DOI 10.36622/1682-7813.2025.28.2.002
УДК 004.056

СПОСОБ ФОРМИРОВАНИЯ ЭЛЕКТРОННЫХ ДИСЦИПЛИН В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВИЗУАЛИЗИРОВАННОЕ ИНТЕРАКТИВНОЕ ПРЕДСТАВЛЕНИЕ УЧЕБНОГО МАТЕРИАЛА С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

А.Г. Остапенко, Е.А. Москалева, А.Г. Краснобородкин, Д.А. Катюрин, Н.И. Баранников, М.А. Грамыкин

Научная статья посвящена совершенствованию учебного процесса в области информационной безопасности за счёт разработки курса видеолекций, где в роли оратора выступает нейросетевой аватар. Определен и реализован концепт курса видеолекций с учетом инновационных технологий обучения. На основе психологии восприятия информации разработан нейросетевой помощник, а также создан ресурс доступа с возможностью просмотра цикла клипов, прохождения тестирования по соответствующей тематике и решения задач в игровом формате.

Ключевые слова: информационная безопасность, нейросетевой аватар, нейросети, учебный процесс, клиповое мышление.

Введение

В последние десятилетия человечество переживает беспрецедентный информационный бум. Ежедневное потребление информации увеличилось в тысячи раз, причём её формат также претерпел расширение – это и текстовая информация, и изображения, видео, а также смешанные формы. Рост объема данных (170 зеттабайт к 2025 году [1]) увеличивает уязвимость пользователей к социальной инженерии, что делает людей легкой мишенью для фишинга, мошенничества и других атак.

Такого рода феномен стал полной неожиданностью для неподготовленного к этому человеческого мозга. С началом эпохи цифровизации начинают появляться новые недуги, связанные с огромным объёмом знаний, включая синдром информационной усталости и переутомление мозга, вызванное растущим потоком данных. Эти явления не только снижают продуктивность, но и создают критические уязвимости в сфере информационной безопасности. Следствием системной перегрузки становятся поверхностное восприятие информации, снижение внимательности, эмоциональное выгорание и другие факторы, которые делают пользователей уязвимыми к атакам социальной инженерии, включая фишинг и компрометацию деловой почты.

В результате, влияние множества факторов – цифровизация информации, увеличение её объёма, изменение шаблонов потребления информации, переполненная информационная среда и присутствие большого количества спама, – привело к выделению обособленного типа восприятия данных – «клиповое мышление» [2,3]. Эта тенденция особенно остро проявляется у поколений Z и Альфа, выросших в условиях цифровой среды, где снижение способности к критическому осмыслению контента создаёт серьезные угрозы обеспечению социальной и кибербезопасности, где уровень требований стремительно растёт в ходе технологической гонки вооружений (ежегодно кратно увеличивается количество и качество кибератак).

Целью данной работы является повышение качества учебного процесса в области кибербезопасности за счёт создания и внедрения методического обеспечения, основанного на интерактивном представлении учебного материала с использованием нейросетевых технологий.

В результате исследования работ [2,3] в области клипового мышления, а также методов обучения в высших учебных заведениях, были выявлены следующие противоречия между:

- эскалацией информационного противоборства и стремительным ростом арсеналов кибервооружений, порождающих ежегодно кратно возрастающий объём

профессиональных знаний в области информационной безопасности (ИБ), и ограниченностью их восприятия современной молодёжью на фоне понижающегося уровня её базовой подготовки, что значительно повышает риски успешности атак класса «социальная инженерия»;

- содержанием учебного процесса в высших учебных заведениях по группе специальностей «Информационная безопасность» и существующими тенденциями молодёжи к потреблению ярких картинок и запоминающихся образов;

- необходимостью увеличения количества и качества осваиваемых студентами знаний и традиционными подходами современных образовательных программ по специальностям ИБ-профиля;

- стремлением качественно и доступно преподносить материал и методами его разработки, которые не включают участие самих студентов в формировании его представления и доработке визуальной составляющей, которая зачастую вообще отсутствует.

В связи с этим, были определены следующие **задачи**:

- определить набор уязвимостей человеческого восприятия, характерный для современного поколения молодежи, с выделением наиболее критичных из них в части социальной инженерии;

- создать информационное обеспечение с целью формирования видеоматериала дисциплины «Введение в специальность» для специалистов по защите информации;

- разработать модель нейросетевого аватара и представляемого им видеоматериала на основе современных потребностей образовательного процесса по группе специальностей «Информационная безопасность»;

- разработать платформу, позволяющую осуществлять дистанционный доступ к циклу и дополнить её разделом тестирования с элементами геймификации.

Актуальность проблемы «клиповости» мышления среди современного поколения

Исследователи выделяет следующие особенности индивида – представителя молодого поколения, попадающего под определение феномена «клиповое» мышление [4]:

- отсутствие аналитических способностей, неумение выделять ключевую информацию и устанавливать причинно-следственные связи. Это приводит к несистемному запоминанию информации и неумению правильно её интерпретировать и использовать;

- доминация кратковременной памяти, ввиду чего услышанная и увиденная информация стирается за считанные дни. Это связано с неопровержимым фактом – запоминание происходит благодаря построению логических связей в мозге, что у адептов клиповой культуры практически не происходит. Студенту, который способен системно запоминать информацию, не составит труда воспроизвести её через долгое время благодаря определённым «триггерам», например, практическому опыту;

- фрагментарность мышления не позволяет запоминать информацию в большом объёме, что не позволяет в достаточной мере овладеть материалом. Это приводит к потере интереса во время обучения, а также к быстрой утомляемости и неусидчивости.

Говоря о способе восприятия человеком информации, нельзя не упомянуть, что множество компьютерных атак с последующим нелегальным завладением личной или корпоративной информацией происходит именно посредством использования несовершенства человеческой природы. Такой класс атак получил название «социальная инженерия», и направлен на использование слабостей личности в целях обмана, шантажа, кражи.

С ростом доступного объёма информации, увеличивающегося экспоненциально [1], когнитивные возможности человека сталкиваются с новыми вызовами. Перманентное взаимодействие с цифровыми технологиями, начиная с раннего возраста, приводит к трансформации восприятия данных и формированию системных уязвимостей. Например, снижение внимательности у пользователей, ежедневно обрабатывающих огромные массивы информации, повышает риск пропуска критических деталей в запросах или случайного клика по вредоносной ссылке в фишинговых письмах. Ещё одной распространённой уязвимостью становится переоценка доверия к информации — автоматическое принятие сообщений от источников, выдающих себя за «администраторов» или «техподдержку», без

верификации подлинности. Эта тенденция усугубляется тем, что современные пользователи получают десятки уведомлений ежедневно, что снижает их способность критически оценивать каждое из них. Таким образом, человек, с самого рождения тесно контактирующий с цифровыми технологиями, приобрёл уникальный набор уязвимостей, представленный в табл. 1.

Таблица 1

Уязвимости человеческого восприятия

Группа	№	Уязвимости
Образование	Уяз.1	Низкий уровень знаний
	Уяз.2	Отсутствие критического склада ума
	Уяз.3	Сложность в определении посильных задач
	Уяз.4	Завышение собственного уровня компетентности
	Уяз.5	Фрагментарное мышление
	Уяз.6	Поверхностные, терминологические знания
	Уяз.7	Рассеянное внимание
	Уяз.8	Неумение принимать решения самостоятельно
	Уяз.9	Принятие невзвешенных решений
Воспитание	Уяз.10	Стремление встроиться в западный мейнстрим и получить преференции
	Уяз.11	Отсутствие авторитетов
	Уяз.12	Необоснованные амбиции
	Уяз.13	Цифровая зависимость
	Уяз.14	Социальная изоляция
	Уяз.15	Эмоциональная зависимость от соцсетей
	Уяз.16	Высокое доверие к технологиям
	Уяз.17	Эмоциональная связь с виртуальными персонажами
	Уяз.18	Развитие высокой самооценки
	Уяз.19	Аномальная психика и низкая культура
	Уяз.20	Несформированность личности и жизненных взглядов
	Уяз.21	Неокрепшая психика детей и юношей
	Уяз.22	Низкая терпимость к неудачам
	Уяз.23	Эмоциональная нестабильность
	Уяз.24	Острые переживания из-за недостатков внешности

С точки зрения обеспечения информационной безопасности социальная инженерия представляет собой метод эксплуатации психологических уязвимостей человека для получения несанкционированного доступа к данным, системам или ресурсам. Злоумышленники активно используют эмоциональные триггеры (страх, доверие, ощущение срочности) и ограничения когнитивных процессов, такие как невнимательность или склонность к автоматическим решениям. Это позволяет им манипулировать жертвами, вынуждая передавать конфиденциальные данные, скачивать вредоносное ПО или нарушать правила безопасности. Эффективность таких атак основана на том, что человеческий фактор часто становится самым слабым звеном в защите ИТ-инфраструктуры.

Ядром обработки информации в мозге являются четыре фундаментальные функции: восприятие, запоминание, принятие решений и выполнение действий. На этот процесс влияют два типа когнитивных факторов — долгосрочные и краткосрочные. Долгосрочные формируют устойчивые паттерны поведения и восприятия. Краткосрочные факторы, включая когнитивную нагрузку, стресс и снижение внимания, временно нарушают баланс между аналитическим мышлением и импульсивной реакцией. Эти параметры создают индивидуальные «точки входа» для психологического воздействия, а когнитивные уязвимости

становятся ключевой точкой входа для кибератак, особенно при сочетании долгосрочных и краткосрочных факторов [4]. Возрастные особенности могут снизить способность распознавать фишинговые сообщения, а стресс – ускорить принятие ошибочных решений. Когда такие условия воздействуют на функции мозга, они ослабляют критическое мышление и увеличивают вероятность успешного применения методов социальной инженерии. Схематичное представление этих взаимосвязей, отражающее влияние факторов на когнитивные процессы, приведено на рис. 1.

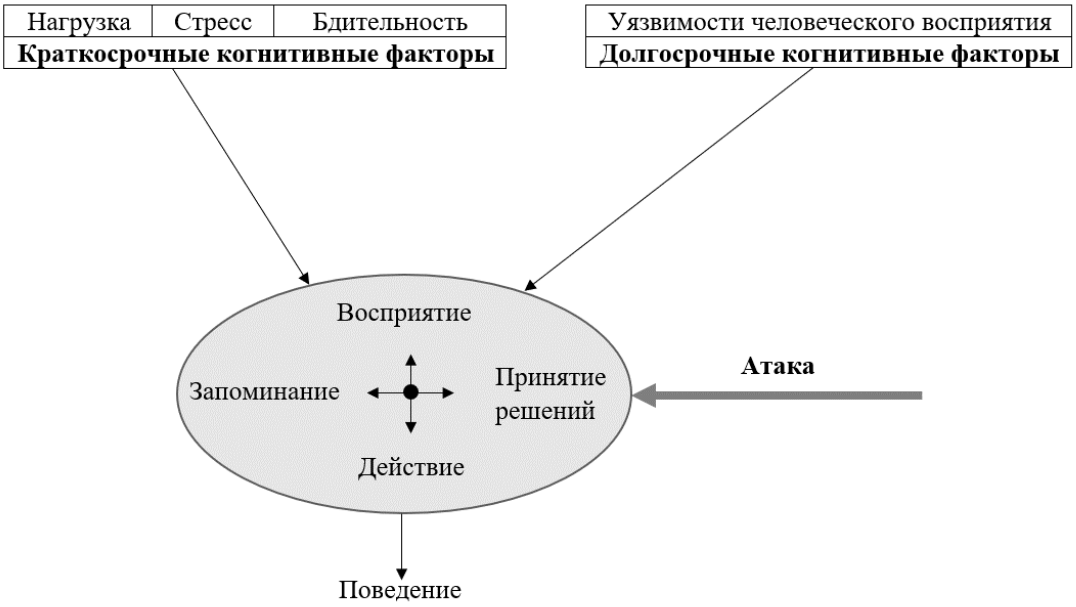

Рис. 1. Селективная схема человеческого познания с учётом атак класса «социальная инженерия»

Таким образом, становится очевидным суть негативного влияния «клипового» мышление – порождение уязвимостей, используемых злоумышленниками с целью реализации атак и нанесения ущерба (моральный, репутационный, материальный).

С целью минимизации негативов, возникших в эпоху клипового мышления, необходимо совершенствование образовательной среды для создания профессионально благоприятного развития личности.

Нейросетевой курс по информационной безопасности как обновлённый взгляд на текущий процесс образования

В ответ на растущий спрос на специалистов по информационной безопасности и необходимость повышения качества их обучения, курс «Введение в специальность» был существенно переработан. Ключевым нововведением стало использование нейросетевого аватара для озвучивания фактологического лекционного материала. Использование искусственного интеллекта позволяет легко адаптировать внешность и образ аватара под конкретную тему лекции. Например, при рассказе о правовой защите информации можно использовать аватара в строгом костюме, ассоциирующегося с юристом или профессионалом по ИБ. Для тем, посвященных описанию атак, подойдет образ хакера, что повышает вовлеченность аудитории благодаря лучшему визуальному соответствию материалу. Важно, чтобы аватар был хорошо виден на экране и ассоциировался с материалом, но при этом не отвлекал внимание яркими цветами и резкими движениями [5, 6]. Структура видеолекций оптимизирована для эффективного усвоения с учетом феномена «клиповое мышление». Длительность видеолекции не привышает 45 минут, что соответствует пределу концентрации внимания аудитории. Лекция начинается с 5-минутного вступления, кратко анонсирующего тему и концентрирующего внимание студентов. Основная часть лекции, продолжительностью 25 минут приходится на пик сосредоточенности. Материал

визуализируется с помощью презентации, на которой выделяется основная мысль, короткие тезисы, термины и схемы. Для большей наглядности используется цветовое выделение. В презентацию встроены практические примеры, которые демонстрируют работу уязвимостей и атак. После лекции проводится 15 минутное тестирование. Оно включает множество вопросов по только что пройденной теме и служит для эффективного закрепления полученных знаний.

Разработка технологии нейросетевого аватара стала возможной благодаря достижениям в машинном обучении, а именно созданию генеративно-состязательных сетей (GAN). В основе их работы лежит принцип взаимодействия двух независимых нейронных моделей. Первая сеть – генератор, которая отвечает за создание изображений. При запуске алгоритм получает на вход набор случайных параметров, не содержащий заранее заданной информации. Эти данные преобразуются в выходные кадры. Сформированное изображение затем анализируется второй частью системы – дискриминатором. Для оценки реалистичности созданного изображения дискриминатор сравнивает его с эталонными примерами, взятыми из реальных данных. Далее он выдаёт числовое значение качества. Эта оценка передается обратно генератору, который использует ее для корректировки своих внутренних параметров с целью улучшения результата. Между двумя моделями возникает конкуренция. Генератор пытается «обмануть» дискриминатор, создавая всё более реалистичные изображения, а дискриминатор, в свою очередь, совершенствует способность отличать подделку от оригинала. Именно такое соревнование позволяет системе постепенно повышать качество генерации. На рис. 2 представлена архитектура генеративно-состязательных сетей.

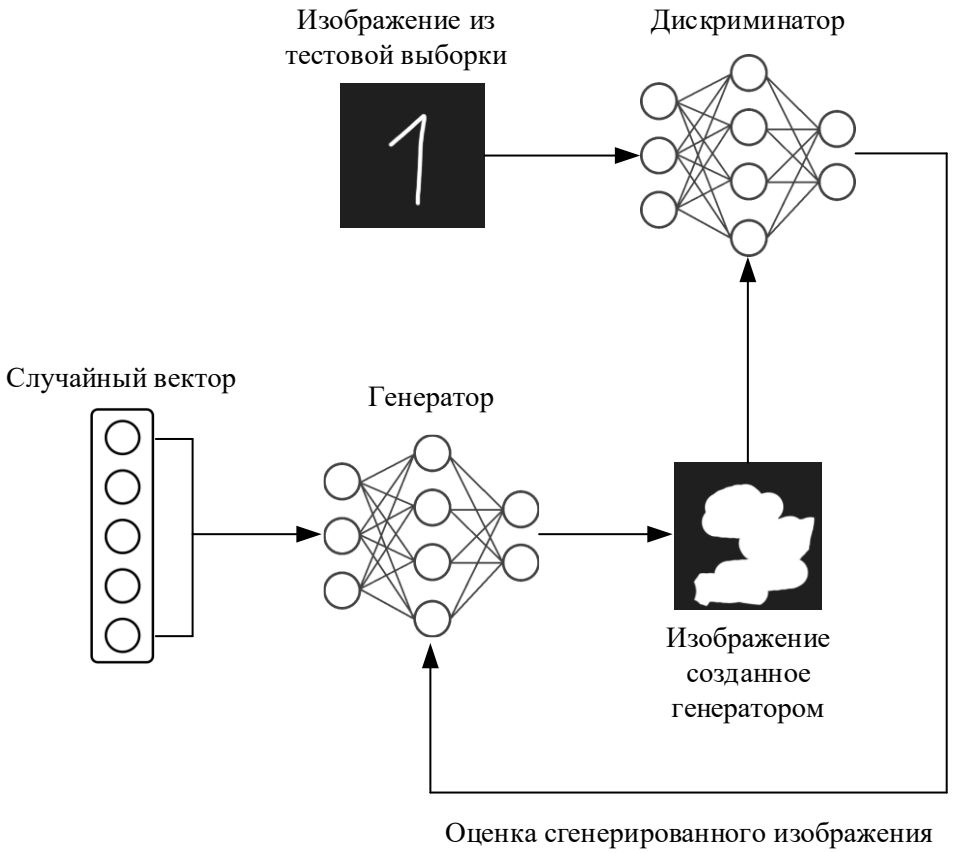

Рис. 2. Архитектура генеративно-состязательных сетей

Модель нейросетевого аватара, её характеристики и особенности

Создание динамичного цифрового аватара, способного синхронизировать мимику и речь, представляет собой многоэтапный процесс, объединяющий передовые методы машинного обучения и компьютерного зрения. Каждый этап требует тщательной подготовки данных и слаженного взаимодействия

компонентов системы. Для работы модели требуются следующие исходные данные:

- исходное изображение аватара – портрет человека в анфас, соответствующий разрешению 256x256 пикселей. Изображение должно быть снято при равномерном освещении, без выраженных эмоций, чтобы модель могла корректно воспроизводить нейтральное состояние аватара в моменты тишины. Это обеспечивает плавные переходы между анимацией губ во время речи и неподвижным положением лица в паузах;

- аудиофайл – несжатый звуковой файл формата .wav, содержащий сгенерированную речь аватара. Длительность записи определяет продолжительность итогового видео. Качество аудио напрямую влияет на точность синхронизации губ с фонемами, поэтому важно сохранять чистоту звука без шумов и искажений;

- список произносимых фонем в речи аватара – структурированный массив данных, в котором каждая фонема сопоставляется с конкретным кадром видео. Этот список формируется на основе временных меток, полученных при анализе аудиофайла, и представляет собой последовательность числовых кодов, где каждое значение соответствует определённой артикуляции губ;

- коэффициенты особенностей лица рассказчика – параметры, описывающие геометрию лица, текстуру кожи, освещение и другие визуальные характеристики. Они извлекаются из опорного видео с рассказчиком с помощью алгоритмов компьютерного зрения, таких как Deep3DFaceRecon. Эти данные обеспечивают индивидуальные черты аватара, включая форму глаз, носа, рта и динамику мимики;

- коэффициенты, описывающие движение головы рассказчика – матрица, отражающая траекторию поворотов и наклонов головы в пространстве. Они рассчитываются на основе анализа опорного видео и определяют естественность жестов аватара, такие как кивки, повороты и микродвижения головы, усиливающие визуальную достоверность создаваемого изображения.

Схема генерации аватара с требуемыми компонентами изображена на рис. 3.

Рис. 3. Схема генерации аватара

Для обеспечения комплексной подготовки данных, необходимых для генерации аватара, были разработаны четыре специализированных модуля. Каждый из них выполняет уникальную функцию, преобразуя исходные материалы (текст, аудио, видео) в структурированные данные, совместимые с моделью аватара. Эти модули работают

последовательно, обеспечивая высокую точность и согласованность между аудио и видео составляющими:

- модуль генерации голоса;
- модуль определения фонем;
- модуль захвата особенностей лица рассказчика;
- модуль захвата движений головы.

Модуль генерации голоса.

Модуль синтеза речи представляет собой многофункциональный компонент, построенный на основе передовых технологий генерации аудио. Он выполняет преобразование текстового контента лекций в речь, передающую интонационную выразительность и эмоциональный тон оригинального голоса. Все создаваемые аудиозаписи сохраняются в формате .wav, что обусловлено высокой степенью совместимости этого формата с нейросетевыми алгоритмами, а также – отсутствием потерь качества, связанных со сжатием. Это позволяет избежать необходимости дополнительной конвертации, которая может вносить искажения в звуковые параметры. Основной задачей модуля является генерация речи, максимально приближенной к естественному звучанию. Для достижения этой цели используется модель XTTS_V2, поддерживающая клонирование голоса по эталонной аудиозаписи и адаптацию к особенностям произношения. Модель обучена работать с более чем 15 языками, включая специализированную терминологию, что упрощает обработку текстов без предварительной сегментации.

Для ускорения вычислений реализована интеграция с графическими процессорами через CUDA, что снижает время генерации в 5–7 раз. Это особенно актуально при работе с объемными материалами, такими как длинные лекции или пакетные задания. Модуль также поддерживает конвейерную обработку. Одновременно можно отправлять на синтез несколько текстов, без необходимости повторного запуска программы. Процесс работы модуля можно представить в виде схемы на рис. 4.

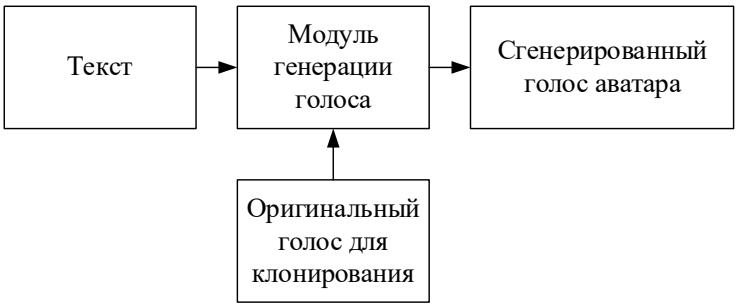

Рис. 4. Схема работы модуля генерации голоса аватара

Модуль определения фонем

Модуль определения фонем взаимодействует с уже сгенерированным голосовым файлом аватара. Его основная цель – разделить аудиозапись на минимальные звуковые элементы (фонемы) и привязать их к временной шкале, обеспечивая точное соответствие между речью и визуальной анимацией губ и мимики. Эта информация служит основой для построения движений лица, которые должны воспроизводиться синхронно с речью, создавая естественное восприятие.

Первым шагом в обработке становится разделение аудиофайла на речевые сегменты и тишину. Для этого используется библиотека pydub с функциями detect_silence и detect_nonsilence, которые анализируют уровень громкости и длительность тишины между словами. Использование этих функций позволяют точно определить границы слов, исключая шумы и артефакты. Этот этап критичен для последующих вычислений. Ошибки в сегментации приведут к рассинхронизации анимации.

После разделения на слова используется нейросетевая модель Allosaurus, обученная на речевых данных множества языков. Она анализирует каждый речевой сегмент, выделяя фонемы и их тайминги с точностью до миллисекунд. Эти данные затем преобразуются в формат, совместимый с моделью аватара: числовые коды фонем связываются с временной

шкалой, а паузы обозначаются отдельной меткой SILENCE. Такой подход позволяет аватару сохранять нейтральное выражение в моменты тишины, избегая лишних движений губ.

Качество работы модуля напрямую влияет на реалистичность аватара. Ошибки в определении фонем или их таймингов вызывают несоответствие между звучанием и визуальной анимацией, что снижает воспринимаемую естественность. Процесс работы модуля можно представить в виде схемы на рис. 5.

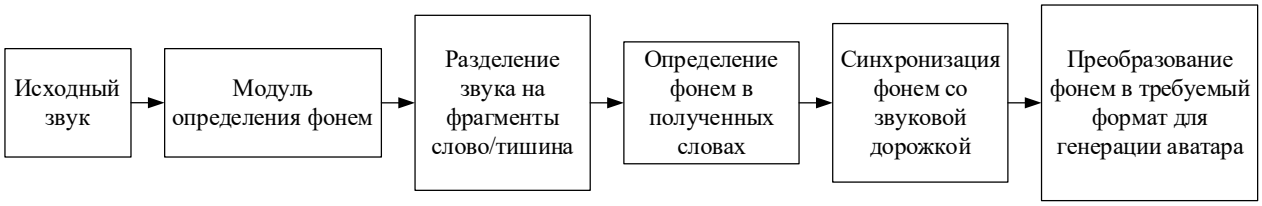

Рис. 5. Схема работы модуля определения фонем

Модуль захвата особенностей лица рассказчика

Данный модуль отвечает за формирование визуальной составляющей аватара. Для создания реалистичного изображения система использует параметры 3DMM, извлекаемые из опорного видео с применением методов компьютерного зрения. Работа модуля начинается с обработки видеозаписи и идентификации рассказчика в кадре. На следующем этапе выделяются ключевые точки лица, определяющие его форму, расположение глаз, рта и носа. После этого из видео извлекаются параметры, включающие:

- вектор уникальных черт лица (1x80). Каждая компонента вектора кодирует индивидуальные особенности человека из исходного видео (расстояние между глазами, форму носа);

- вектор мимики (1x64). Используется для управления выражением лица. Каждая компонента вектора управляет отдельными участками лица;

- вектор текстурных параметров (1x80). Описывает визуальные свойства кожи на отдельных участках лица;

- вектор положения головы (1x3). Три эйлеровых угла, определяющие положение головы;

- вектор освещения и цветокоррекции (1x27). Коэффициенты для моделирования условий освещения и коррекции цвета;

- вектор смещения головы относительно камеры (1x3);

- матрица ключевых точек лица (2x68). Хранит 68 точек, которые очерчивают контуры глаз, носа и рта рассказчика.

С помощью полученных параметров строится виртуальная 3D маска, которая позволяет при генерации учитывать множество полученных параметров.

Модуль захвата движений головы.

Модуль анализирует движения головы и лица на видео для создания реалистичной анимации аватара. В основе работы лежат методы компьютерного зрения: трекинг ключевых точек и анализ оптического потока, обрабатывающие каждый кадр. Эти технологии вычисляют параметры положения головы (углы поворота, смещение в пространстве) и динамику мимики.

Собранные покадровые данные формируются в единую временную последовательность. Она используется для повышения реалистичности анимации за счет учета микродвижений головы, присутствующих в исходных данных.

Покадровый сбор информации о движении головы позволяет:

- синхронизировать анимацию с речью: естественные покачивания головы подчеркивают эмоциональную окраску;

- клонировать поведение: уникальные паттерны движений человека переносятся на аватара, что повышает уровень схожести.

Схема работы модуля движений головы представлена на рис. 6.

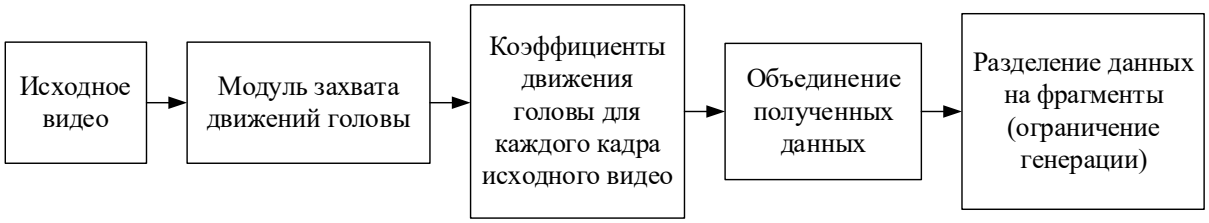

Рис. 6. Модуль захвата движений головы

Таким образом, была разработана модульная программная экосистема для генерации реалистичного аватара, объединяющая пять ключевых компонентов. Система позволяет использовать пользовательские материалы (изображение, аудио, видео) для создания персонажей, а её ключевое преимущество — повторное использование коэффициентов. Параметры мимики и движения головы, однажды полученные из опорного видео, можно применять для генерации новых анимаций без повторной обработки исходных данных.

На рис. 7 представлена архитектура экосистемы, где каждый модуль выполняет строго определённую задачу, обеспечивая слаженную работу всей системы.

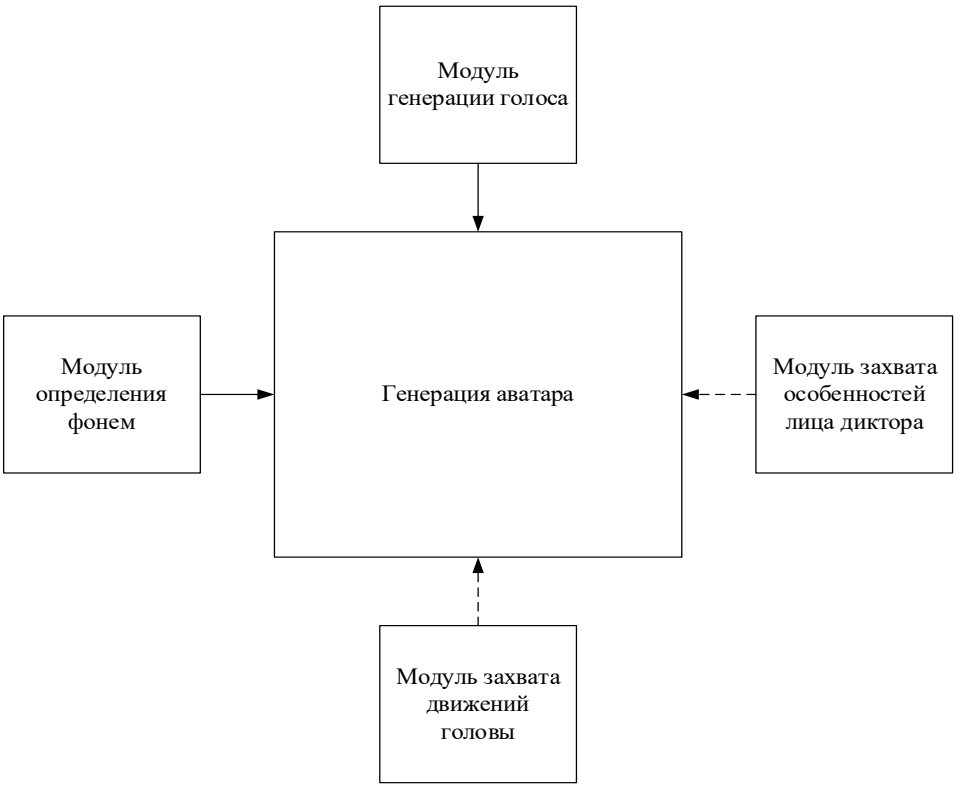

Рис. 7. Модуль захвата движений головы аватара

Для озвучивания курса по основам защиты информации были взяты несколько шаблонов лиц, сгенерированных нейросетью. Для этого с использованием разработанного нейросетевого инструментария из выбранного исходного видео был получен шаблон лица, двигающий головой и губами в соответствии с озвучиваемым текстом.

Голос нейросетевого аватара должен подходить его внешнему виду. Последние исследования показывают, что для получения максимального внимания со стороны слушателей в мужском голосе должны преобладать низкие тона, а в женском - высокие [7]. Необходимо также учитывать скорость произношения слов, качество речи, расстановку акцентов и пауз.

Фон для аватара и одежда не должны выделять его на фоне представляемого материала. В данном случае реализация популярной и повсеместно используемой в маркетинге стратегии добавления контрастных цветов

будет отбирать внимание аудитории, что негативно скажется на запоминании представляемого материала.

Ресурс для размещения лекционного материала и тестирования

Весь курс видеолекций размещён на специально разработанном сайте. Площадка оказалась наиболее удобной для размещения цикла видеолекций, а также для обеспечения непрерывного доступа к ней со стороны преподавателей и студентов.

Схематичное представление ресурса доступа с входящими в него модулями представлено на рис. 8.

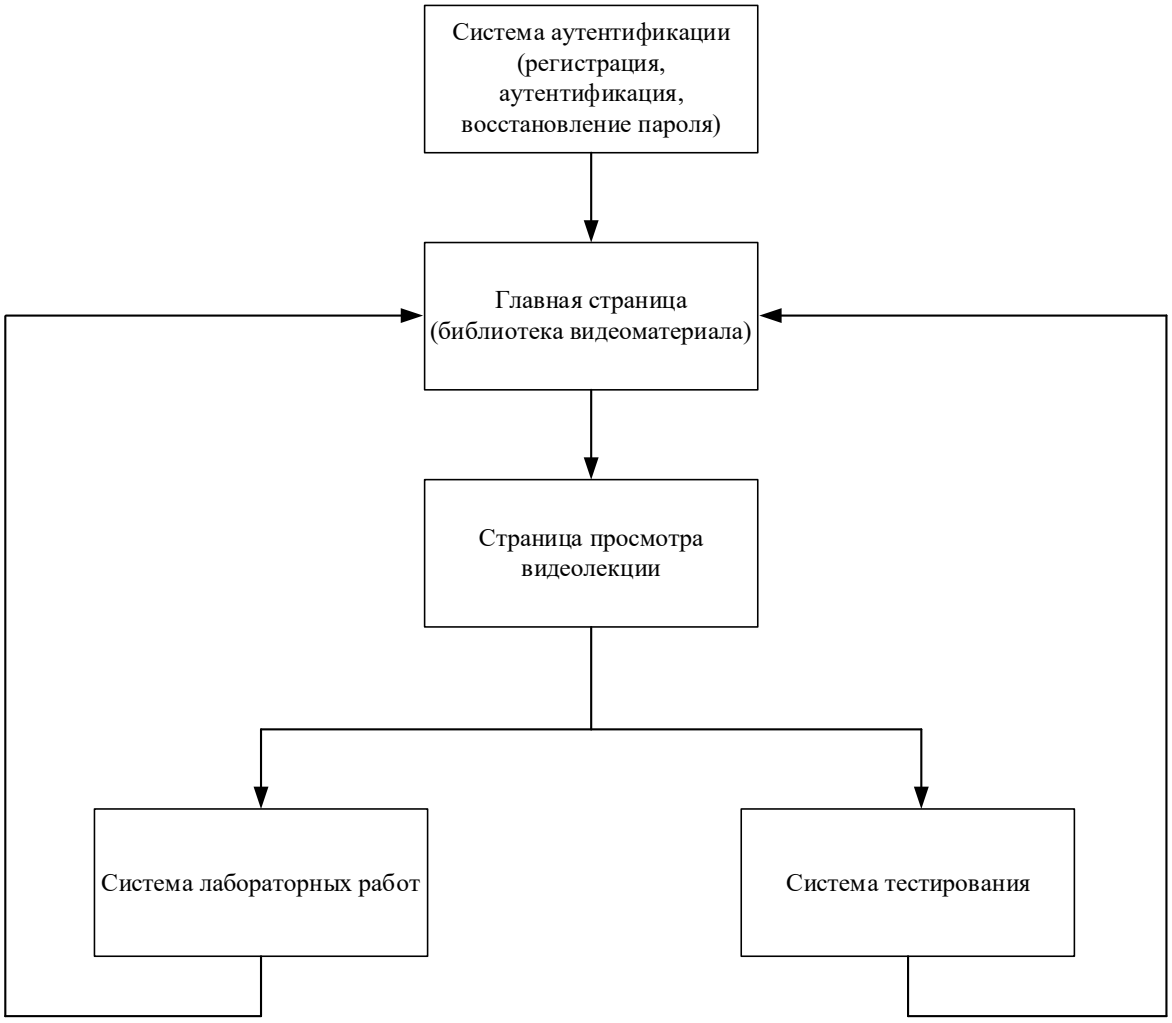

Рис. 8. Схематичное представление взаимодействия структурных элементов ресурса

Образовательная платформа реализована в виде веб-приложения, построенного по традиционной трехуровневой архитектуре:

- клиентская часть формирует интуитивно понятный пользовательский интерфейс для взаимодействия с системой. Визуальная составляющая автоматически адаптируется под разные устройства. Этот уровень отвечает за передачу пользовательских запросов на сервер для обработки и получение результата;

- серверная часть принимает входящие запросы от пользователей и обрабатывает их. На этом уровне происходят основные вычисления и расчеты. Сервер взаимодействует с базой данных, выступая посредником между пользователем и хранилищем;

- база данных представляет собой комплекс взаимосвязанных таблиц, организованных по реляционной модели. Это обеспечивает целостность и согласованность хранимой информации. Доступ к данным осуществляется через структурированные SQL-запросы, формируемые серверным уровнем, что исключает прямое взаимодействие с клиентской частью.

Для разработки клиентской части приложения использован Vue.js, который позволяет создавать высокопроизводительные одностраничные веб-приложения. Благодаря ему страница обновляется мгновенно, без необходимости полной перезагрузки, что ускоряет работу и повышает удобство использования. В качестве серверной платформы выбран Node.js, обеспечивающий параллельную обработку множества запросов. Это критично для веб-приложения, построенного на постоянном взаимодействии компонентов. Выбранная связка Vue.js и Node.js является традиционной для современных веб-приложений и обеспечивает высокую совместимость и устойчивость. Для хранения данных применена открытая реляционная система управления базами данных MariaDB, демонстрирующая высокую производительность даже при выполнении комплексных SQL-запросов.

На образовательной платформе реализованы следующие модули, поддерживающие учебный процесс:

- главная страница: содержит коллекцию обучающих видео, упорядоченных в соответствии с последовательностью занятий в аудитории. Предусмотрена функция поиска, позволяющая быстро находить нужный материал;

- раздел «Тестирование»: включает задания для закрепления знаний по каждой теме. Для каждого урока доступны 90 вариантов вопросов, из которых случайным образом формируется индивидуальный тест с произвольным количеством заданий. Система автоматически проверяет тест и выдает результаты тестирования, содержащие детализированную информацию по каждому ответу на вопрос;

- раздел «Игры»: интерактивные тренажёры, разработанные с опором на методику изучения технических специальностей. Эта часть делает обучение более увлекательным и способствует лучшему усвоению информации;

- раздел «Результаты тестирования»: личный кабинет, где можно анализировать итоги пройденных тестов и отслеживать динамику успеваемости.

Заключение

Таким образом, основными полученными **результатами** являются:

- выделение уникального набора уязвимостей человека для поколения Альфа, а также их классификация и оценка влияния в случае проведения атак класса «социальная инженерия»;

- разработан и создан информационный материал для создания нейросетевых видеолекций курса «введение в специальность» специалистов по защите информации;

- создан нейросетевой аватар, излагающий лекционный материал;

- создана площадка для размещения разработанного нейросетевого видеокурса, которая была дополнена разделом тестирования и лабораторных работ с элементами геймификации.

Список литературы

1. Статистика больших данных. URL: https://xmldatafeed.com/statistika-bolshih-dannyh-2022-skolko -sushhestvuet-bolshih-dannyh/ (дата обращения: 20.04.25).

2. Семеновских Т.В. Феномен «клипового мышления» в образовательной вузовской среде / Т.В. Семеновских // Науковедение. 2014. Вып. 5 (24), сентябрь-октябрь. 10 с. URL: https://naukovedenie.ru/PDF/105PVN514.pdf (дата обращения: 20.04.25).

3. Купчинская М.А. Клиповое мышление как феномен современного общества / М.А. Купчинская, Н.В. Юдалевич // Бизнес-образование в экономике знаний. 2019. № 3 (14) С. 66-71.

4. Montanez R, Golob E, Xu S. Human Cognition Through the Lens of Social Engineering Cyberattacks. Front Psychol. 2020 Sep 30;11:1755. doi: 10.3389/fpsyg.2020.01755. PMID: 33101096; PMCID: PMC7554349.

5. Психология цвета в рекламе. URL: https://accent.su/blog/psihologiya-tsveta-v-reklame/ (дата обращения: 20.04.25).

6. Ижденева И.В. Развитие ассоциативного мышления студентов при изучении математических и информатических дисциплин / И.В. Ижденева // Вестник красноярского государственного педагогического университета им. В.П. Астафьева (Вестник КГПУ). 2015. № 1 (31). С. 153-157. (дата обращения: 20.04.25).

7. Why we’re attracted to certain voices. URL:

https://brighterworld.mcmaster.ca/articles/why-were-attracted-to-certain-voices/ (дата обращения: 20.04.25).

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 26.04.2025

Информация об авторах

Остапенко Александр Григорьевич – д-р техн. наук, профессор, заведующий кафедрой, Воронежский государственный технический университет, email: alexostap123@gmail.com

Москалева Екатерина Алексеевна – канд. техн. наук, доцент, доцент кафедры систем информационной безопасности, Воронежский государственный технических университет, e-mail: ea.vrn@yandex.ru

Краснобородкин Александр Геннадьевич – студент, Воронежский государственный технических университет, e-mail: a.krasnoborodkin@internet.ru

Катюрин Дмитрий Александрович – студент, Воронежский государственный технических университет, e-mail: d.katiurin@yandex.ru

Баранников Николай Ильич – д-р техн. наук, профессор, Воронежский государственный технический университет, email: alexanderostapenkoias@gmail.com

Грамыкин Максим Алексеевич – студент, Воронежский государственный технических университет, e-mail: alexanderostapenkoias@gmail.com

METHOD FOR DEVELOPING ELECTRONIC COURSES IN THE FIELD OF CYBERSECURITY: VISUALIZED INTERACTIVE PRESENTATION OF TEACHING MATERIALS USING NEURAL NETWORK TECHNOLOGIES

A.G. Ostapenko, E.A. Moskaleva, A.G. Krasnoborodkin, D.A. Katyurin, N.I. Barannikov, M.A. Gramikin

The article is devoted to improving the educational process in the field of information security through the development of a video lecture course, where a neural network «avatar» acts as the speaker. During the course of the work, the concept of the video lecture course was defined and implemented, taking into account innovative teaching technologies. Based on the psychology of information perception, a neural network assistant was developed, and a resource was created that allows users to view a series of clips, take tests on relevant topics, and solve problems in a game format.

Keywords: information security, neural network «avatar», neural networks, learning process, clip thinking

Submitted 26.04.2025

Information about the authors

Alexsandr G. Ostapenko – Dr. Sc. (Technical), Professor, Head of Department, Voronezh State Technical University, e-mail: alexostap123@gmail.com

Ekaterina A. Moskaleva – Cand. Sc. (Technical), Associate Professor, Department of Information Security Systems, Voronezh State Technical University, e-mail: ea.vrn@yandex.ru

Alexander G. Krasnoborodkin – student, Department of Information Security Systems, Voronezh State Technical University, e-mail: a.krasnoborodkin@internet.ru

Dmitry A. Katyurin – student, Department of Information Security Systems, Voronezh State Technical University, e-mail: d.katiurin@yandex.ru

Nikolay I. Barannikov – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Maxim A. Gramikin – student, Department of Information Security Systems, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com