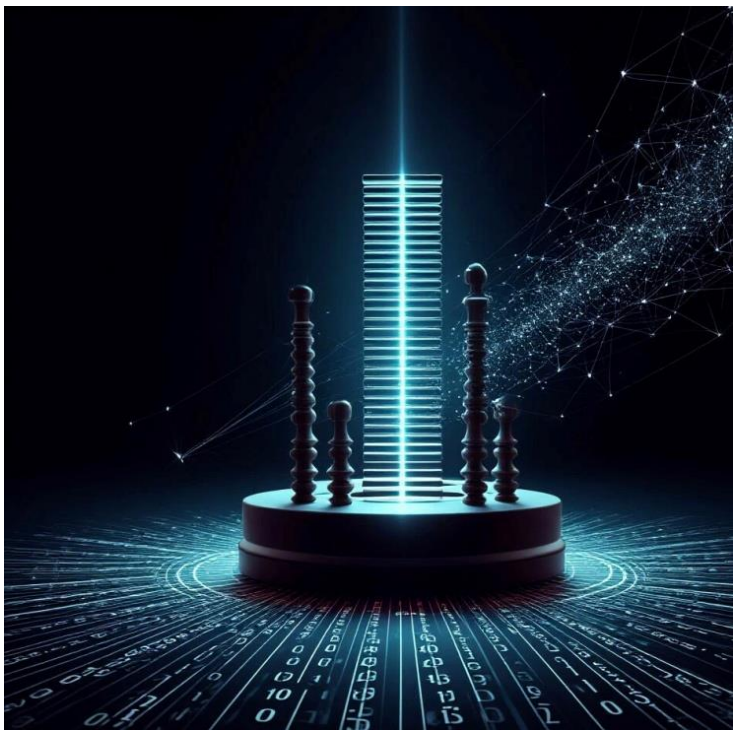
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ
«ЯСЕНОВСКАЯ ШКОЛА №2 ИМ. Д.В. ЛАЗУТИНА»

ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА

НА ТЕМУ: "ИСТОРИЯ РАЗВИТИЯ КОМПЬЮТЕРОВ: ОТ АРИФМОМЕТРА ДО СОВРЕМЕННЫХ СМАРТФОНОВ. ЦИФРОВОЙ СЛЕД: ЧТО МЫ ОСТАВЛЯЕМ В ИНТЕРНЕТЕ И КАК ЭТО ВЛИЯЕТ НА НАШУ ЖИЗНЬ"



Подготовили: обучающийся 7-А класса - Казимир Давид,
обучающийся 7-Б класса – Махотенко Дмитрий,
обучающаяся 7-Б класса - Лотош Татьяна

Руководитель: учитель математики - Скупейко М.И.

г. Ровеньки, пгт.Ясеновский

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования:

Компьютеры стали неотъемлемой частью нашей повседневной жизни, начиная с простейших механических устройств прошлого века и заканчивая мощными смартфонами современности. За короткий промежуток времени технологии совершили огромный скачок вперед, кардинально преобразив многие сферы человеческой деятельности. Этот путь развития заслуживает подробного изучения, ведь понимание истории помогает осознать перспективы дальнейшего прогресса.

Параллельно развитию технологий стремительно растет количество цифровых следов, которые каждый из нас оставляет в сети ежедневно. Каждый клик, каждое сообщение и даже простое посещение сайта становится частью огромной базы данных, доступной различным компаниям и организациям. Как именно этот цифровой след влияет на нашу жизнь? Какие риски и возможности он создает? Эти вопросы становятся особенно актуальными в эпоху всеобщего распространения цифровых платформ и сервисов.

Эта работа ставит перед собой цель проследить эволюцию компьютерных технологий и проанализировать последствия цифрового следа, который мы оставляем в виртуальном пространстве. Она призвана расширить наши представления о роли технологий в современном обществе и выявить возможные направления дальнейшего исследования и совершенствования системы защиты личной информации.

Цель работы:

Изучить историю развития вычислительных технологий от первых механических устройств до современных мобильных гаджетов, а также исследовать влияние цифрового следа на личную жизнь пользователей, выявляя потенциальные угрозы и преимущества для современного общества.

Задачи:

1. Изучение исторического контекста: Описать основные этапы развития вычислительной техники, начиная с первых механических калькуляторов и заканчивая современными высокопроизводительными компьютерами и мобильными устройствами.
2. Анализ эволюции интерфейсов взаимодействия: Рассмотреть изменения способов взаимодействия человека с компьютером, включая переход от командных строк к графическим интерфейсам и сенсорным экранам.

3. Исследование влияния цифровизации на общество: Проанализировать, каким образом развитие компьютерной техники повлияло на повседневную жизнь людей, экономику, образование и социальную сферу.

4. Оценка рисков и преимуществ цифрового следа: Определить типы данных, формирующих цифровой след каждого пользователя, оценить их значение и возможное использование третьими лицами.

5. Выявление мер по защите персональных данных: Предложить рекомендации по повышению уровня информационной безопасности и минимизации возможных негативных последствий хранения и обработки персональных данных.

Эти задачи позволят достичь поставленной цели и сформировать полное представление о развитии компьютеризированных технологий и влиянии цифрового следа на современную жизнь.

Объект исследования:

Объектом исследования является процесс развития вычислительных технологий и их воздействие на человеческую деятельность, а также формирование и хранение цифровых следов пользователями в интернет-пространстве.

Предмет исследования:

Предметом исследования выступают ключевые исторические события и тенденции развития компьютерных технологий, механизмы формирования цифрового следа, способы сбора и анализа персональной информации, а также меры по обеспечению конфиденциальности и информационной безопасности в условиях повсеместного присутствия сетевых технологий.

Гипотеза:

Развитие компьютерных технологий оказывает значительное влияние на социальные процессы и поведение пользователей в интернете, способствуя увеличению объема и разнообразия создаваемого ими цифрового следа. Чем больше информации хранится онлайн, тем выше риск её несанкционированного использования, однако современные методы шифрования и контроля позволяют минимизировать эти риски при условии осознанного подхода к управлению своими цифровыми ресурсами.

Методы исследования

Для достижения поставленных целей и решения сформулированных задач будут использованы следующие научные методы:

Теоретические методы:

Исторический метод – изучение исторических этапов развития вычислительной техники и анализа ключевых изобретений, повлиявших на современное состояние отрасли.

1. **Сравнительный анализ** – сопоставление особенностей различных поколений компьютеров и подходов к обработке информации.
2. **Контент-анализ** – исследование материалов публикаций, научных статей и статистических отчетов, посвященных проблемам защиты персональных данных и управления цифровым следом.

Эмпирические методы:

1. **Анкетирование** – сбор первичной информации о восприятии риска утраты приватности среди пользователей интернет-сервисов.
2. **Наблюдение** – отслеживание поведения пользователей в социальных сетях и интернет-ресурсах для выявления типичных моделей действий и формирования цифрового следа.

Аналитический метод:

1. **Статистический анализ** – обработка полученных эмпирических данных для выявления закономерностей и тенденций.

Использование комплекса указанных методов позволит обеспечить всестороннее и объективное рассмотрение проблемы и достижение заявленных результатов исследования.

Прикладная ценность исследования

Проведенное исследование имеет высокую прикладную значимость благодаря следующим аспектам:

1. **Повышение осведомленности населения**: Результаты исследования способствуют формированию у пользователей интернета понимания важности сохранения своей приватности и правильного обращения с персональными данными.
2. **Разработка рекомендаций по кибербезопасности**: Анализ механизмов формирования цифрового следа позволяет разработать практические советы и руководства по защите информации для частных лиц и организаций.
3. **Оптимизация государственных инициатив**: Исследование может стать основой для разработки законодательных актов и нормативных документов, направленных на защиту прав граждан в киберпространстве.

Таким образом, данное исследование представляет интерес не только для академического сообщества, но и для широкого круга читателей, заинтересованных в

обеспечении собственной информационной безопасности и понимании перспектив развития цифровых технологий.

I ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.ИСТОРИЯ РАЗВИТИЯ КОМПЬЮТЕРОВ

1.1 Эволюция вычислительных устройств

Эволюцию вычислительных устройств можно условно разбить на несколько этапов:

ручной (до XVII века);

механический (до конца XIX века);

электромеханический (до середины XX века);

электронный (по настоящее время).

Идея создать прибор для вычислений появилась еще примерно 3 тыс. лет до нашей эры в Древнем Вавилоне — там создали первые счетные доски, известные нам как "абаки". Позже их переняли и адаптировали в Древней Индии, Древнем Китае, Древней Греции и Древнем Риме. Приборы использовали для торговли, учетов, обучения арифметике.

В Средние века вычислительная техника почти не развивалась. Только в Новое время случился рост объемов расчетов: это сподвигло изобретателей создать механические вычислительные машины.

В конце XV — начале XVI века Леонардо да Винчи спроектировал счетное устройство, содержавшее 13 параллельных стержней с большими и маленькими зубчатыми колесами. Так, 10 оборотов одного стержня приводили к одному полному обороту второго, и так далее. Профессиональное сообщество до сих пор спорит об этом устройстве и его предназначении.

Активное развитие счетных устройств пришлось на XVII век. В 1623 году Вильгельм Шиккард разработал первую модель арифмометра, в 1642 году Блез Паскаль сконструировал суммирующую машину "Паскалина", а в 1673 году Готфрид Вильгельм Лейбниц предложил свой вариант арифмометра.

В 1804 году Жозеф Жаккар создал автоматизированный ткацкий станок, в котором использовались перфокарты (от лат. perforo, что означает "пробивать") — картонные карточки, на которых с помощью отверстий закодирована информация. Устройство позволило производить ткани со сложными узорами. Но ближе всех к созданию компьютера оказался профессор математики Кембриджского университета Чарльз Бэббидж в XIX веке.

Профессор Бэббидж разработал принципы построения вычислительных машин: программное управление, хранение данных на перфокартах и деление информации на

разные типы. Его первым проектом стала разностная машина, предназначенная для автоматизации приближенных вычислений. Над ней Бэббидж работал с 1822 года.

В Великобритании математик заручился господдержкой, после чего строил разностную машину на протяжении девяти лет, но так и не завершил проект. Однако часть изобретения работала и выполняла расчеты.

В процессе работы у Бэббиджа родилась идея нового изобретения — аналитической машины. Она была прообразом современного цифрового компьютера, роль "блока питания" которого должен был выполнять паровой двигатель. Устройство состояло из склада (жесткого диска), мельницы (процессора), печатающего устройства и управляющих барабанов (микропрограмм).

Подготовкой карт операций — программ — занималась Ада Лавлейс, дочь британского поэта Джорджа Байрона. Она стала первым программистом в мире, впоследствии в ее честь назвали язык программирования Ada. Сам проект Бэббиджа остался нереализованным.

По мнению эксперта Алексея Бутырина, машина Бэббиджа — классический пример изобретения, опередившего свое время. Идеи ученого были верными — это подтвердили опыты современных энтузиастов, которые достроили его разностную машину по авторским чертежам и обнаружили, что она функционирует так, как и задумывалось. Для этого им потребовались современные технологии металлообработки.

Важный вклад в автоматизированную обработку информации внес русский изобретатель Семен Корсаков, который жил и работал в XIX веке. Он сконструировал механические устройства, в которых информация кодировалась на перфокартах. Среди его изобретений:

прямолинейный гомеоскоп с неподвижными частями;

прямолинейный гомеоскоп с подвижными частями;

плоский гомеоскоп;

идеоскоп;

простой компаратор.

Чтобы продвинуть устройства, в 1832-м Корсаков написал трактат "Начертание нового способа исследования при помощи машин, сравнивающих идеи". В том же году он представил изобретения Императорской Академии наук в Санкт-Петербурге. Там их отклонили, так как не увидели практической пользы.

Изобретения Корсакова были забыты, а вновь использовать перфокарты для обработки информации предложили только в 1888-м. Это сделал американский инженер

Герман Холлерит, который построил первую электромеханическую счетную машину — табулятор. Устройство могло считывать и суммировать данные, которые кодировались на перфокартах.

Холлерит стоял у истоков IBM — в 1896 году он основал компанию Tabulating Machine Company, которая в 1911 году объединилась с двумя другими фирмами в Computing-Tabulating-Recording. Позже ее переименовали в IBM. Компания долгое время выпускала табуляторы, но уже в 1937 году ученый Говард Эйкен предложил ей проект первой электромеханической вычислительной машины — "Марк 1". В 1944-м IBM построила ее и установила в Гарвардском университете.

Вес такого устройства превышал 4 т, его длина и высота — 16 и 2,5 м соответственно, а общая длина проводов составила 800 км. Компьютер мог осуществлять три операции сложения и вычитания в секунду, а на деление уходило до 15 секунд. Эта машина уже обладала чертами более поздних ЭВМ, но все еще была электромеханической, а не электронной, и работала довольно медленно.

1.2 Хитроумная машина Семена Корсакова

В России XIX века был свой Чарлз Бебидж — Семен Корсаков, дворянин, успешный государственный деятель, который помимо гомеопатии увлекался еще и изобретением интеллектуальных машин.

В 1832 году Корсаков опубликовал брошюру «Начертание нового способа исследования при помощи машин, сравнивающих идеи» и представил ее Академии наук. Для хранения и кодирования информации он предлагал использовать перфокарты — те самые деревянные пластинки с отверстиями, которые тогда применялись только в ткацких станках Жаккарда.

Всего машин было пять: линейный гомеоскоп с неподвижными деталями, линейный гомеоскоп с подвижными деталями, плоский гомеоскоп, идеоскоп и простой компатор. Все машины помогали не только упорядочивать, но и сравнивать большие объемы данных. Сам Корсаков использовал их для составления базы лекарств по гомеопатии. Ученый задавался вопросом «Как найти нужное лекарство для пациента?». И нашел ответ: нужно «набрать» на деревянной пластинке всю картину болезни, например тошнота, головная боль, температура, и сравнить, совпадут ли выдвижные штырьки с отверстиями перфокарты.

Но тогда никто не оценил идеи Корсакова, изобретение отклонили, хотя подобным образом уже тогда можно было классифицировать практически любую информацию, в

том числе военные сведения. Сам ученый тоже понимал, что время для его машин еще не пришло (приложение А).

1.3 Кто изобрел компьютер?

Несмотря на то что основоположником идеи первого механического компьютера считается Чарлз Бебидж, только в 40-е годы XX века люди всерьез задумались о необходимости строить мощные машины, способные автоматически выполнять сложные технические расчеты. И для этого была веская причина — Вторая мировая война. Умение кодировать и декодировать большие объемы информации давало неоспоримое преимущество в военных действиях. Разработки велись в разных странах, поэтому на роль отца-основателя компьютера претендовали сразу несколько ученых.

Немецкого инженера Цузе часто называют изобретателем компьютера. Он первым объединил в вычислителе арифметические и логические операции, ввел термин «машинное слово», а также изобрел язык программирования Plankalkul. В 1938 году была готова его машина с программным управлением Z1. Сегодня ее воссозданная модель хранится в Музее вычислительной техники в немецком Падеборне.

Z1 ученый строил в гостиной дома родителей, она помещалась на площади примерно 4 кв.м и была полностью механической, на рычажной основе. Далее были модели Z2, где уже применялись электромагнитные телефонные реле, и Z3, которая умножала два числа за пять секунд. Последнюю использовали для проектирования крылатых ракет «Фау».

Именно Z3 считают первым работоспособным программируемым компьютером. Z4 должна была стать еще более мощной машиной, но в 1942 году руководство Третьего рейха было уверено, что война скоро закончится, и вкладывать деньги в долгосрочные проекты не посчитало нужным.

Во время бомбардировок Берлина все машины Цузе были уничтожены, за исключением недостроенной модели Z4, которую ученый успел вывезти в Альпы. Иногда о машинах Цузе говорят как о «компьютерах Гитлера» (из-за источника финансирования), но при этом сам Цузе членом партии не был и, по слухам, идеологию фашизма не разделял (приложение Б).

Американский физик Джон Атанасов в 1939 году опубликовал концепцию современной вычислительной машины, где расчет проводится с помощью логических (а не математических) действий и где использовалась двоичная система исчисления.

В том же году вместе с напарником Клиффордом Э.Берри он строит машину ABC (Atanasoff Berry Computer), способную решать линейные уравнения с несколькими

десятками неизвестных. Ее называют первым электронным компьютером. Оперативное запоминающее устройство ABC было выполнено на вращающемся барабане с конденсаторами, а арифметическое — на радиолампах. Данные вводились с помощью перфокарт. Но проект так и не был закончен, потому что США вступили в войну и Атанасов перешел на службу в военно-морскую лабораторию.

При этом в 1973 году окружной суд США в Миннеаполисе признал, что основные идеи Дж. Моучли, реализованные позже в ENIAC, были получены от Атанасова (приложение C).

Все, кто хоть немного интересуется информатикой и IT, встречали термин «машина Тьюринга». Алан Тьюринг — английский математик, автор того самого теста, который успешно должен пройти искусственный интеллект к 2029 году.

24-летний Тьюринг в 1936 году выпускает работу, где описывает устройство для решения проблемы математической логики, создает первую модель универсальных вычислений. По сути, он объяснил, что машина может решить любую задачу при условии, что ее (задачу) можно алгоритмизировать.

Машина Тьюринга состоит из программы, ленты с ячейками, автомата или головки для чтения и записи. Данные подаются на ленту, которая поделена на ячейки, каждая из которых либо содержит символ, либо является пустой. Машина может обрабатывать символы, стирать или записывать их в соответствии с инструкциями внутри памяти. Запись, вычисление и сдвиг — именно эти три операции повторяет машина Тьюринга. Этот алгоритм даже сегодня используют для оценки возможностей квантовых компьютеров (ПРИЛОЖЕНИЕ D).

Американцы Моучли и Эккерт в 1945 году презентовали компьютер ENIAC (Electronic Numerical Integrator and Calculator) — первый электронный цифровой вычислитель для широкого спектра задач, работал полностью на электронных схемах.

Проект, разработанный еще в 1942 году, лежал без дела, пока им не заинтересовались американские военные. В условиях строгой секретности машину весом 30 т, занимавшую площадь почти 300 кв. м, собирали более двухсот специалистов.

ENIAC работал на лампах (их было 17 468!) и мог выполнять 5 тыс. операций сложения в секунду. Правда, лампы все время приходилось менять, потому что они перегорали, и это существенно осложняло взаимодействие с компьютером.

Первая в мире ЭВМ — ENIAC — была готова уже после завершения Второй мировой войны, и ее сразу же задействовали в работах по созданию водородной бомбы (ПРИЛОЖЕНИЕ E).

1.4 Первый компьютер в России

В нашей стране история вычислительной техники началась в 1948 году. Авторы первого проекта автоматической цифровой вычислительной машины — Исаак Брук и Башир Рамеев. 4 декабря они получили авторское свидетельство на изобретение, поэтому именно эта дата считается неофициальным днем рождения российской информатики.

Рамеев и Брук вдохновились идеей ENIAC, но делали упор на то, что бесконечно ломавшиеся электронные лампы стоит заменить на миниатюрные полупроводниковые диоды, которые впоследствии можно будет использовать не только для стационарных, но и передвижных компьютеров. Однако вычислительную машину М-1 удалось собрать только к декабрю 1951 года (ПРИЛОЖЕНИЕ F).

А в 1948 году Сергей Лебедев — директор Института электротехники Академии наук в Киеве — начинает работать над малой электронной счетной машиной МЭСМ, которая в итоге и получит статус первой в Союзе электронной цифровой вычислительной машины, ее выпустят на несколько месяцев раньше, чем М-1.

МЭСМ размещалась на площади 60 кв. м. 6 тыс. электронных ламп и трехадресная система команд позволяли выполнять 50 операций в секунду, но внешняя память у машины отсутствовала. МЭСМ не стали запускать в серийное производство, однако большинство первых советских программистов обучались именно на ней. Позже под руководством Лебедева были созданы 15 типов ЭВМ — от ламповых до суперкомпьютеров на интегральных схемах.

1.5 Первый персональный компьютер

В 1980-х годах прошлого века началась эпоха персональных компьютеров — малогабаритных машин, которыми могли пользоваться люди без профильного образования.

Чтобы уменьшить в разы аппаратную часть компьютера, понадобились микропроцессоры. Впервые их начала выпускать компания Intel в 1971 году. При стоимости $200 четырехбитный Intel 4004 превосходил по производительности ENIAC — выполнял 60 тыс. операций в секунду.

Первый персональный компьютер, который получил массовое распространение, выпустила в 1981 году компания IBM. Модель PC 5150 имела объем памяти 64 килобайта, а жесткий диск в нем заменяли маленькие дисководы.

Но еще в 1977 году был представлен один из успешных персональных компьютеров того времени — Apple II, который потом в различных вариациях успешно продавался в течение 16 лет.

Первым советским ПК считается ПЭВМ «Агат» 1982 года, где за основу был взят микропроцессор, похожий на тот, что стоял в Apple II. Но даже после этого в стране не возник компьютерный бум, как в США. Видимо, считалось, что советским гражданам высокотехнологичные машины дома попросту не нужны — это же не холодильник и не телевизор. Однако это не остановило народных умельцев — инженеры-самоучки, проявляя чудеса смекалки, собирали собственные компьютеры по чертежам, которые были опубликованы в иностранных журналах (ПРИЛОЖЕНИЕ G).

1.6 Что нас ждет в компьютерах будущего?

Компьютеры с ИИ

Этот пункт идет первым, потому что такие системы уже реализованы. Сейчас идет активное развитие искусственного интеллекта — ИИ решает любые задачи, пишет тексты, сценарии, создает видео, фотографии. Решает любые задачи практически во всех областях. Недавно сообщалось, что ИИ за два дня помог найти потенциальное решение задачи по борьбе с супербактерией, которую ученые исследовали более 10 лет. Ученые решили эту задачу самостоятельно, а потом решили дать вводные искусственному интеллекту. Представьте, сколько же ИИ сэкономил времени?

Для полноценной работы искусственного интеллекта в том виде, в котором он есть, нужны большие мощности и огромное количество данных — ИИ должен обучаться, чтобы решать задачи. Пройдет немного времени, и привычные компьютеры уже не будут такими. Например, вам не нужно будет заполнять таблицу в Excel руками, достаточно будет попросить компьютер это сделать и дать ему вводные. Появятся компьютеры со встроенными ИИ-модулями (например, нейропроцессорами), которые смогут выполнять задачи локально, без подключения к интернету — такие ПК будут по-настоящему «умными» и адаптивными.

Современные ОС уже начали использовать искусственный интеллект для улучшения работы, но пока еще далеко не на полную мощность. Пройдет время, и компьютер будет смело конкурировать с человеческим мозгом.

Квантовые компьютеры

Обычные компьютеры работают с битами, которые имеют в двоичной системе всего два состояния — 0 и 1. Представьте себе — абсолютно весь цифровой контент, будь то текст, фильм, фотография, представлены огромным количеством символов 01 в определенной последовательности. Компьютер преобразовывает данные цифры в то, что мы наблюдаем сейчас на экране.

Квантовый компьютер работает иначе — он использует кубиты, которые могут находиться одновременно сразу в двух состояниях (суперпозиция): 1 и 0. Кубиты могут быть представлены электронами, фотонами или другими частицами.

Пока что квантовые компьютеры находятся в стадии эксперимента и исследования. Уже есть рабочие прототипы, но есть множество нюансов. Хоть и скорость такого вычисления во много раз превышает скорость работы обычных компьютеров, но есть проблемы:

- Кубиты очень чувствительны к любым внешним воздействиям и должны работать в температуре, близкой к абсолютному нулю (-273°C);
- Квантовой декогеренции — потеря информации во время взаимодействия частиц друг с другом. Ученым еще не удается «поймать» все ошибки и сделать устройство идеальным, но они работают с алгоритмами коррекции.

Несмотря на все сложности, мировое научное сообщество считает, что квантовые вычисления могут кардинально изменить подход к обработке данных в ряде сфер.

Биокомпьютеры

Представьте себе, что компьютер будет «живым»? И это совсем не шутки! Компьютеры могут использовать биологические компоненты для своей работы. Только один ДНК человека содержит 1,6 гигабайта информации, если переводить данные в наши любимые компьютерные термины. А 1 грамм ДНК может хранить до 215 петабайт данных!

В одном петабайте 1 миллион гигабайт. Представили себе? Всё, что ученые смогли создать за этот и прошлый век, по факту ничто с тем, что сотворила с нами Вселенная.

Технологию можно назвать пока экспериментальной — существуют биохимические системы на основе ДНК, которые выполняют простые логические операции, но они пока не являются полноценными компьютерами. Также существуют технологии редактирования ДНК (например, CRISPR), но это уже область генной инженерии, а не вычислений.

Кстати, это уже не фантастика: компания Cortical Labs недавно представила CL1 — первый в мире биокомпьютер, объединяющий живые нейроны с обычными чипами. Такой гибрид способен обучаться быстрее классических машин и может использоваться, например, в разработке лекарств. И это только начало.

Если ученые доведут эти технологии до стабильной работы, то это откроет путь к нанороботам, которые будут внедряться в живой организм и «лечить» все болезни, обновлять клетки и увеличивать жизнь организма. Также биокомпьютеры будущего будут

взаимодействовать с человеческим организмом, что позволит победить многие болезни и недуги.

Оптические компьютеры

Несмотря на фантастический технический прогресс в создании чипов, данные технологии будут медленнее, чем скорость света. На сегодняшний день нет способа передать информацию быстрее (согласно Эйнштейну), чем скорость света (300 000 км/с).

Пройдет время, и компьютеры могут быть созданы по оптической технологии — где вместо электричества сигнал будет передаваться с помощью света. Пока что такие технологии очень громоздкие — классическая электроника здесь выигрывает. Но если все-таки создадут полноценный оптический компьютер, то его скорость работы будет в разы быстрее. Также такой компьютер не будет потреблять большого количества энергии.

Оптические технологии уже применяются, в частности в оптоволоконных кабелях для передачи данных на большие расстояния — их пропускная способность и скорость выше, чем у классических медных кабелей.

2 ЦИФРОВОЙ СЛЕД

2.1 Что такое цифровой след?

Цифровой след — это совокупность данных, которые пользователь оставляет в интернете: история посещённых сайтов и поисковые запросы, сообщения в мессенджерах, посты и лайки в соцсетях, геолокация, данные транзакций и файлы в облаке. Полностью стереть цифровой след практически невозможно: интернет всё помнит.

Влияние цифрового следа на жизнь может быть как положительным, так и отрицательным.

Положительные стороны:

- персонализация сервисов — на основе пользовательской информации компании могут предлагать более релевантные товары, фильмы, музыку;
- упрощение взаимодействия с технологиями — сохранённые пароли, автоматическое заполнение форм и персонализированные рекомендации экономят время;
- анализ и саморазвитие — цифровые данные помогают отслеживать прогресс в разных областях: от физической активности до профессиональных навыков.

Отрицательные стороны:

- утечка личных данных — массивы информации, содержащие персональные данные, регулярно становятся целью кибератак;
- репутационные проблемы — любой пост, комментарий или фотография могут быть сохранены и использованы против их автора;
- манипуляция поведением через алгоритмы — алгоритмы соцсетей и новостных агрегаторов, анализирующие следы, формируют «информационные пузыри», показывая только то, что соответствует предполагаемым взглядам и интересам, отфильтровывая альтернативные точки зрения.

2.2 Типы цифрового следа

1. Активный — данные, которые пользователь сознательно оставляет в интернете:

- публикации и комментарии в социальных сетях;
- загруженные фото и видео;
- заполненные анкеты и регистрационные формы;
- электронные письма и сообщения в мессенджерах;
- отзывы о товарах или услугах.

2. Пассивный — информация, которая собирается автоматически, часто без ведома пользователя:

- публикации и комментарии в социальных сетях;
- загруженные фото и видео;
- заполненные анкеты и регистрационные формы;
- электронные письма и сообщения в мессенджерах.

2.3 Что собирает цифровой след?

Цифровые следы собирают:

- **Крупные корпорации и поисковые системы** (Яндекс, Google и др.) — для персонализации рекламы, поиска и рекомендаций.
- **Социальные сети и платформы** — чтобы подбирать релевантный контент и таргетированную рекламу.
- **Рекламодатели и маркетологи** — для анализа поведения пользователей и повышения эффективности рекламных кампаний.
- **Интернет-провайдеры** — фиксируют историю посещений и активности.
- **Владельцы продуктов и сервисов** — для улучшения пользовательского опыта и оптимизации продуктов.
- **Потенциальные работодатели** — проверяют цифровые следы кандидатов, чтобы оценить их репутацию и соответствие ценностям компании. practicum.yandex.ru +1
- **Государственные органы** — для обеспечения безопасности, расследования преступлений, сбора налогов и социального мониторинга.
- **Хакеры и киберпреступники** — используют данные для кражи личности, мошенничества, шантажа.

2.4 Угрозы

С развитием технологий цифровой след становится все более сложным и всеобъемлющим. Новые тренды открывают как возможности, так и риски для пользователей интернета:

1. **Искусственный интеллект и анализ данных.** Искусственный интеллект играет ключевую роль в обработке больших данных. Алгоритмы способны анализировать миллиарды единиц информации, чтобы предсказать поведение пользователей, их предпочтения и даже психологические особенности;
2. **Развитие "интернета вещей".** Количество подключенных устройств растет: от "умных" холодильников до автомобилей. Каждый из них собирает данные о владельце, создавая еще более детализированный цифровой след;
3. **Блокчейн и децентрализация данных.** Технологии блокчейна — цепочки блоков данных, защищенных с помощью криптографии, с информацией о транзакциях —

обещают дать пользователям больший контроль над своими данными. Информация благодаря им хранится децентрализованно, что затрудняет ее сбор третьими лицами;

4. **Обезличивание данных.** Хотя компании утверждают, что используют данные в обезличенном виде, современные методы анализа позволяют сопоставлять разрозненные фрагменты информации и идентифицировать человека;

5. **Развитие законодательства.** Такие инициативы, как GDPR (General Data Protection Regulation) в ЕС или закон "О персональных данных" в России, направлены на защиту данных пользователей. Однако на глобальном уровне законы все еще остаются разрозненными;

6. **Этические вопросы.** Кто должен нести ответственность за защиту цифрового следа: пользователи, компании или правительства? Этот вопрос становится все более актуальным с увеличением объемов данных.

Российское законодательство о цифровом следе

В России защита персональных данных регулируется Федеральным законом №152-ФЗ "О персональных данных". Этот закон определяет, как компании и государственные структуры должны собирать, хранить, обрабатывать и передавать данные граждан. Основные положения закона включают:

- обязательное согласие пользователя на обработку данных;
- возможность отозвать это согласие в любое время;
- защиту данных от несанкционированного доступа.

За соблюдение этого закона отвечает Роскомнадзор. Он проводит проверки и имеет право блокировать ресурсы, нарушающие требования, в соответствии со статьей 15.5. Федерального закона "Об информации, информационных технологиях и о защите информации".

Однако специфика цифрового мира такова, что все эти меры в полном объеме не защищают от утечек данных, в том числе и крупных, как в нашей стране, так и во всем мире.

Некоторые меры по защите цифрового следа в России

Одним из современных проектов в России, влияющих на формирование цифрового следа, является "Цифровой профиль гражданина". Эта инициатива предполагает централизованное хранение информации о гражданах, включающей данные из различных государственных структур: налоговой службы, Пенсионного фонда, ЗАГСа и других. Чтобы использовать эти данные, коммерческая компания должна будет получить согласие самого гражданина и указать цели такого использования.

Концепция суверенного интернета, реализуемая в рамках российского законодательства, также направлена на создание независимой инфраструктуры для работы интернета внутри страны. Это повышает безопасность данных, снижая зависимость от зарубежных серверов.

Россия активно участвует в обсуждении вопросов кибербезопасности на международных площадках. Однако различия в подходах к защите данных между странами пока затрудняют создание глобальных стандартов.

2.5 Перспективы и вызовы в сфере защиты цифрового следа

Краткий обзор отчётов и аналитики по безопасности данных от компаний Kaspersky, Group-IB и Positive Technologies за 2025 год

Positive Technologies

- В 2025 году компания показала значительный рост объёма отгрузок — до 35 млрд рублей, что вдвое превышает динамику рынка кибербезопасности в России. Объём инвестиций в *R&D* составил около 9 млрд рублей. Компания отмечает рост числа кибератак и изменение их структуры, что влияет на развитие новых продуктов и услуг по защите информации

Kaspersky

- Глобальная выручка компании в 2025 году достигла 836 млн долларов США (+4% за год). Продажи решений для бизнеса (*B2B*) выросли на 16%, причём для крупных предприятий — на 21%, для малого и среднего бизнеса — на 7%. В России и СНГ корпоративные продажи увеличились на 24%. Особенно быстро растут новые решения для защиты от сложных киберугроз (+30%). В среднем ежедневно обнаруживается до 500 000 вредоносных файлов. Компания активно развивает продукты на базе искусственного интеллекта и расширяет линейку решений для промышленных и корпоративных клиентов

В России действует множество организаций, специализирующихся на защите от киберугроз. Они разрабатывают программное обеспечение, внедряют комплексные системы безопасности, проводят аудит, обучение и реагирование на инциденты.

Таблица 1 - Крупнейшие российские компании по кибербезопасности

Компания	**Основные направления деятельности**	**Ключевые продукты и услуги**
Лаборатория Касперского	Антивирусы, комплексная защита предприятий, *Threat Intelligence*,	*Kaspersky Endpoint Security, Kaspersky Industrial*

	защита критической инфраструктуры	*CyberSecurity, Kaspersky Symphony XDR*
Positive Technologies	Анализ защищённости, мониторинг и реагирование на инциденты, защита критической инфраструктуры	*MaxPatrol, PT Application Firewall, PT Container Security*
InfoWatch	Защита от утечек данных (*DLP*), мониторинг действий сотрудников, поведенческий анализ	*InfoWatch Traffic Monitor, ARMA NGFW*
Solar (ГК «Ростелеком»)	Защита от утечек, управление доступом, межсетевые экраны, киберучения	*Solar Dozor, Solar inRights, Solar NGFW,* Национальный киберполигон
UserGate	Межсетевые экраны нового поколения (*NGFW*), анализ событий ИБ, защита электронной почты	*UserGate NGFW, UserGate SIEM*
Код Безопасности	Средства защиты информации для госорганов и бизнеса, криптография, защита виртуализации	*vGate, Континент WAF, Континент NGFW*
Гарда (ГК «ИКС Холдинг»)	Защита баз данных, анализ трафика, предотвращение утечек, защита от *DDoS*	*Гарда DBF, Гарда Маскирование, Гарда AntiDDoS*
BI.ZONE	Управление киберрисками, реагирование на инциденты, обучение сотрудников	*BI.ZONE Security Fitness,* услуги по аудиту и пентестам

Avanpost	Управление доступом и идентификацией, многофакторная аутентификация	*Avanpost IDM, Avanpost MFA+, Avanpost Unified SSO*
Инфотекс (ViPNet)	Криптографич. защита каналов связи, межсетевые экраны, защита промышленных сетей	*ViPNet,* средства защиты конечных точек

Ключевые тенденции и направления развития:

- **Рост числа атак через подрядчиков и цепочки поставок** — компании внедряют сервисы проверки защищённости подрядчиков.
- **Искусственный интеллект в атаках и защите** — автоматизация выявления угроз, поведенческий анализ, защита ИИ-систем.
- **Импортозамещение** — переход на отечественные решения для защиты критической инфраструктуры.
- **Развитие сервисов киберстрахования и аутсорсинга ИБ** — компании всё чаще заказывают услуги мониторинга и реагирования (*SOC*).
- **Ужесточение требований регуляторов** — новые стандарты ФСТЭК России, обязательное реагирование на инциденты, аудит подрядчиков (ПРИЛОЖЕНИЕ Н).

2.6 Цифровая грамотность для граждан - основа защиты

С ростом количества данных, которыми мы обмениваемся в интернете, возрастает необходимость цифровой осознанности. Большинство пользователей недостаточно осведомлены о рисках, связанных с их цифровым следом в интернете, и не принимают элементарных мер предосторожности.

Подростки публикуют личную информацию в социальных сетях, не понимая, что это может быть использовано против них. В России существуют образовательные инициативы, среди которых уроки цифровой грамотности в школах. Однако их пока недостаточно.

Важно понимать, что защиту цифрового следа нельзя возложить только на государство или компании. Каждый пользователь должен осознавать последствия своих действий в Сети и быть готовым к ответственности за опубликованную информацию.

Цифровые следы — это неизбежная часть жизни в эпоху интернета. Не оставить сегодня цифрового следа пользователя в Сети невозможно. Он влияет на репутацию, безопасность и свободу действий. Осознанный подход к защите цифрового следа в

интернете, использование человеком современных инструментов и понимание принципов работы данных помогут сохранить баланс между удобством технологий и защитой личной информации.

II ПРАКТИЧЕСКАЯ ЧАСТЬ

3.1 Анкетирование и анализ цифрового следа

Цель: выяснить, насколько современные пользователи осведомлены о своём цифровом следе и его последствиях.

Методика: Проведено анкетирование среди учащихся и преподавателей (общее число участников — 112 человек). В анкете были вопросы:

1. Ваш возраст:

- до 14 лет;
- 14–18 лет;
- 19–25 лет;
- 26–35 лет;
- старше 35 лет.

2. Пользуетесь ли вы интернетом ежедневно?

- Да;
- Нет.

3. Какие устройства вы используете для выхода в интернет?

- Смартфон;
- Компьютер/ноутбук;
- Планшет;
- Другое (укажите).

4. Знаете ли вы, что такое «цифровой след»?

- Да, хорошо знаю;
- Слышал(а), но не уверен(а);
- Нет, не знаю.

5. Используете ли вы сложные пароли (более 8 символов, с цифрами и знаками)?

- Всегда;
- Иногда;
- Нет, использую простые.

6. Как часто вы меняете пароли от важных аккаунтов (почта, соцсети, банковские сервисы)?

- Раз в месяц;
- Раз в полгода;
- Раз в год;

- Никогда не меняю.

7. Используете ли вы двухфакторную аутентификацию (подтверждение входа по SMS или в приложении)?

- Да, везде, где возможно;
- Только для важных сервисов;
- Нет, не использую.

8. Публикуете ли вы в интернете личную информацию (адрес, телефон, номер школы/работы)?

- Да, часто;
- Иногда;
- Никогда.

9. Сталкивались ли вы с попытками мошенничества в интернете (фишинг, подозрительные письма, звонки)?

- Да, неоднократно;
- Один раз;
- Нет.

10. Знаете ли вы, как защитить свои данные при использовании публичных Wi-Fi сетей?

- Да, знаю и использую VPN/другие способы;
- Слышал(а), но не применяю;
- Нет, не знаю.

11. Что, по-вашему, самое важное для защиты персональных данных? (выберите не более 3 вариантов)

- Сложные пароли;
- Двухфакторная аутентификация;
- Антивирус;
- Осторожность при публикации информации;
- Регулярное обновление программ;
- Другое (укажите).

12. Хотели бы вы узнать больше о защите данных и цифровом следе?

- Да;
- Нет;
- Уже достаточно знаю.

Результаты:

- 56% респондентов знают о понятии «цифровой след», но только 30% регулярно проверяют настройки приватности.
- 40% участников признались, что хотя бы раз сталкивались с неприятностями из-за информации, размещённой в сети (например, утечка личных фото, спам, мошенничество).
- 60% не задумываются о том, что их старые публикации могут повлиять на будущее (например, при приёме на работу).

Вывод: большинство пользователей недооценивают риски, связанные с цифровым следом, и не принимают достаточных мер для защиты своих данных.

Эксперимент: анализ цифрового следа

Цель: продемонстрировать, какую информацию о человеке можно найти в открытых источниках.

Ход эксперимента:

1. Выбраны 3 добровольца (с их согласия).
2. Поиск информации проводился только по открытым данным: социальные сети, форумы, блоги, публичные базы данных.
3. Фиксировались все найденные сведения: ФИО, город проживания, учебные заведения, места работы, интересы, фотографии.

Результаты:

- За 15 минут удалось собрать достаточно подробный «портрет» каждого добровольца.
- Были найдены старые фотографии, публикации с личной информацией, комментарии, которые участники считали удалёнными.
- В одном случае обнаружена информация о месте работы и даже домашний адрес.

Вывод: цифровой след формируется не только осознанно (публикации), но и неосознанно (лайки, комментарии, метаданные фото). Удаление информации с одной платформы не гарантирует её полного исчезновения из интернета.

3.2 Рекомендации по минимизации влияния цифрового следа

Цифровой след — это совокупность всех данных, которые пользователь оставляет в интернете: публикации, комментарии, лайки, история поиска, метаданные фотографий и др. Чтобы снизить риски, рекомендуется придерживаться следующих правил.

1. Контроль личной информации

- **Не публикуйте** в открытом доступе личные данные: адрес, номер телефона, паспортные данные, место работы или учёбы.
- **Ограничьте** круг лиц, которые могут видеть ваши публикации, с помощью настроек приватности в социальных сетях.

- **Избегайте** размещения фотографий документов, билетов, ключей и других предметов, по которым можно получить доступ к вашим аккаунтам или имуществу.

2. Управление контентом

- **Регулярно проверяйте** свои старые публикации и удаляйте те, которые могут быть использованы против вас (например, провокационные фото, резкие высказывания).
- **Не делитесь** информацией о своих планах на отпуск или длительном отсутствии дома — это может привлечь злоумышленников.
- **Будьте внимательны** к комментариям и лайкам: даже удалённые записи могут сохраняться в кэше поисковых систем или на сторонних ресурсах.

3. Безопасность аккаунтов

- **Используйте сложные и уникальные пароли** для каждого сервиса. Не храните пароли в заметках или в виде текстовых файлов на компьютере.
- **Включите двухфакторную аутентификацию** везде, где это возможно.
- **Проверяйте**, какие сторонние приложения имеют доступ к вашим аккаунтам (например, через «Вход с помощью Google/Facebook»), и отзывайте разрешения у ненужных сервисов.

4. Работа с устройствами и приложениями

- **Отключайте геолокацию** в приложениях, если она не требуется для работы (например, в соцсетях, фоторедакторах).
- **Проверяйте разрешения** приложений: не давайте доступ к контактам, микрофону, камере без необходимости.
- **Используйте VPN** при подключении к общественным Wi-Fi сетям для защиты передаваемых данных.

5. Цифровая грамотность и критическое мышление

- **Не переходите** по подозрительным ссылкам и не скачивайте файлы из непроверенных источников.
- **Будьте осторожны** с фейковыми новостями и мошенническими сайтами: проверяйте информацию перед тем, как делиться ею.
- **Объясняйте детям и подросткам** основы безопасного поведения в интернете, так как они часто не осознают последствия своих действий.

6. Регулярный мониторинг

- **Периодически «гуглите» себя**: это поможет узнать, какая информация о вас доступна в интернете.

ВЫВОД

Минимизация цифрового следа — это не разовое действие, а постоянный процесс. Осознанное отношение к своим действиям в интернете, регулярный аудит личной информации и соблюдение правил цифровой гигиены позволяют значительно снизить риски для репутации и безопасности.

В ходе исследовательской работы была рассмотрена история развития вычислительной техники — от первых механических арифмометров до современных смартфонов, ставших неотъемлемой частью жизни каждого человека. Анализ показал, что стремительное развитие технологий не только расширило возможности общения и получения информации, но и привело к формированию нового явления — **цифрового следа**.

Проведённое анкетирование и практический эксперимент подтвердили, что большинство пользователей не в полной мере осознают, какой объём личной информации становится доступным в интернете и как это может повлиять на их жизнь. Было установлено, что цифровой след формируется не только осознанно (публикации, комментарии), но и неосознанно (метаданные, история поиска, лайки), а его последствия могут проявляться в виде угроз безопасности, репутационных рисков и даже ограничений при трудоустройстве.

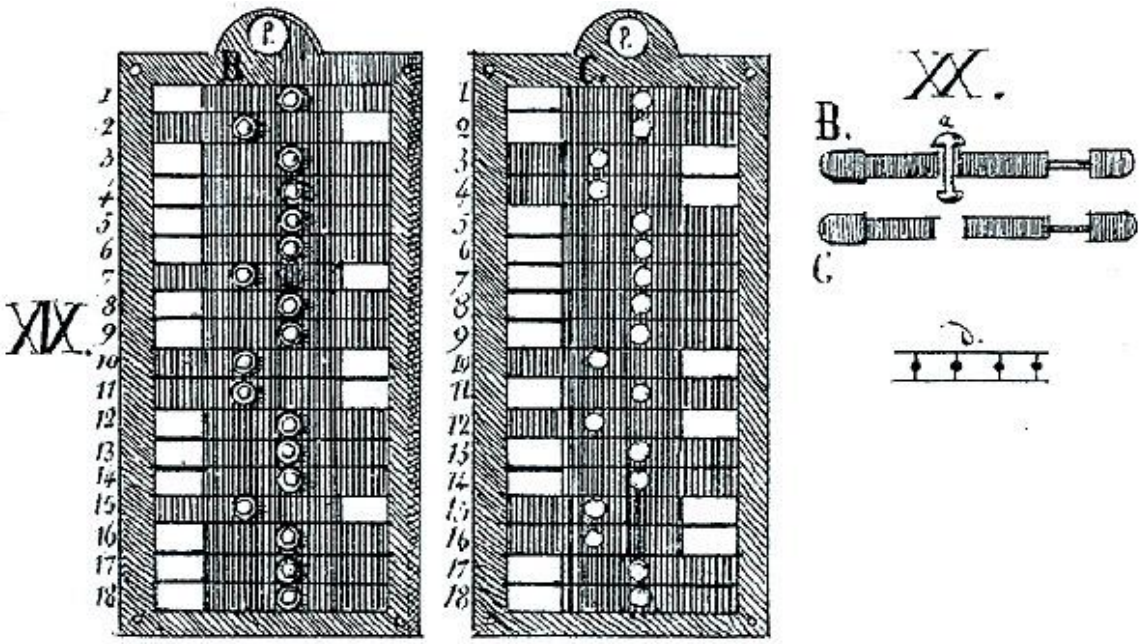
Главный вывод работы: современный человек должен не только владеть цифровыми технологиями, но и обладать высоким уровнем цифровой грамотности. Осознанное отношение к своим действиям в сети, регулярный контроль публикуемой информации и соблюдение рекомендаций по защите личных данных позволяют минимизировать негативное влияние цифрового следа и использовать возможности интернета максимально безопасно и эффективно.

ЛИТЕРАТУРА

1. Кордемский Б.А., Ахадов А.А.
   Удивительный мир чисел: (Матем.головоломки и задачи для любознательных): Кн. Для учащихся. – М.: Просвещение 1986. – 144с.: ил.
2. Арисава Макото
   Что такое компьютер / Пер. с яп. М.А.Терешина. – К.6 Выща шк. Головноеизд-во, 1988. – 168 с.: 23 ил., 5 табл.
3. Звенигородский Г.А.
   Первые уроки программирования/ Под ред. А.П.Ершова. – М.: Наука. Главная редакция физико – математической литературы, 1985. – 208 с. – (Библиотечка «Квант», Вып. 41.) – 30 к.
4. Касаткин В.Н.
   Введение в кибернетику: Пособие для факультатив. занятий в 9 кл. – 3-е изд., перераб. и доп. – К.: Рад.шк., 1986. – 176 с.
5. https://tass.ru/obschestvo/24390587
6. https://issek.hse.ru/news/450602433.html
7. https://ptsecurity.com/research/knowledge-base/from-vulnerability-to-resilience/#id8
8. https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Threat-and-Information-Security-Forecast-2026
9. https://www.kp.ru/money/uslugi-rossiya/luchshie-kompanii-po-kiberbezopasnosti-v-rossii/
10. https://www.kaspersky.com/about/press-releases/kaspersky-reports-2025-financial-results-driving-revenue-to-836-mln
11. https://1prime.ru/20260330/vyruchka-868766098.html
12. https://invest-era.ru/analytics-and-news/positive-technologies-khakerskie-ataki-kardinalno-menyayut-perspektivi
13. https://tass.ru/novostnye-razdely/22574131
14. https://trends.rbc.ru/trends/industry/650408f49a79475d78ba7a9e
15. https://dzen.ru/a/Z-Ks_EgTQWrVvy8q?utm_referrer=yandex.ru

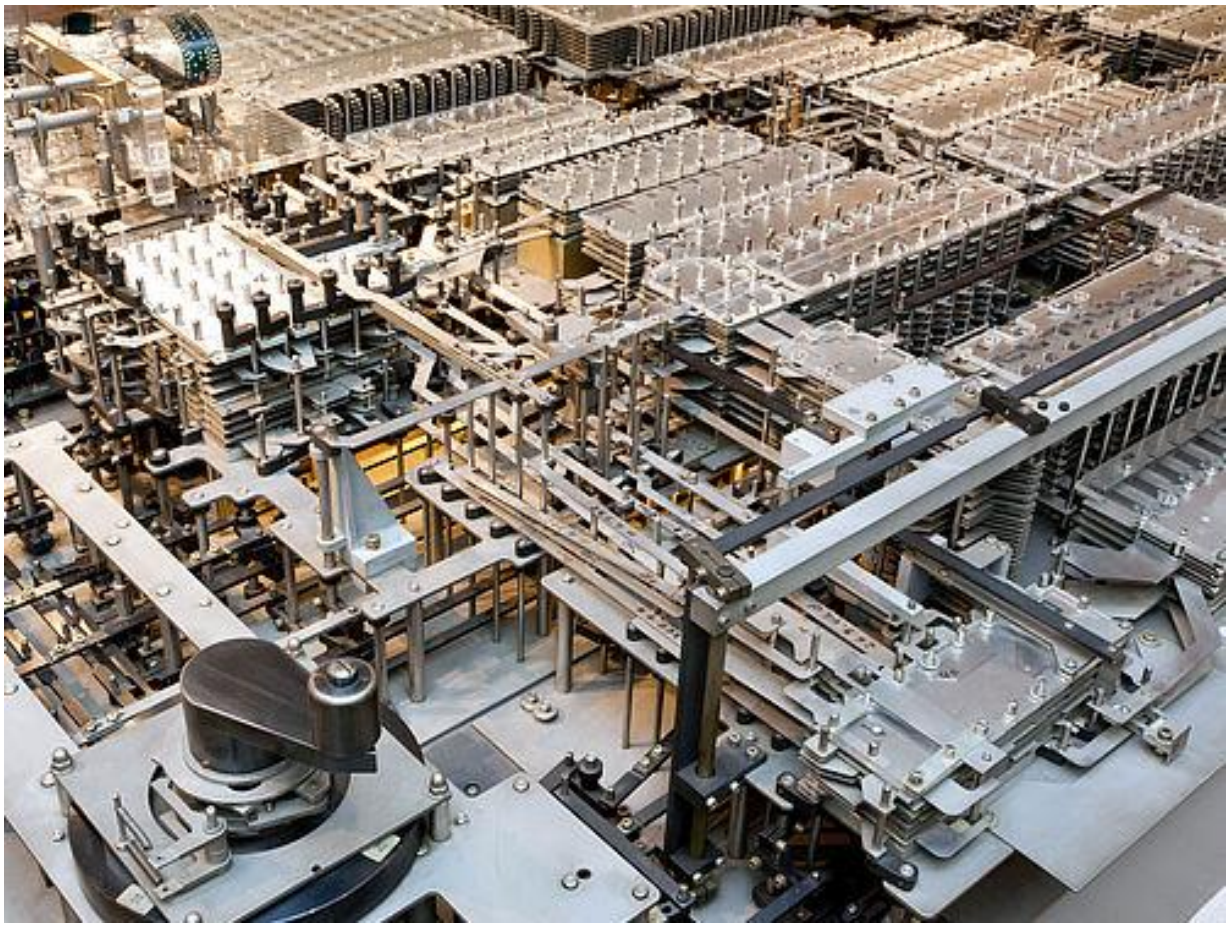
ПРИЛОЖЕНИЕ А

Рисунок 1 - Простой компаратор



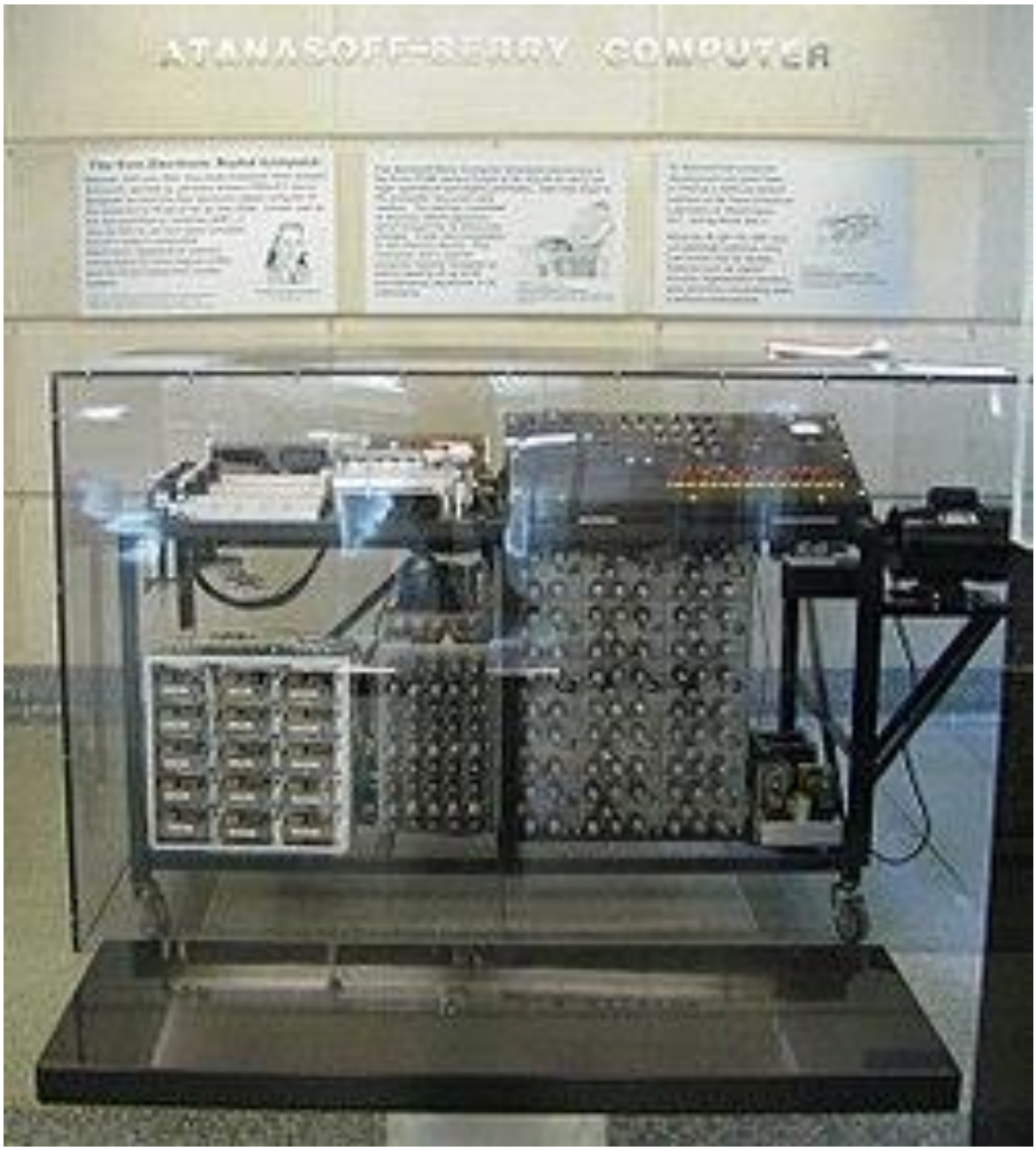
ПРИЛОЖЕНИЕ В

Рисунок 2 - Фото вычислительной машины Z4



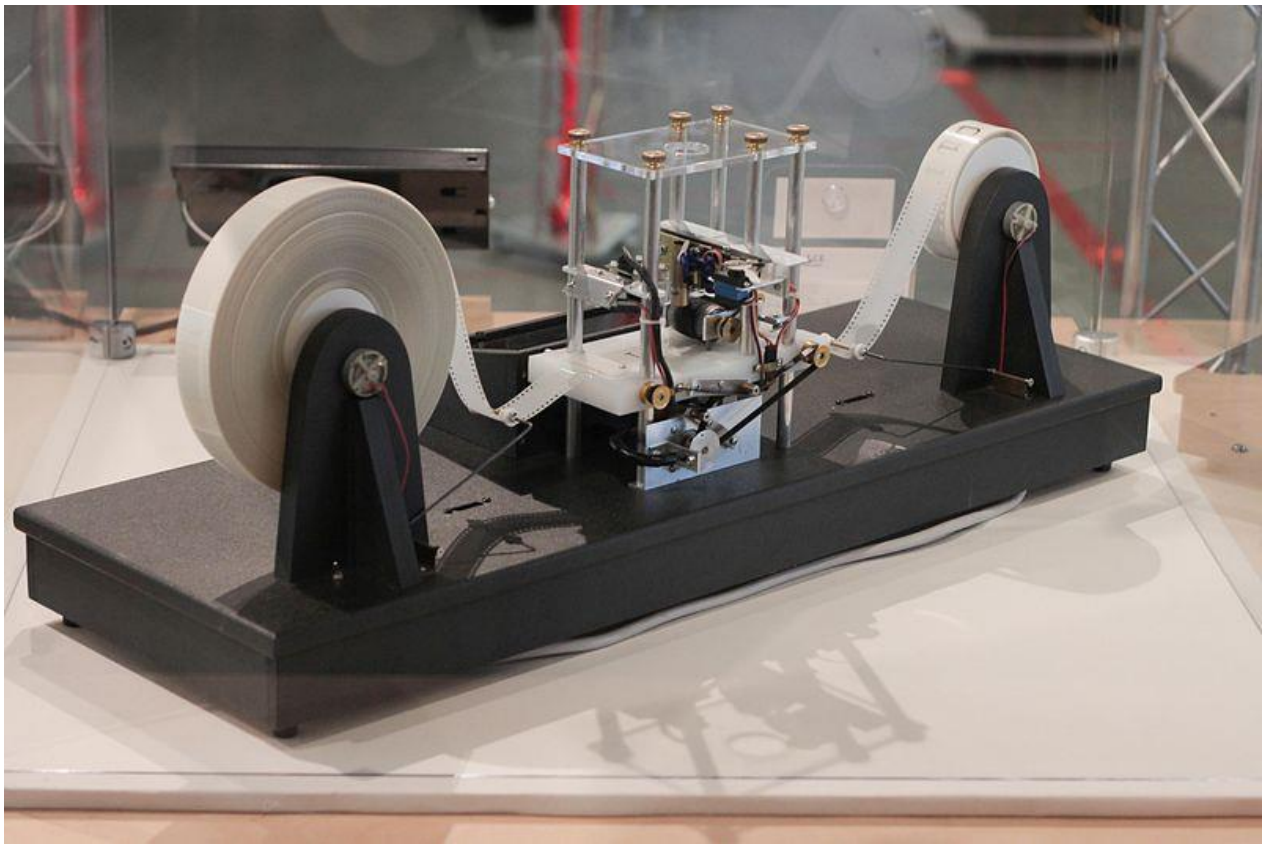
ПРИЛОЖЕНИЕ С

Рисунок 3 - Копия компьютера Атанасова — Берри



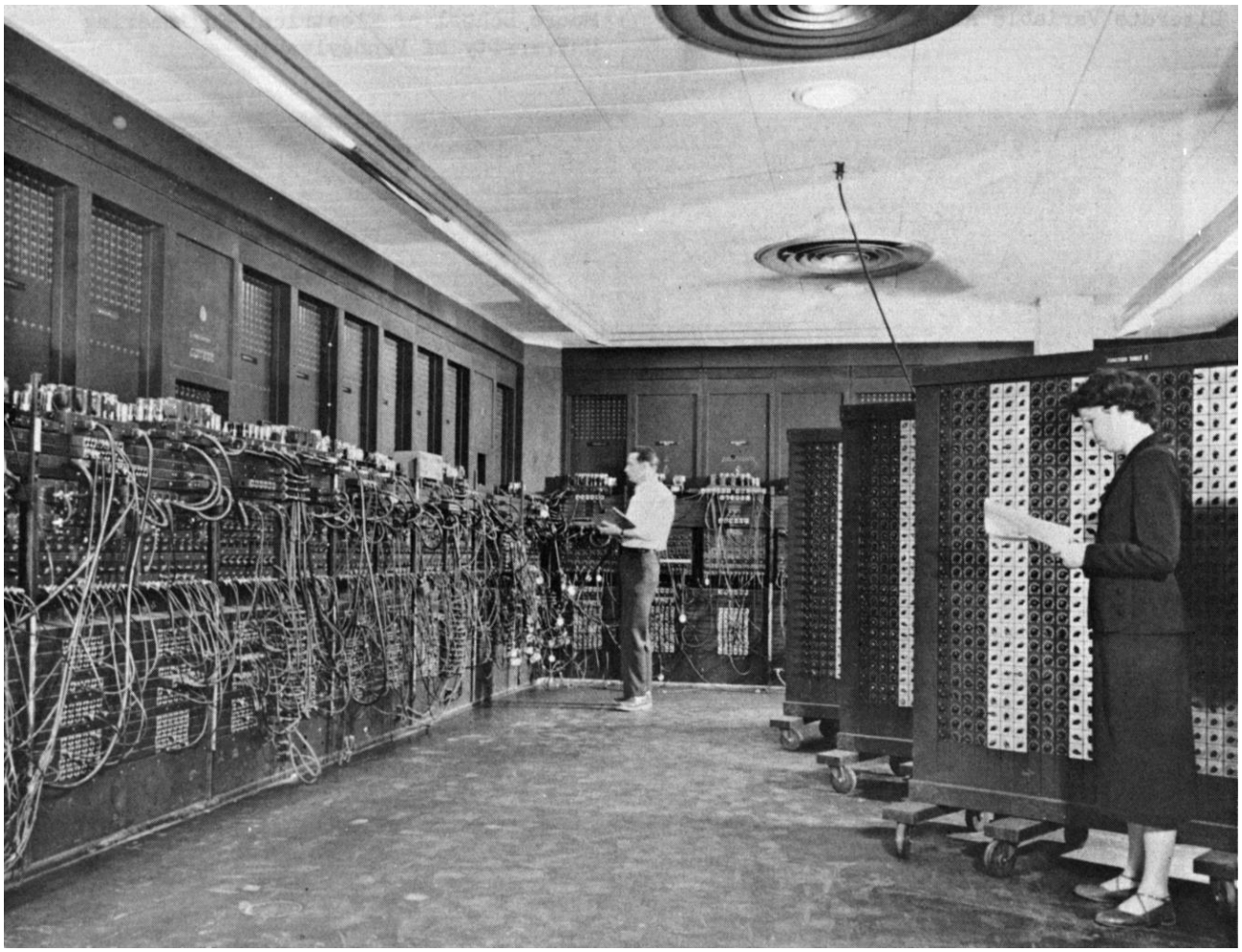
ПРИЛОЖЕНИЕ D

Рисунок 4 - Модель машины Тьюринга



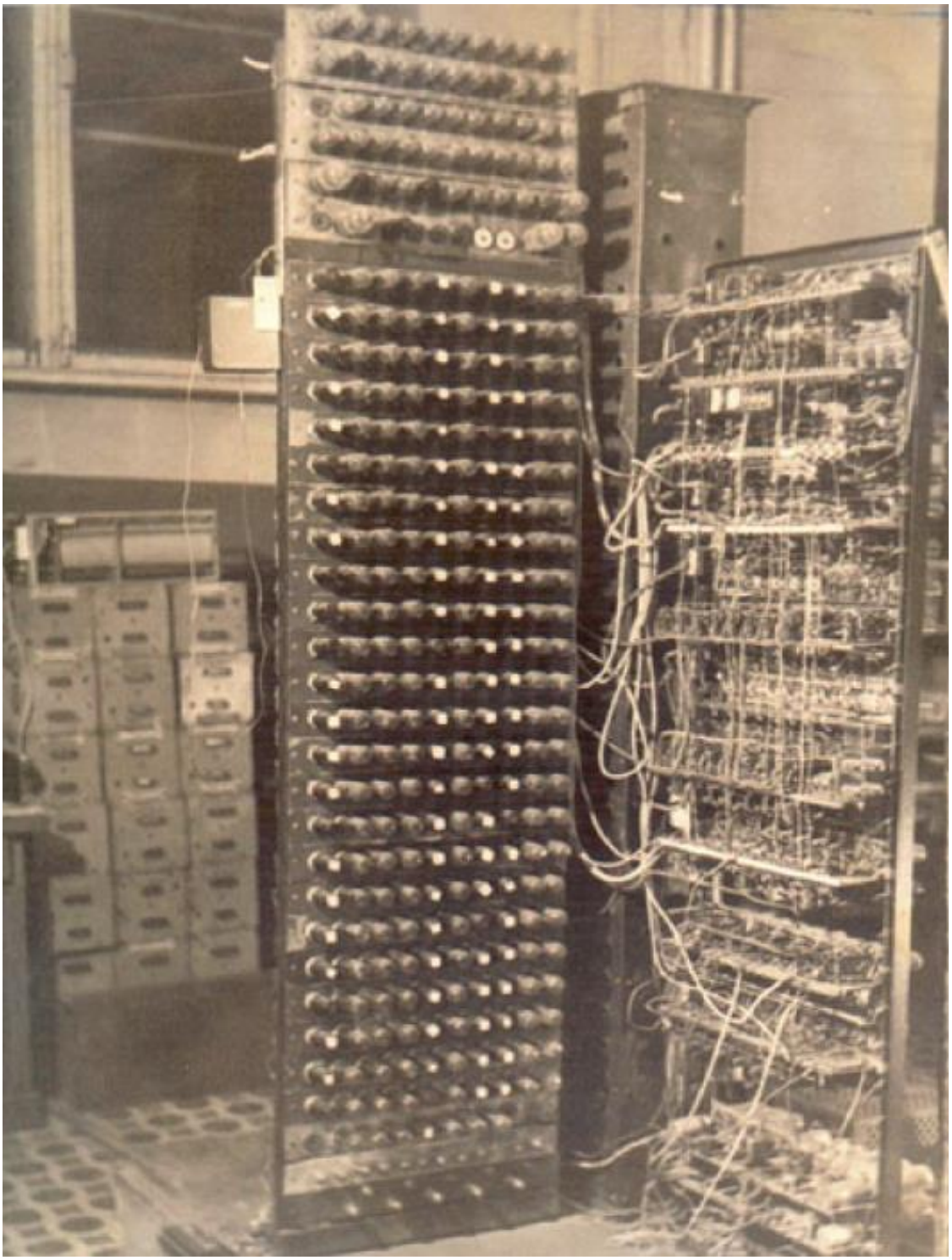
ПРИЛОЖЕНИЕ Е

Рисунок 5 – Первая в мире ЭВМ — ENIAC



ПРИЛОЖЕНИЕ F

Рисунок 6 - Фото АЦВМ М-1



ПРИЛОЖЕНИЕ G

Рисунок 7 - Один из трех первых ПЭВМ «Агат-7»

ПРИЛОЖЕНИЕ Н

Рисунок 8. Основные темы прогнозов на 2026 год: развитие киберугроз

Рисунок 9. Основные темы прогнозов на 2026 год: развитие средств защиты информации