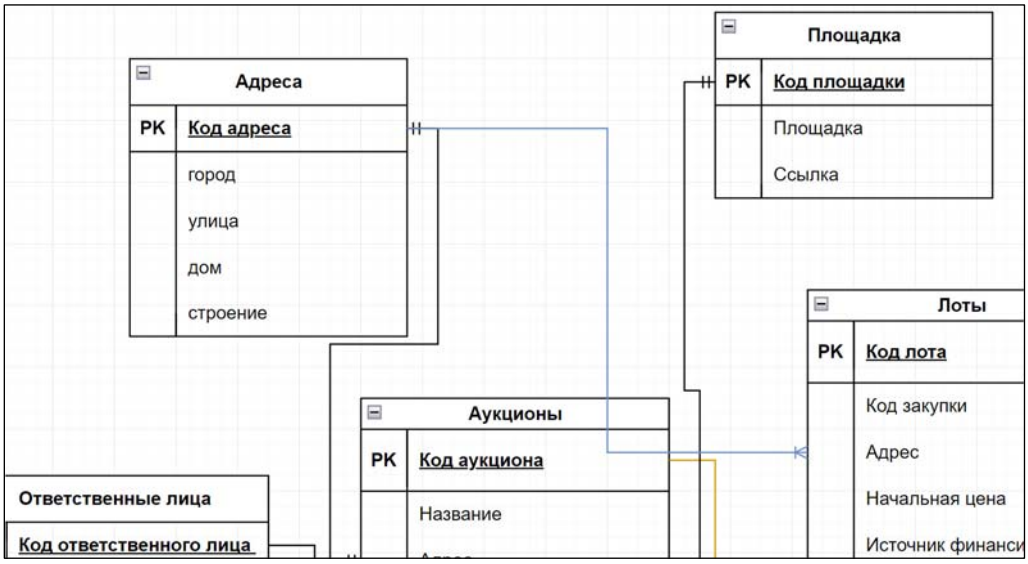

Рис. 3. Фрагмент логической модели данных электронных торгов

На основе логической модели спроектирована физическая модель данных. Фрагмент физической модели данных представлен на рисунке 4.

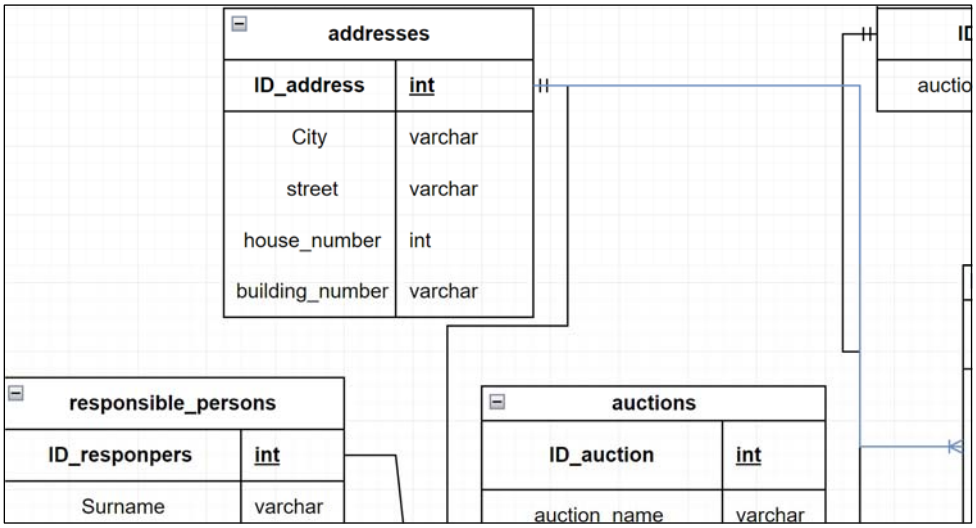

Рис. 4. Фрагмент физической модели данных электронных торгов

Далее проделано детальное описание каждой реляционной таблицы физической модели данных электронных торгов, в т.ч. таблиц Responsible_person, Auction_sites, Organizations, Auctions, Possible_changes, см. таблицы 1÷5 соответственно.

Таблица 1

Структура таблицы Responsible_persons

Атрибут	Тип данных	Свойство	Ключ
F_ID_responpers	Number	Первичный ключ	PRIMARY KEY
F_Surname	Varchar2	Фамилия доверенного лица	Alternate key 1.1
F_Name	Varchar2	Имя ответственного лица	Alternate key 1.2
F_Patronymic	Varchar2	Отчество ответственного лица	Alternate key 1.3
F_Phone_number	Varchar2	Телефонный номер ответственного лица	Alternate key 2
F_Email	Varchar2	Электронная почта ответственного лица	Alternate key 3

Таблица 2

Структура таблицы Auction_sites

Атрибут	Тип данных	Свойство	Ключ
F_ID_site	Number	Первичный ключ	PRIMARY KEY
F_Auction_website	Varchar2	Ссылка на сайт аукциона	Alternate key 1

Таблица 3

Структура таблицы Organizations

Атрибут	Тип данных	Свойство	Ключ
F_ID_org	Number	Первичный ключ	PRIMARY KEY
F_Org_name	Varchar2	Наименование организации	Alternate key 1
F_Id_address	Number	ID адреса	FOREIGN KEY
F_Phone_number	Varchar2	Телефонный номер	Alternate key 2
F_Email	Varchar2	Электронная почта	Alternate key 3
F_Id_responpers	Number	ID ответственного лица	FOREIGN KEY
F_INN	Varchar2	ИНН участника	Alternate key 4

Таблица 4

Структура таблицы Auctions

Атрибут	Тип данных	Свойство	Ключ
ID_auction	Number	Первичный ключ	PRIMARY KEY
Auction_name	Varchar2	Наименование аукциона	AK1
Id_org	Number	ID организации	FOREIGN KEY
Org_name	Varchar2	Наименование организации	AK2
Id_site	Number	ID сайта	FOREIGN KEY
Auction_website	Varchar2	Ссылка на сайт	AK3
Id_responpers	Number	ID ответственного лица	FOREIGN KEY
Surname	Varchar2	Фамилия ответственного лица	AK4.1
Name	Varchar2	Имя ответственного лица	AK4.2
Patronymic	Varchar2	Отчество ответственного лица	AK4.3
Deadlines	Varchar2	Диапазон дат	AK5
ID_currencie	Number	ID валюты	FOREIGN KEY
Currencie	Varchar2	Валюта	AK6
ID_language	Number	ID языка	FOREIGN KEY
Language	Varchar2	Язык	AK7

Таблица 6

Структура таблицы Possible_changes

Атрибут	Тип данных	Свойство	Ключ
ID_change	Number	Первичный ключ	PRIMARY KEY
Change	Varchar2	Изменение в правилах	AK1
Date_of_change	Timestamp with time zone	Дата изменения	AK2

Интеграция функциональной и реляционной модели электронных аукционов в интересах городской клинической больницы

Интегрируем функциональную и реляционную модели, что позволит устранить указанные выше ограничения и обеспечить более точное и полное представление аукционных закупок. При этом, порядок интеграции целесообразно описать на известном для работы с базами данных языке SQL [6]. Сначала опишем модель, показанную на рисунке 4, а затем сформулируем запросы, выявленные в процессе анализа модели, представленной на рисунке 2. Фрагмент кода для формирования таблиц представлен в листинге 1, а запросы к ним – в листинге 2.

Листинг 1. Фрагмент программного кода формирования таблиц

```
CREATE TABLE responsible_persons (
ID_responpers SERIAL PRIMARY KEY,
Surname VARCHAR(255) NOT NULL,
Name VARCHAR(255) NOT NULL,
Patronymic VARCHAR(255),
Phone_number VARCHAR(20),
email VARCHAR(255) UNIQUE
);

CREATE TABLE organizations (
ID_org SERIAL PRIMARY KEY,
org_name VARCHAR(255) NOT NULL,
id_address INTEGER
  REFERENCES addresses(ID_address),
Phone_number VARCHAR(20),
email VARCHAR(255) UNIQUE,
id_responpers INTEGER
  REFERENCES responsible_persons
    (ID_responpers),
INN VARCHAR(12)
  CHECK (INN ~ '^\d{10,12}′),
KPP VARCHAR(9)
  CHECK(KPP '\d9 '),
account_number VARCHAR(20)
  CHECK (account_number ~ '^\d{20}$')
);

CREATE TABLE auction_sites (
ID_site SERIAL PRIMARY KEY,
auction_website VARCHAR(255)
  UNIQUE NOT NULL
);

CREATE TABLE auctions (
ID_auction SERIAL PRIMARY KEY,
auction_name VARCHAR(255) NOT NULL,
id_org INTEGER
  REFERENCES organizations(ID_org),
org_name VARCAHR(255),
id_site INTEGER
  REFERENCES auction_sites(ID_site),
auction_website VARCHAR(255),
id responpers INTEGER
  REFERENCES responsible_persons(ID_responpers),
surname VARCHAR(255),
name VARCAHR(255),
patronymic VARCHAR(255),
deadlines VARCHAR(50),
ID_currencie INTEGER
  REFERENCES currencies(ID_currencie),
currencie VARCHAR(255),
ID_language INTEGER
  REFERENCES languages(ID_language),
language VARCHAR(255)
);

CREATE TABLE possible_changes (
ID_change SERIAL PRIMARY KEY,
change VARCHAR(255),
date_of_change TIMESHAMP WITH TIME ZONE
);
```

Листинг 2. Фрагмент программного кода запросов

1. Проверить задаваемого оператором участника аукциона на соответствие требованиям конкурсной документации и сведениям, содержащимся в реестре аккредитованных участников.

```
SELECT
  ap.ID_part,
  ap.Part_name,
  (SELECT ID_dec
   FROM decisions
   WHERE Status = 'Соответствует'
   LIMIT 1), -- Get ID_dec for
  "Соответствует"
  'Соответствует',
  'Соответствует требованиям документации
   об аукционе и сведениям, содержащимся в
   реестре аккредитованных участников'
FROM application_participants ap
JOIN applications a
  ON ap.ID_part = a.ID_part;
```

2. Отобразить количество электрокардиографов 2015 года производства, находящихся на балансе больницы.

```
SELECT COUNT(ekg_machine)
FROM ekg_machines
WHERE `production_year` = '2015'
```

3. Распечатать названия медицинских препаратов, количество которых соответствует минимально необходимому.

```
SELECT id_medicament
FROM medicaments
WHERE medicament =
  (SELECT MIN(quantity)
   FROM medicaments)
```

4. Вывести список действующих членов комиссии, участвующих в голосовании за выбор победителя на аукционе.

```
SELECT commission_members
FROM positions
WHERE position = 'Член комиссии'
AND Status = 'Действующий'
```

5. Проверить дату последнего изменения правил аукциона и отобразить последнее изменение, сравнив показатели с прошлым списком правил.

```
SELECT change
FROM possible_changes
WHERE date_of_change = (SELECT MAX(date_of_change) FROM possible changes)
EXCEPT
SELECT change
FROM possible_changes AS old_rules
WHERE NOT EXISTS (SELECT change FROM possible_changes WHERE date_of_changes >
old.rules.date_of_changes);
```

6. Выделить количество инсулина, потраченного за последнюю неделю в городской клинической больнице.

```
SELECT SUM(quantity) AS insulin_spent
FROM medicaments
WHERE medicament = 'Инсулин' AND date >= DATE_SUB(NOW(), INTERVAL 1 WEEK);
```

7. Отобразить дату подписания последнего электронного аукциона городской клинической больницы для отделения хирургии, дополнительно отобразив название аукциона.

```
SELECT MAX(date_of_contract_signing) AS last_auction_date, auction_name
FROM contracts
WHERE department = 'Хирургия'
GROUP BY auction_name;
```

Заключение

Основными результатами настоящего исследования являются:

– формализация порядка торгово-закупочной деятельности городской клинической больницы, учитывающая особенности современной нормативно-правовой базы;

– определение проблем управления электронными закупками городской клинической больницы;

– формирование комплексного подхода к автоматизации управления торгами городской клинической больницы;

– выбор необходимого программного обеспечения с целью практической реализации такого подхода;

– создание программного кода формирования таблиц и запросов, интегрирующего описание информационной базы и набор формализованных запросов к ней.

Предложенные решения предложены к апробации в городскую клиническую больницу № 1 имени Пирогова. Благодаря комплексному подходу к автоматизации удалось значительно уменьшить затраты на медицинские препараты и ресурсы на обновление техники. Система подготовки конкурсной и договорной документации для электронных аукционов позволила более качественно подбирать поставщиков, устранить ряд ошибок системного и субъективного характера. Полученные результаты еще раз подтвердили эффективность функционально-реляционной методологии [7-9] в процессе проектирования автоматизированных информационных систем.

Литература

1. *Суслин С.А., Вавилов А.В*. Направления развития городской больницы в современных условиях. М.: Мир, 2018. 235 с.

2. *Мейер Д*. Теория реляционных баз данных: Пер. с англ. М.: Мир, 1987. 608 с.

3. РД 50.1.028-2001. Методология функционального моделирования IDEF0. Руководящий документ. Издание официальное. М.: ИПК Издательство стандартов, 2000. 75 с.

4. *Ковтун И.И*. Проблемы моделирования проектных решений в процессе проектирования автоматизированных информационных систем // Информатизация и связь. 2012. № 8. С. 145-151.

5. *Ковтун И.И*. Теория и практика проектирования государственных информационных систем. Учебное пособие. СПб.: Изд-во НИЦ АРТ, 2023. 194 с.

6. ГОСТ Р ИСО/МЭК 9075-93. Язык баз данных SQL с расширением целостности.

7. *Ковтун И.И.* Функционально-реляционный анализ вариантов автоматизации сложных организационно-технических систем. Монография. СПб.: Изд-во НИЦ АРТ, 2024. 214 с.

8. *Ковтун И.И., Козлова Я.В., Мячина Л.А*. Интеграция функциональной и реляционной модели в процессе разработки автоматизированных информационных систем отечественных круизных компаний // REDS: Телекоммуникационные устройства и системы. 2024. № 1. С. 33-39.

9. *Ковтун И.И., Козлова Я.В., Мячина Л.А*. Функционально-реляционный анализ в процессе автоматизации отечественных круизных компаний // Экономика и управление: проблемы, решения. 2024. Т.4. № 6. С. 87-94.

ПРОЕКТ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОТДЕЛА ФЕДЕРАЛЬНОГО ФОНДА ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ

Окулов Максим Денисович
ФГБОУ ВО Национальный исследовательский университет «МЭИ», студент, Москва, Россия
maxim999555@yandex.ru

Денисенко Вера Константиновна
ФГБОУ ВО Национальный исследовательский университет «МЭИ», научный руководитель, ассистент кафедры БИТ, Москва, Россия

Аннотация
В данной статье представлен проект автоматизированной системы для информационно-аналитического отдела ФФОМС. Система имеет защищенное исполнение. Рассматриваются основные аспекты ее функционирования. Включены исследования угроз безопасности информации и уязвимостей. Проведен анализ и создана усовершенствованная модель защиты информации. Спроектированы логический и физический уровни модели данных. Выполнен сравнительный выбор средств защиты. Рассмотрено шифрование базы данных. Это обеспечивает надежную защиту данных в процессе работы.

Ключевые слова
Автоматизированная система, анализ данных, шифрование, угрозы безопасности, защита информации

Введение

Сейчас технологии развиваются быстро, и объемы обрабатываемой информации растут. Защита данных становится важной задачей для государственных учреждений, особенно в здравоохранении. ФФОМС отвечает за доступность и качество медицинских услуг для граждан России. Это требует надежных решений в области информационной безопасности. Поэтому проект автоматизированной системы для информационно-аналитического отдела ФФОМС направлен на создание улучшенной модели защиты информации. Эта модель будет интегрирована в деловые процессы фонда. В проекте особое внимание уделяется строению и анализу модели защиты информации. Это включает проектирование модели данных автоматизированной системы. Необходимо разработать логический и физический уровни модели данных. Логический уровень будет организовывать данные и их взаимосвязи. Физический уровень обеспечит безопасное и эффективное хранение данных. Реализация этого проекта повысит уровень безопасности информации в ФФОМС. Она также создаст основу для более эффективного управления данными. Это положительно скажется на качестве медицинских услуг и удовлетворенности граждан. В статье мы подробно рассмотрим ключевые аспекты проектирования автоматизированной системы, включая механизмы защиты и ожидаемые результаты.

Исследование области функционирования объекта защищенной автоматизации

Работа ФФОМС направлена на осуществление общего нормативного и организационного управления системой ОМС. Для фонда лучше всего подойдёт линейно-функциональная структура управления.

Система ФФОМС представляет собой связь нескольких частей: IT-отдел, бухгалтерия, юридический отдел, планово-экономический отдел, информационно-аналитический отдел, отдел организации и мониторинга системы ОМС, отдел кадров (рис. 1).

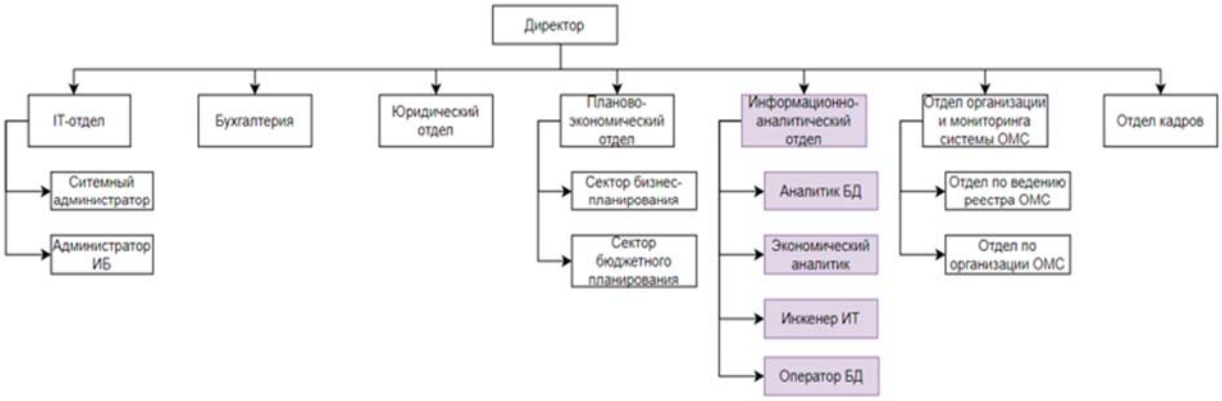

Рис. 1. Организационная структура управления

В процессе автоматизации будет затронут 1 отдел – информационно-аналитический отдел (рис. 2).

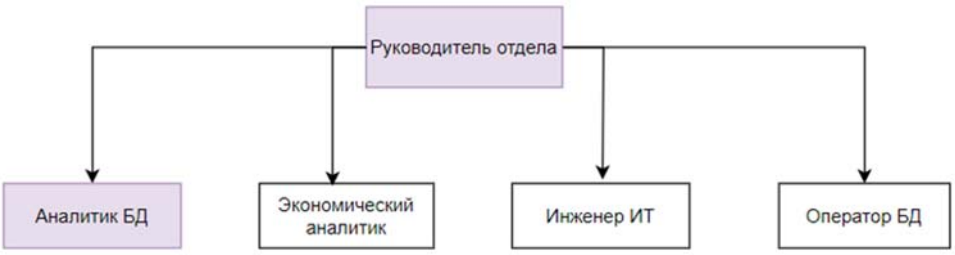

Рис. 2. Структура информационно-аналитического отдела ФФОМС

Оценка угроз безопасности информации и уязвимостей автоматизированной системы

Данный раздел подразумевает под собой метод моделирования угроз и нарушителей безопасности информации в автоматизированных системах защиты информации (АСЗИ) для анализа данных страховых компаний. Он разработан с учётом специфики и условий работы информационных систем государственных учреждений, а также с учетом предъявляемых требований законодательства РФ в области обеспечения информационной безопасности.

Цель анализа угроз информационной безопасности – выявить все потенциальные риски. Эти риски могут нанести ущерб системе. Система работает в соответствии с определенной архитектурой и условиями эксплуатации [1].

Рассмотрим этапы процесса моделирования угроз и нарушителя безопасности информации:

– определение возможных негативных последствий, в результате реализации угроз безопасности информации;

– определение возможных объектов воздействия угроз;

– оценку возможности реализации угроз и определение их актуальности.

Под основными объектами защиты информационной безопасности в ФФОМС приоритетной областью является ИСПДн, а именно «Автоматизированная система в защищённом исполнении информационно-аналитического отдела ФФОМС».

При оценке угроз безопасности информации разберем основные требования [2]:

– определение негативных последствий от реализации угроз;

– определение возможных объектов воздействия угроз;

– оценка способов реализации (возникновения) угроз;

– оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;

– оценка сценариев реализации угроз безопасности информации в системах и сетях.

В результате моделирования угроз безопасности информации формируется перечень актуальных угроз безопасности информации.

ИСПДн предопределена для обработки и хранения информации о страховых компаниях, их показателях и клиентах компании, с целью анализа этих данных и дальнейшем составлении разного вида отчетности.

Персональные данные страховых компаний, обращающихся в ФФОМС, обрабатываются с целью:
– ведения учета общего количества компаний;
– ведения обработки заявок на ОМС и другие медицинские услуги, которые к ним поступают;
– аналитика показателей страховых компаний (оформления счёта);
– осуществления формирования необходимой отчетности.

Персональные данные обрабатываются в соответствии с согласием на обработку персональных данных (ПДн).

Информационная система персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с персональными данными сотрудников: сбор, систематизацию, накопление, хранение, уточнение, обновление, изменение, использование, распространение (передачу), обезличивание, блокирование, уничтожение персональных данных.

Функции автоматизированной системы [3]:
– добавление, редактирование, удаление информации о страховых компаниях и их показателях;
– автоматизация анализа и обработки данных, а также коммуникации между сотрудниками;
– автоматизация процесса коммуникации руководителя отдела и аналитиков;
– наличие многопользовательского режима работы с документами;
– автоматизация процессов формирования отчетов по деятельности информационно-аналитического отдела ФФОМС.

Построение и анализ усовершенствованной модели защиты информации в ходе делового процесса функционирования объекта защищенной автоматизации

Для наглядности построим модель защиты информации в процессе анализа данных страховых компаний (рис. 3).

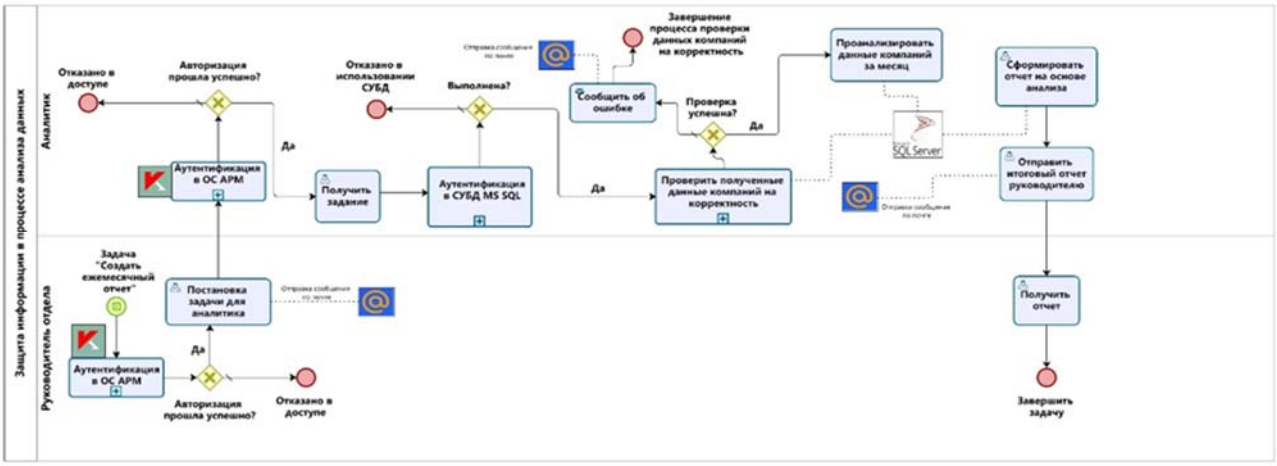

Рис. 3. Усовершенствованная модель защиты информации

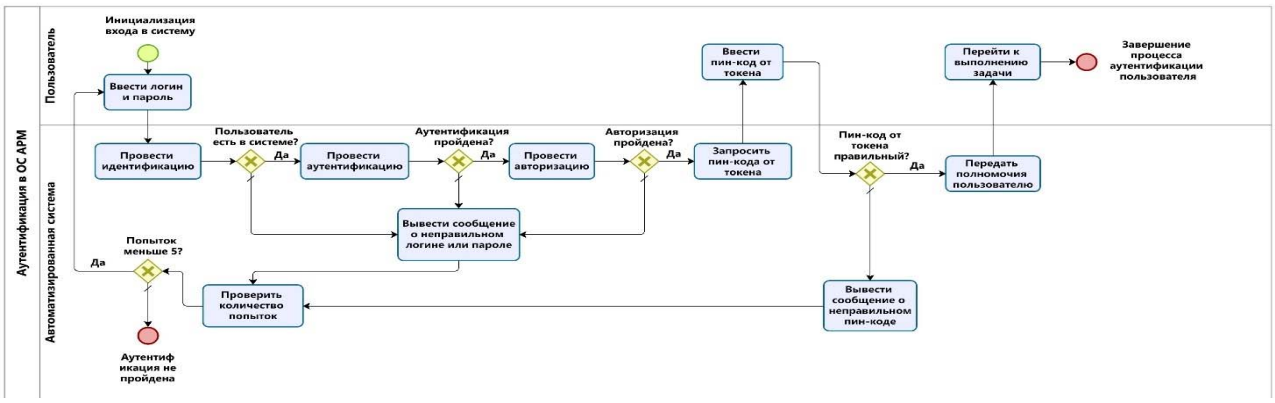

Рис. 4. Схема процедуры двухфакторной парольной авторизации для входа в ОС АРМ

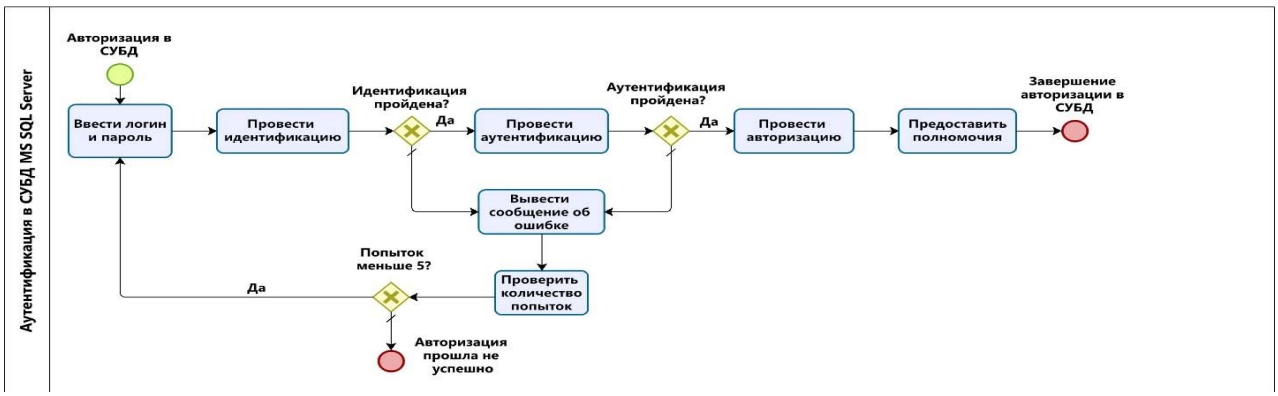

Рис. 5. Схема процедуры аутентификации при входе в СУБД

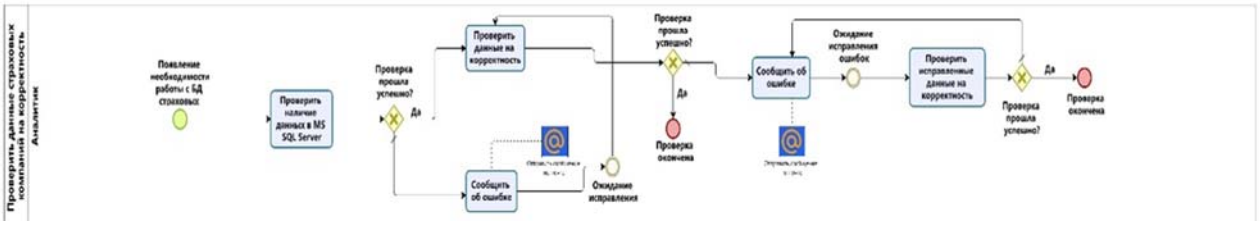

Рис. 6. Схема процедуры проведения проверки данных

В процессе участвуют аналитик и руководитель информационно-аналитического отдела.

Процесс начинается с появления у руководителя задачи «Создать ежемесячный отчет» по определенным страховым компаниям. Руководитель проводит процедуру однофакторной парольной авторизации для входа в операционную систему (ОС) компьютера своего автоматизированного рабочего места, создает задачу для аналитика в системе, а затем направляет ее ему. Аналитик также в начале своей работы авторизируется в системе (рис. 4). Вторым фактором было добавлено предоставление токена Rutoken для повышения защищенности системы. Если на одном из этапов происходит ошибка, система выводит об этом сообщение и даёт возможность повторить вход, если ошибок было меньше 5.

Была внедрена антивирусная защита от Лаборатории Касперского в АРМ аналитика и руководителя информационно-аналитического отдела.

В случае, если авторизация успешно пройдена, аналитик приступает к выполнению задачи. Он проходит авторизацию в системе (рис. 5), проверяет полученные данные на наличие и корректность, если обнаружил ошибку, сообщает об этом коллегам или руководителю своего отдела по электронной почте (рис. 6).

После того как аналитик проверил все данные, он приступает непосредственно к своей задаче – анализу (сравнивает данные страховых компаний за пройденный год). Полученные данные обрабатываются, и на их основе начинают формировать отчет. Затем данные сохраняются и отправляет готовый отчет руководителю по электронной почте.

Проектирование логического уровня модели данных

В качестве метода проектирования базы данных используем метод семантического моделирования данных (сущность-связь) в нотации IDEF1X, являющейся подмножеством SADT методологии [4].

Использование CASE-средства CA ERwin Data Modeler для проектирования моделей данных в рамках ФФОМС позволяет эффективно управлять информацией и улучшать процессы. Для ФФОМС логическая модель может включать сущности, такие как пациенты, страховые полисы, медицинские учреждения, страховые компании и медицинские услуги. Например, сущность "Пациенты" может содержать атрибуты, такие как идентификатор пациента, ФИО, дата рождения, пол и адрес. Сущность "Страховые полисы" может включать номер полиса, идентификатор пациента, идентификатор страховой компании, дату начала и дату окончания действия полиса (рис. 7.)

Имя сущности	Определение
Страховая организация	Данные о медицинской организации, контактная информация
Регион	Номер и название региона
Показатель здоровья	Данные о здоровье
Активность	Данные, показывающие активность медицинской организации за определенный период
Рейтинг	Данные о работе медицинской организации за определенный период
Бюджет	Данные о бюджете

Рис. 7. Сущности / определения

На рисунке 8 представим данные: родительскую и дочернюю сущность, имя и тип связи, семантику связи от родительской сущности к дочерней.

Родительская сущность	Дочерняя сущность	Имя связи	Тип связи	Семантика связи от родительской сущности к дочерней
Регион	Показатель здоровья	Регион-Показатель _здоровья	1:M	Имеет
Регион	Медицинская организация	Регион- Медицинская _организация	1:M	Состоит из
Страховая организация	Активность	Медицинская _организация-Активность	1:M	Имеет
Медицинская организация	Рейтинг	Медицинская _организация-Рейтинг	1:M	Имеет
Медицинская организация	Бюджет	Медицинская _организация-Бюджет	1:M	Владеет

Рис. 8. Связи между сущностями

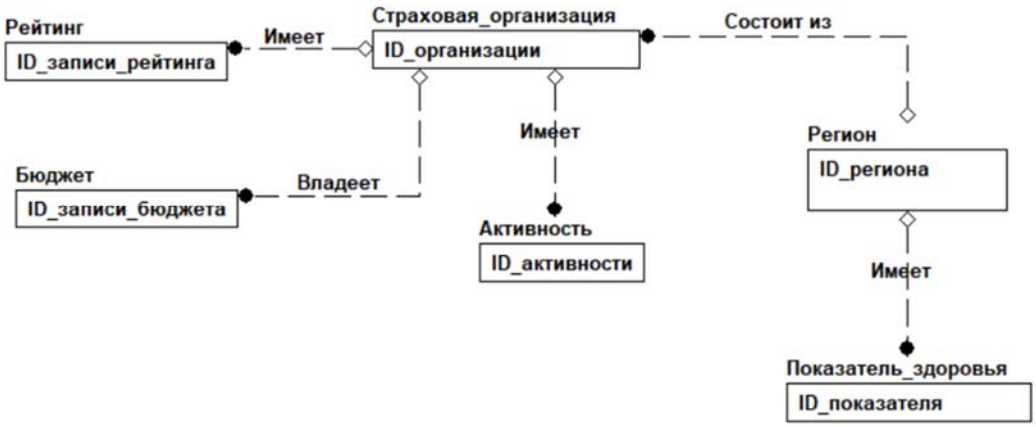

Рис. 9. ER-диаграмма

ER-диаграмма (рис. 9.) демонстрирует ключевые бизнес-правила в определенной области [5]. Например, в диаграмме представлены связи: ФФОМС может обслуживать несколько медицинских учреждений, при этом каждое медицинское учреждение может иметь контракты с несколькими фондами медицинского страхования (многое ко многим). Или же, информационные объекты ФФОМС и мед. учреждение могут связаны отношением один ко многим, так как один фонд может обслуживать много мед. учреждений, в то время как каждое медицинское учреждение может иметь контракт только с одним ФФОМС.

У каждого ключа имеются определенные условия: количество атрибутов в первичном ключе – минимально; не принимают неопределенных значений; схожи с экземпляром сущности.

Модель данных, основанная на ключах – KB-модель (рис. 10-11). PK – первичный ключ, FK – внешний ключ.

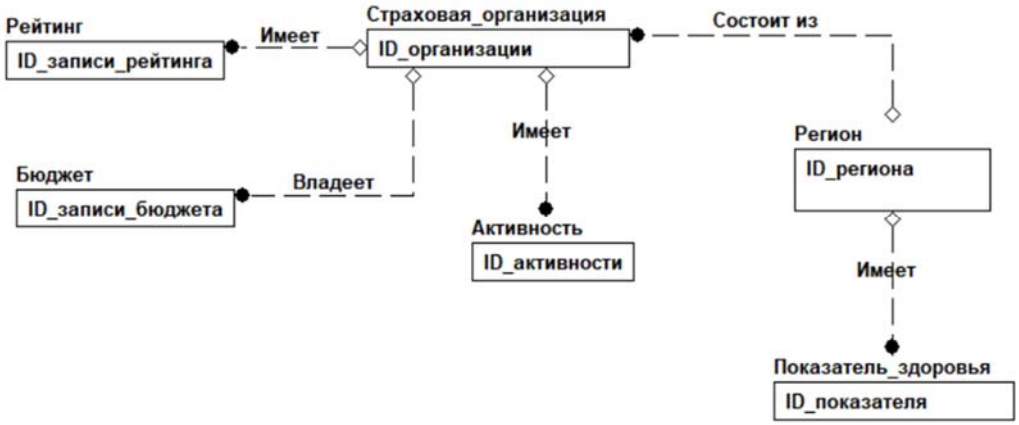

Рис. 10. KB-модель

Имя сущности	Наименование атрибута	Ключ
Страховая организация	ID_организации	PK
	ID_региона	FK
	Название организации	
	Количество пациентов	
	Адрес организации	
	Номер телефона организации	
	Электронная почта организации	
Регион	ID _региона	PK
	Название региона	
Показатель здоровья	ID_показателя	PK
	ID_региона	FK
	Дата	
	Количество потерпевших	
Активность	ID_активности	PK
	ID_организации	FK
	Дата	
	Количество обращений	
	Количество полисов	
Рейтинг	ID_записи рейтинга	PK
	ID_организации	FK
	Дата	
	Рейтинг	
Бюджет	ID_записи бюджета	PK
	ID_организации	FK
	Год	
	Бюджет	

Рис. 11. Атрибуты, сущности

На рисунке 12 каждая детерминанта имеет свой уникальный код (ID_организации), рассмотрим функциональную часть.

Детерминанта	Функциональная часть
ID _организации	ID _региона, Название _организации, Количество _пациентов, Адрес _организации, Номер _телефона _организации, Электронная _почта _организации
ID _региона	Название _региона
ID _показателя	ID _региона, Дата, Количество _потерпевших
ID _активности	ID _организации, Дата, Количество _обращений, Количество _полисов
ID _записи _рейтинга	ID _организации, Дата, Рейтинг
ID записи _бюджета	ID _организации, Год, Бюджет

Рис. 12. Функциональная зависимость

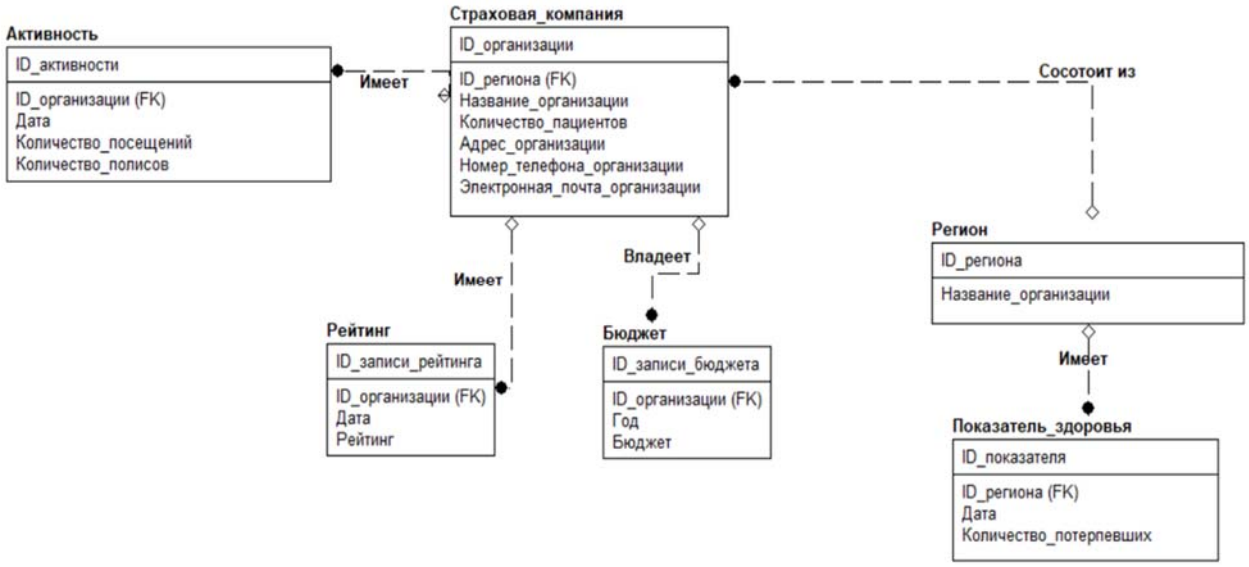

Рис. 13. FA-модель

Атрибутивная модель полного типа (рис. 13). Конкретно рассмотрим функциональную зависимость, где "Страховая компания", которая включает название организации, количество пациентов, адрес организации, номер телефона организации и электронную почту организации. Страховые компании имеют свой рейтинг, владеют определенным бюджетом. В каждом регионе конкретные страховые компании и определенный показатель здоровья (в зависимости от количества потерпевших).

Проектирование физического уровня модели данных

Детально рассмотрим трансформационную модель, которая изображена на рисунке 14. На этом рисунке отчетливо видно, как определяются домены атрибутов сущностей, а также определим области допустимых значений и типы данных. Таблица состоит из имени и описания атрибутов, где используется название атрибута, ключ и шифр домена. У каждой таблицы имеется уникальное название атрибута. Происходит идентификация каждой записи, а также связывание двух разных таблиц между собой за счет первичного и внешнего ключей. Шифр домена служит для обеспечения безопасности передачи данных.

Имя таблицы	Описание атрибутов		
	Название атрибута	Ключ	Шифр домена
Страховая организация	ID_org	PK	D1
	ID_ reg	FK	D1
	Org_name		D8
	Num_of_pat		D1
	Address		D8
	Org_number		D5
	Org_email		D6
Регион	ID_reg	PK	D1
	Reg_name		D7
Показатель здоровья	ID_ ind	PK	D1
	ID_reg	FK	D1
	Date		D4
	Num_of_victims		D1
Активность	ID _act	PK	D1
	ID_org	FK	D1
	Date		D4
	Num_of_visits		D1
	Num_of_policy		D1
Рейтинг	ID_note_of_rat	PK	D1
	ID_org	FK	D1
	Date		D4
	Rating		D9
Бюджет	ID_note_of_budg	PK	D1
	ID_org	FK	D1
	Year		D3
	Budget		D2

Рис. 14. Поля таблиц, их описание и домены

D1, D2, D3 – целочисленные данные; D4 - дата; D5, D6, D7, D8, D9 – строка символов переменной длины.

Трансформационная модель была оптимизирована под формат выбранной СУБД (рис. 15).

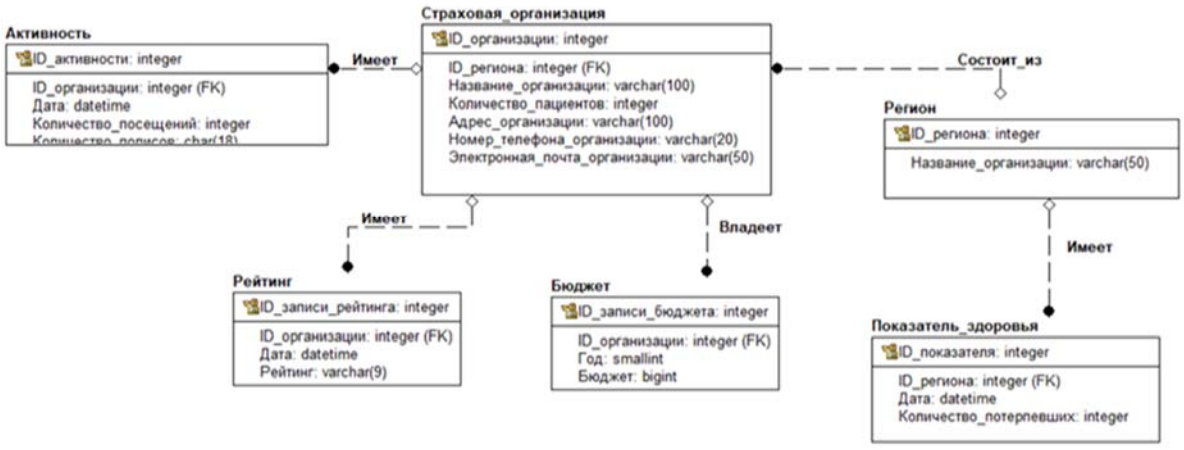

Рис. 15. Т-модель базы данных анализа данных страховых организаций

Сравнительный выбор средств защиты информации

Для выполнения проекта по созданию системы безопасности проводится исследование доступных на рынке решений для защиты информации.

На рисунке 16 представлен сравнительный выбор антивирусного программного обеспечения.

Характеристика	Kaspersky Endpoint Security	Dr.Web Enterprise Security Suite	ESET NOD32 Secure Enterprise Pack
Компания-вендор	АО «Лаборатория Касперского»	ООО «Доктор Веб»	ООО «ИСЕТ Софтвер»
Особенности			
Контроль подключенных устройств	Да	Да	Да
Защита веб-трафика	Да	Да	Нет
Управление утечками данных	Да	Нет	Да
Защита от DDoS-атак	Да	Нет	Нет
Сертификация			
ФСТЭК	№4068	№3509	-
ФСБ	№СФ / СЗИ-0673	№СФ / СЗИ-0450	-
Классы			
Профиль защиты	Б2, В2, Г2	А2, Б2, В2, Г2	-
Уровень доверия	2	2	-

Рис. 16. Сравнительный выбор антивирусного программного обеспечения

По результатам приведенных параметров наиболее функциональным решением для антивирусной защиты является Kaspersky Endpoint Security (KES), так как предоставляет больше возможностей для защиты.

На рисунке 17 представлен сравнительный выбор средств для защиты сети.

Характеристика	VipNet Coordinator	ТСС Diamond VPN/FW
Компания-вендор	АО «ИнфоТеКС»	ООО «ТСС»
Особенности		
Балансировка нагрузки	Да	Нет
Шифрование ГОСТ	Да	Да
Защита от DDoS-атак	Да	Да
Сертификация		
ФСТЭК	№3692	№4066
ФСБ	СФ / 525-4429	-
Классы		
Уровень доверия	4	4
Профиль защиты СОВ	С4	С4
Профиль защиты МЭ	А4, Б4	А4, Б4, В4

Рис. 17. Сравнительный выбор средств для защиты сети

По результатам приведенных параметров наиболее функциональным решением для защиты сети является VipNet Coordinator.

Проект системы защиты информации автоматизированной системы

Автоматизированная система в защищенном исполнении информационно-аналитического отдела ФФОМС функционирует внутри информационно-аналитического отдела и IT-отела.

Рядом с IT-отделом в отдельном помещении находится серверная, доступ к которой осуществляется через физический ключ от замка шкафа. Все сервера, контроллеры домена и главные роутеры находятся в серверном шкафу. Доступ в помещение осуществляется через СКУД.

На рисунке 18 представлена физическая схема сети автоматизированной системы анализа данных страховых организаций.

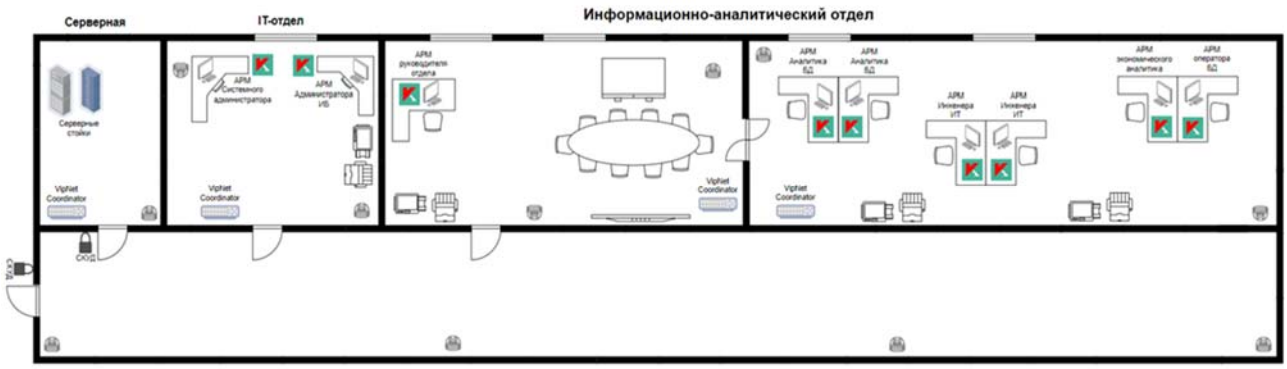

Рис. 18. Физическая схема сети АСЗИ

На рисунке 19 представлена логическая схема сети автоматизированной системы в защищенном исполнении анализа данных страховых организаций.

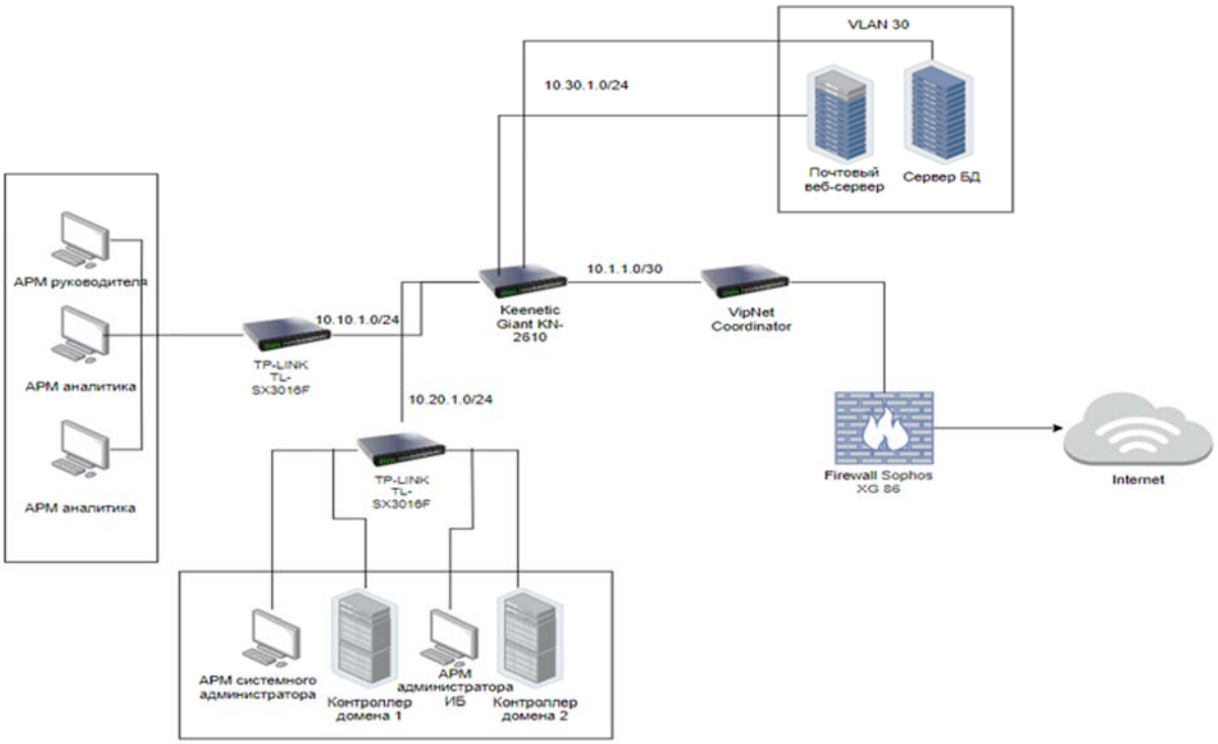

Рис. 19. Логическая схема сети АСЗИ

Шифрование базы данных

Шифрование базы данных будет происходить с применением технологии прозрачного шифрования данных (TDE) [6].

Создание главного ключа шифрования и его резервной копии показано на рисунке 20.

```
USE master;
DROP Master KEY
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'MASTERKEYKR'
BACKUP MASTER KEY
TO FILE = 'D:\Backup\MasterKRBackup.bak'
ENCRYPTION BY PASSWORD = 'MasterKRBackupfordb'
SELECT * FROM sys. key_encryptions
```

100 %

Results | Messages

	key_id	thumbprint	crypt_type	crypt_type_desc	crypt_property
1	101	0x01	ESKM	ENCRYPTION BY MASTER KEY	0xCCEB2D60767FE69A1C845C8E6B7C9CCBF822F7E2B605E2...
2	101	NULL	ESP2	ENCRYPTION BY PASSWORD V2	0x1CCAB7CF4042253A69CD7D1CBE20F1954D6C6282AAD3A39...
3	102	0x01	ESKM	ENCRYPTION BY MASTER KEY	0xFFFFFFFF500100000100000D08C9DDF0115D1118C7A00C...
4	102	0x0300000001	ESKM	ENCRYPTION BY MASTER KEY	0xFFFFFFFF500100000100000D08C9DDF0115D1118C7A00C...

Рис. 20. Ключ БД master и его резервная копия

Создание сертификата CRTKR и его резервной копии с закрытом ключом показано на рисунке 21.

SQLQuery7.sql - A...KWARD\prost (58))* | SQLQuery5.sql - A...KWARD\prost (57))* | SQLQuery4.sql - A...KWARD\pr

```
USE master;
CREATE CERTIFICATE CRTKR WITH SUBJECT = 'fordbCRT'
BACKUP CERTIFICATE CRTKR
TO FILE = 'D:\Backup\FORDBCRT'
WITH PRIVATE KEY
(FILE ='D:\Backup\PrivateFORDBCRT',
ENCRYPTION BY PASSWORD = 'FORDBCRTKR*');
SELECT * FROM sys.certificates WHERE NAME = 'CRTKR'
```

100 %

Results | Messages

```
Msg 15232, Level 16, State 1, Line 2
Сертификат с именем "CRTKR" уже существует или уже добавлен в базу данных.
```

Рис. 21. Создание сертификата CRTKR и его резервной копии с закрытым ключом

Проверка наличия резервных копий главного ключа шифрования и сертификата с закрытым ключом в папке представлено на рисунке 22.

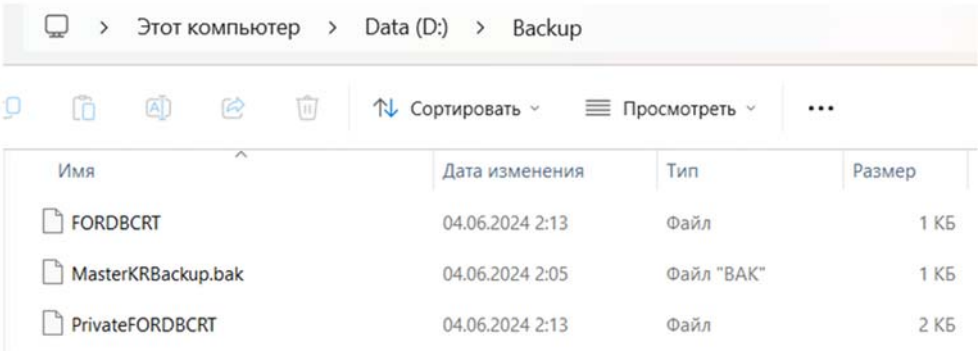

Рис. 22. Проверка наличия резервных копий главного ключа шифрования и сертификата с закрытым ключом в папке

Создание ключа шифрования в базе данных учета платных дополнительных образовательных услуг с использованием сертификата CRTKR, а также включение шифрования представлено на рисунке 23.

Рис. 23. Создание ключа шифрования в базе данных АИС учёта

Проверка создания ключа шифрования в базе данных учета платных дополнительных образовательных услуг представлена на рисунке 24.

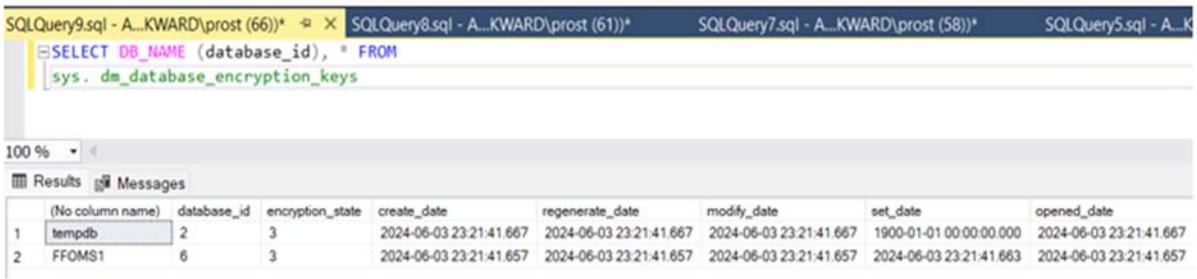

Рис. 24. Создание ключа шифрования

Сведения о текущем положении базы данных представлены в графе encryption_state. По данным SQL Server Books Online (BOL), база данных АИС учёта платных дополнительных образовательных услуг находится в состоянии 3, означает, что процесс первоначального шифрования базы данных завершен. В результате включения шифрования для нашей базы данных база данных tempdb также стала шифроваться.

Проверка вывода зашифрованных баз данных представлена на рисунке 25.

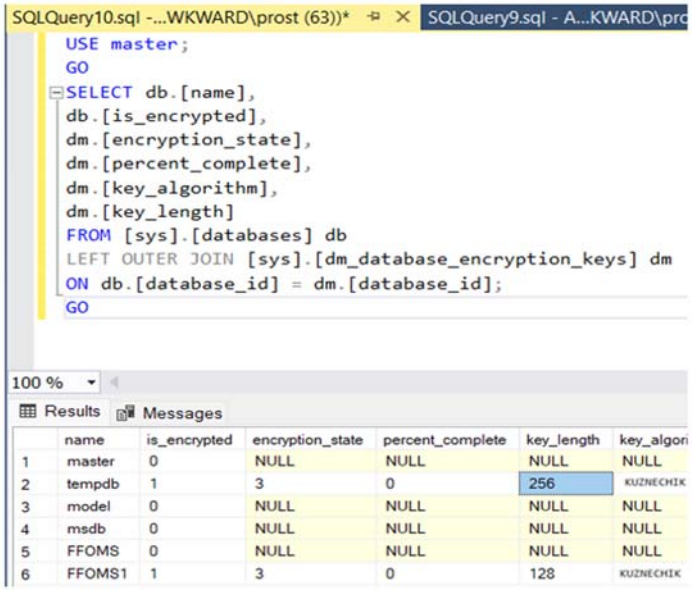

Рис. 25. Вывод списка зашифрованных баз данных

База данных АСЗИ учета платных дополнительных образовательных услуг успешно зашифрована.

Заключение

В заключение, проект автоматизированной системы для информационно-аналитического отдела ФФОМС предлагает комплексный подход к безопасности информации. Исследования функционирования системы и оценка угроз помогли выявить основные уязвимости. Это стало основой для создания усовершенствованной модели защиты. Учтены требования к защите персональных данных в соответствии с законодательной базой. Проектирование логического и физического уровней модели данных, а также выбор средств защиты информации обеспечивают надежную архитектуру системы. Внедрение шифрования базы данных усиливает защиту конфиденциальной информации. Разработанная система соответствует современным требованиям безопасности и помогает эффективно работать информационно-аналитическому отделу, защищая данные в процессе делового взаимодействия.

Литература

1. *Жмуров Д.Б.* Анализ угроз безопасности информации в автоматизированных системах управления технологическими процессами // Самара: Изд-во Инсома-Пресс. 2017. С. 90-95.

2. *Лещук Д.А., Цветов Г.С.* Информационная безопасность автоматизированных систем управления // Молодой ученый. 2022. № 47 (442). С. 13-14.

3. *Дроботун Е.Б.* Методический подход к формированию функциональных требований к системе защиты от компьютерных атак для автоматизированных систем управления и его программная реализация // Международный журнал Программные продукты и системы. 2017. DOI:10.15827/0236-235X.120.690-698

4. *Иванов К.К.* ER-моделирование. Особенности семантического моделирования // Молодой ученый. 2017. № 19 (153). С. 24-26.

5. *Бабанов А.М.* Методика структуризации данных в семантических моделях типа «Сущность-Связь» // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2022. № 60. С. 93-101.

6. *Попов Р.С., Ляликова В.Г.* Шифрование информации в базе данных // Вестник науки. 2022.Т.1. № 12 (57). С. 375-379.

ЭВОЛЮЦИЯ ИНТЕРАКТИВНОЙ РЕКЛАМЫ В УСЛОВИЯХ СТАНОВЛЕНИЯ ЭКОНОМИКИ ВПЕЧАТЛЕНИЯ

Брушкова Людмила Алексеевна
Московский технический университет связи и информатики, доцент кафедры социальных отношений, рекламы и связи с общественностью, кандидат социологических наук, Москва, Россия
lbrushkova@yandex.ru

Аннотация
Статья посвящена рассмотрению феномена интерактивной рекламы и основных этапов ее эволюции за последние 30 лет. Автор показывает, что интерактивная реклама эволюционирует как под воздействием развития информационных технологий, так и становления экономики впечатления. Эмпирической базы работы являются данные статистики и социологических исследований. Автор приходит к выводу, что интерактивная реклама в современном обществе имеет большой потенциал для своего развития в плане более эффективного воздействия на потенциальную аудиторию.

Ключевые слова
Интерактивная реклама, потребительское поведение, экономика впечатлений, цифровое общество, постмодернизм, гедонизм

Введение

Интерактивная реклама – это такой результат организации процесса рекламирования, при котором, с помощью различных средств и методов, создается особая среда для взаимного обмена информацией между зрителем и рекламой [1]. Это один из наиболее успешных и перспективных видов рекламы, который достаточно эффективно вовлекает аудиторию в процесс коммуникации, позволяя будущим покупателям на своем опыте ознакомиться с той или иной продукцией компании.

Безусловно появление этого феномена связано с цифровизацией общества и становлением экономики впечатления. Как справедливо отмечают исследователи, «хотя интерактивная реклама может существовать не только в виртуальном формате, большую ее часть составляет именно цифровая реклама, требующая, для своей активации, «клика» потенциального потребителя по определенной интернет-ссылке» [2].

В настоящее время объем рынка цифровой рекламы постоянно увеличивается. По данным Digital Budget, объем рынка digital-рекламы в России во втором полугодии 2024 года вырос на 11% по сравнению с тем же периодом 2023-го и достиг 131,4 млрд рублей.

Результаты исследований

Интерактивная реклама может рассматриваться как часть экономики впечатлений (experience economy), приходящей, по мнению Дж. Пайна и Дж. Гилмора, на смену экономике услуг.

В современных условиях высококонкурентных рынков компании стремятся привлечь внимание к своей продукции, давая потенциальным потребителям уникальные впечатления и опыт, что может стать их (компаний) конкурентным преимуществом. Таким образом, впечатления начинают рассматриваться как отдельный продукт, созданием и распространением которого занимаются специального обученные люди – «режиссеры впечатлений». Клиенты же в этом случае становятся «зрителями» или «гостями» [4].

Ценностным фундаментом экономики впечатления выступает культура постмодернизма, одним из ведущих принципов которой является гедонизм. Гедонизм наших современников выражается, в частности, в таких активностях как игры, шоппинг, посещение ресторанов и др., которые наполнены самооправданием и чувством удовольствия.

Другой отличительной чертой постмодернистской культуры является мифотворчество, на которое указывал Ж. Бодрийяр. По его мнению, реклама участвует в современном социальном мифотворчестве, и ее истинная роль состоит в том, чтобы не информировать покупателя, а дать ему надежду покупателю на то, что решение проблемы, с которой он сталкивается, будет заключаться в приобретении рекламируемого товара [5].

Экономика впечатления предполагает и соответствующие изменения в форматах рекламного продвижения товаров и услуг, когда на первый план выходит управление эмоциями, возникающими у людей при взаимодействии с тем или иным рекламным продуктом.

Акцент не на пассивное восприятие рекламного сообщения, а на активное вовлечение потенциальной аудитории во взаимодействие с этим сообщением (как правило, с помощью различных игровых способов и техник) может сделать интерактивную рекламу более эффективной, в сравнении с традиционными видами, что особенно актуально в условиях роста во всем мире негативного отношения людей к рекламе.

Эволюция современной интерактивной рекламы во многом совпадает с этапами развития онлайн-рекламы. Здесь можно выделить несколько этапов:

1. Эра баннеров (1994-1997 гг.)

Первая онлайн реклама появилась в 1994 г., ознаменовав начало эры цифровой рекламы. Американская компания At&T заплатила за такую рекламу 30000$, и появилась она в первом электронном коммерческом журнале Hotwired. Реклама представляла собой надпись: «Ты когда-нибудь нажимал своей мышью прямо сюда?», нажав на которую пользователи автоматически переходили на сайт At&T [6]. Эта реклама является и первой интерактивной рекламой, размещенной в Интернете.

Данная реклама обеспечила уровень «кликабельности» равный 44%, сделав онлайн рекламу очень популярной. В 1995 г. появляется реклама так называемого «двойного клика», созданная для отслеживания окупаемости по отношению к количеству показов [7].

2. Эра каналов (1998-2004 гг.)

В 1998 г. появляется поисковая система Google, до сих пор являющаяся основным игроком цифрой рекламной индустрии. Она совершила своеобразную революцию, установив в 2000 г. рекламную систему «Google Adwords», главная цель которой – реализация поиска, где появляется реклама, в той или иной мере совпадающая с запросами аудитории, и в принципе не мешающая поиску нужной информации. Данная система используется и сегодня.

В это же время «дебютировала» реклама на мобильных устройствах. Онлайн реклама была на пике популярности в 1990-е гг., и инвесторы вкладывали огромные средства в новые доткомы. Так, с 1995 по 2000 гг. в онлайн рекламу было вложено 8,2 млрд долл. по всему миру.

В середине 2000-х годов был создан первый код для блокировщика рекламы, что привело к началу своего рода «войны» между рекламодателями и блокировщиками рекламы.

В 2002 году Google обновила Adwords, предоставив возможность использования инструмента Payper-click, когда рекламодатели размещают рекламу на сайтах и платят владельцам сайтов за каждый сделанный на рекламу клик.

2003 и 2004 годы ознаменовались выходом на рынок двух онлайн платформ: LinkedIn и Facebook. Спустя месяц после появления, Facebook выпускает свою первую рекламу в формате баннеров под названием «Facebook Flyers».

В середине 2000 гг. в этой сфере произошел сильнейший кризис – лопнул «мыльный пузырь» доткомов. Многие компании закрылись или значительно сократили свой бизнес. Единственной компанией, пережившей эти потрясения, была Google, которая воспользовалась предоставившейся возможностью и заполнила нишу на рынке, оставленную другими игроками. После «кризиса доткомов» интернет-реклама в целом переживала спад, что не коснулось только поисковых систем, высокая эффективность и надежность которых позволила рынку вырасти до 2,3 млрд долл. в 2003 г.

3. Эра социальных сетей (2005-2008 гг.)

В 2005 году появляется YouTube – самая большая в мире платформа видео-рекламы, в следующем году Google покупает YouTube за 1,65 млрд долл. Социальная сеть привнесла новую форму покупательского взаимодействия. Она дала возможность ставить лайки, «репостить» информацию, а также формировать рейтинги различных видов информации, в том числе и рекламной. YouTube предложила компаниям продвигать их продукцию и услуги в видео-формате.

В 2006 году Facebook предложил потенциальным потребителям рекламные ссылки и небольшую по размеру медийную рекламу, ориентированную на социально-демографические показатели и интересы пользователей. Примерно в это же время на рынке появляется Twitter со своим концептом коммуникации со 140 пользователями, а также созданием хештегов. Таким образом, на тот момент социальные сети предоставили рекламодателям множество возможностей достижения потенциальных и существующих покупателей.

4. Нативная эра (2009-2011 гг.)

По мере роста числа компаний, предоставляющих услуги рекламы через Интернет, пользователей все больше стал раздражать лавинообразный наплыв рекламной информации. В этой ситуации

рекламодатели стали использовать менее явные способы продвижения своих продуктов, что привело к наступлению новой (нативной) эры.

В 2010 году появился фотохостинг Instagram, тогда еще исключительно для устройств на базе IOS. Очень быстро данная платформа стала популярным местом для маркетинга и рекламы. Впоследствии фотохостинг был выкуплен Facebook. В следующем году был создан Snapchat, предоставивший возможность добавлять в видео фильтры расширенной реальности (использование в реальном мире элементов цифровой реальности с помощью камер мобильных устройств).

Twitter познакомил аудиторию с продвинутыми твиттами и оплачиваемой рекламой для знаменитостей. Продвинутые твитты позволили пользователям получить доступ к большей аудитории, обеспечив большее вовлечение с самого начала. Компании стали нанимать знаменитостей для продвижения своих брендов среди подписчиков знаменитостей. Например, Чарли Шин побил рекорд, став первым блогером достигшим 1 миллиона подписчиков за 25 часов после создания аккаунта. Спустя несколько дней он стал продвигать спонсорские твитты.

5. Эра смартфонов (2012 г. – настоящее время)

В 2012 году Instagram продемонстрировал спонсорам возможность, позволяющую пользователям запускать рекламу, продвигая старые или новые посты.

Возросшая популярность смартфонов заставила рекламодателей сосредоточится на рекламе внутри мобильных приложений, покинув сеть браузеров мобильных устройств. К примеру, голосовая технология Алекса дала возможность пользователям осуществлять голосовой поиск. В 2015 году объем траффика мобильной рекламы превысил трафик веб-рекламы. Увеличившееся потребление видео-рекламы показало рекламодателям, что это лучшее место для продвижения своей продукции. Маркетинг в реальном времени стал модным словом.

В 2016 году игра Pokemon Go стала своеобразной сенсацией. Применение дополненной реальности на мобильных устройствах привлекло более чем 45 млн пользователей. Естественно, рекламодатели также обратили на это внимание.

Развитие голосовых инструментов, искусственного интеллекта и других цифровых технологий создали новые возможности для развития рекламы. Ключевой целью современных рекламодателей стало понимание и предсказание намерений и поведения потенциальных потребителей с тем, чтобы предоставлять им все более персонализированную менее раздражающую рекламу.

Заключение

Эволюция интерактивной рекламы за последние 30 лет связана как с прогрессом в сфере информационно-коммуникационных технологий, так и формированием экономики впечатления, когда на первый план выходит все более персонализированный подход к каждому потенциальному потребителю.

Как свидетельствуют проведенные исследования, одной из наиболее серьезных проблем в сфере организации рекламной коммуникации является рост негативного отношения населения к рекламе. При этом Россия относится к числу стран, где отмечается наиболее сильное неприятие рекламы. Так, согласно, исследованию Platforma, 79% россиян не доверяют таргетированной и контекстной рекламе, 94% не верят рекламе в социальных сетях [8]. По данным Global Trust in Advertising, в настоящее время Россия, по уровню недоверия рекламе, находится на третьем месте в мире – 53% [9].

Согласно данным недавнего опроса SuperJob, около 59% респондентов-россиян заявили, что испытывают к рекламе только раздражение. Кроме того, почти 58% опрошенных сообщили, что рекламные объявления не стимулируют их совершить покупку

Недостаток доверия к рекламе наблюдается и среди поколения нулевых, которое является в настоящее время самым платежеспособным среди тех, кто является постоянными «резидентами» виртуального мира [10]. Как показывают исследования, наибольшее раздражение у молодежи вызывает такой вид интерактивной рекламы как всплывающая реклама [2].

Другой проблемой является рост числа пользователей, подключающих на своих мобильных устройствах блокировщики рекламы. Результаты исследования Google Analytics показали, что более половины их пользователей (58%) ставят AdBlock, чтобы не видеть рекламу [11]. В 2015 году рекламодателям в мире эта блокировка стоила 22 миллиарда долларов.

Одним из способов решения данной проблемы могло бы быть использование такого интерактивного формата, который позволил бы покупателям делиться на различных площадках своими впечатлениями о сделанных покупках. Так как люди сначала доверяют другим покупателям, а уже потом брендам, поэтому рекламодателям нужно сосредоточиться именно на этой области [12].

Благодаря развитию информационных технологий интерактивная реклама может стать эффективным инструментом воздействия на потенциального потребителя. Так, использование дополненной реальности, воздействие через мобильные приложения помогает вовлечь целевую аудиторию наиболее эффективно.

С другой стороны, для того чтобы быть эффективной, реклама должна продвигать те товары или услуги, чья польза очевидна или, по крайней мере, должна казаться потребителям таковой. Ведь реклама продукции, которая покажется аудитории бесполезной, не будет формировать сильные положительные эмоции, чтобы стимулировать покупательскую активность.

Литература

1. *Еленевская М.* Интерактивная реклама в многоязычном обществе: диверсификация жанра – Жанры речи, 2017. No1(15). С. 101-110. URL: https://www.elibrary.ru/item.asp?id=30268971 (дата обращения: 20.01.2025).

2. *Брушкова Л.*А., *Печерских О.Г.* Интерактивная реклама как новый фактор воздействия на потребительское поведение молодежи // Цифровая социология, 2024. №3. С. 53-61.

3. Расходы на digital-рекламу в России за полгода превысили 131 млрд рублей. 2024. https://www.forbes.ru/biznes/529466-rashody-na-digital-reklamu-v-rossii-za-polgoda-prevysili-131-mlrd-rublej (дата обращения: 20.01. 2025).

4. *Пайн Б.Дж., Гилмор Дж.Х.* Экономика впечатлений: Как превратить покупку в захватывающее действие. Альпина Паблишер. 2018. https://hse.alpinadigital.ru/book/15220 (дата обращения: 20.01.2025).

5. *Бодрийяр Ж.* Общество потребления. М.: Издательство АСТ, 2021. 382 с.

6. *Hesterberg K.* A Brief History of Online Advertising. 2021. Hubspot. https://blog.hubspot.com/marketing/history-of-online-advertising (дата обращения: 20.01.2025).

7. *Mehta N.* Evolution of Digital Advertising: Happy 25th Digital Advertising and Many More to Come. 2019. https://adscholars.com/blog/evolution-of-digital-advertising/ (дата обращения: 20.01.2025).

8. Россияне не верят рекламе и покупают благодаря ей. Как и почему это работает // Cnews. 2023. https://www.cnews.ru/news/line/2023-04-11_rossiyane_ne_veryat_reklame (дата обращения: 20.01.2025).

9. Только 53% россиян доверяют рекламе – Nielsen, 2021. https://adindex.ru/news/researches/2021/12/21/301005.phtml (дата обращения: 20.01.2025).

10. *Quick T.* The Evolution of Advertising Personalization. https://medium.com/@tysonquick/the-evolution-of-advertising-personalization-16147c950819 (дата обращения: 20.01.2025).

11. Исследование: более половины продвинутых пользователей блокируют Google Analytics. 2021. https://habr.com/ru/news/575802/ (дата обращения: 20. 01.2025).

12. *Quick T.* Advertising evolution: how Personalization Has Improved over Time. https://instapage.com/blog/advertising-evolution-how-personalization-has-improved-over-time-4 (дата обращения: 20. 01. 2025).