Подходы к социокультурной и информационной безопасности нейросетевых технологий в разработке чат-ботов

Н. Н. Покровская
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
nnp@spbstu.ru

***Аннотация*. Нейронные сети обучаются на фактическом материале. Люди в своем общении используют как социокультурные правила вежливости и хорошего тона, так и учитывают угрозы для защиты данных, опираясь на длительный опыт и долгосрочное прогнозирование рисков. Человеческое поведение даёт нейросетям примеры как адекватного поведения, так и манер с ограниченным применением в зависимости от контекста, а также неприемлемых и недопустимых поведенческих моделей, например, эмоциональной разрядки в грубом стиле или раскрытия информации в связанных метаданных. На основе разбора нескольких кейсов внедрения и функционирования чат-ботов показаны основные группы этических проблем и основные задачи в сфере информационной безопасности, выявлены ключевые подходы к обеспечению этикета и защиты данных, сформулированы предложения по процедурам для машинного обучения применительно к чат-ботам в корпоративных экосистемах.**

Ключевые слова: нейросеть; цифровизация; цифровая трансформация; бот; чат-бот; экосистема; этика; процедуры; регуляция; информационная безопасность; социокультурное регулирование; защита данных

I. Введение

Разработка приложений технологий искусственного интеллекта прошла ряд этапов от фундаментальных научных открытий и создания инженерно-технологических решений до формирования сложных поведенческих моделей покупателей для разработки маркетинговых стратегий, и попыток решения социальных задач на основе интеллектуальных аналитических систем. Совершенствование цифровых инструментов приводит к переносу социальной регуляции в виртуальное пространство. Коды сетевой или веб-культуры помогли нам построить первые нормативные формулы, которые по-прежнему пригодны для онлайн-общения, даже если сегодня коммуникация происходит в ускоренном режиме в горизонтальных слоях онлайн-сообществ.

Концепция безопасности в цифровой среде отражает проблемное поле, возникшее в связи с социальным поведением. Существенные вопросы кибербезопасности связаны с человеческим восприятием и реакцией [1], включая как биологическую, так и социальную природу человека [2]. Физиолого-психологическая составляющая общения в коллективе определяет бесконечное разнообразие возможных действий и реакций человека, а сложная система ценностей и мотиваций фиксирует ряд ограничений для личного выбора каналов удовлетворения потребностей индивида. Это рассуждение касается как реального, так и виртуального поведения: в первые десятилетия функционирования интернета появились новые правила и обычаи [3] в контексте реализации поведенческих паттернов в соответствии с социальными нормами взаимоуважения и безопасности.

В данной статье исследуются регулятивные механизмы, помогающие обеспечить социокультурную и информационную безопасность на основе выбора в ходе машинного обучения реакций чат-ботов в соответствии с наблюдаемым поведением человека в сети Интернет. Чат-боты представляют основной инструмент, где этические, юридические и технологические правила рассматриваются с точки зрения вопросов безопасности [4]. Маркетинговые кампании по продвижению товаров и услуг, информационные «войны» и коммуникативная конкуренция демонстрируют важность обоих основных видов безопасности, с которыми необходимо работать: «техническая» информационная безопасность включает в себя меры по предотвращению финансовых и физических личных рисков, «этическая» безопасность и забота о социокультурных основаниях касается психологического комфорта индивидов [5], а также защиты набора ценностей и норм, формирующих идентичность сообщества [6].

Кибербезопасность описывает уровень защищённости как программного обеспечения, в качестве пространства для потоков данных, так и самих данных. В статье речь идет о защите формы и содержания информации – персональные данные отражают доступ к активам (право собственности, авторские права и т. д.), содержательно защите подлежат смыслы, видение мира как основание для выбора способа реагирования, которые формируют культуру как механизм воспроизводства общества.

II. Нейронная сеть посредством машинного обучения и цифрового регулирования поведения

Машинное обучение основано на анализе фактов о реальных поведенческих актах людей, которые фиксируются в цифровой среде [7]: регистрируются непосредственно через онлайн-коммуникации людей или с помощью различных способов мониторинга, таких как распознавание лица и действий на основе фото и видео благодаря «умным улицам», дорожным камерам и т. д.

Регуляция поведения человека в сети отличается от офлайн-реакций и поведенческих паттернов [8]. Онлайн-

коммуникация строится на специфическом фильтре восприятия отдалённой, опосредованной физической реальности, на переводе с богатого «языка» бесконечного разнообразия и изменчивости живых существ и меняющейся среды на ограниченные нормы, критерии и предпочтения внутри онлайн-пространства. платформы.

A. Нейросетевые технологии как анализ фактов и зависимостей между фактами

Параметры безопасности для алгоритмов чат-ботов основаны на анализе действительности, реальное поведение человека включает в себя три слоя – настоящее, прошлое и будущее, которые выражаются в реальном поведении, отражающем традиции и обычаи и нацеленном на реализацию заданных целей и ценностей.

Культура представляет собой накопленный опыт сообщества, содержащий способы решения проблем и достижения намеченных целей. Культура интенциональна и направлена на коллективные интересы сообщества. Поскольку информационная безопасность исследует вероятность нанесения ущерба интересам пользователей, то необходимо определить, какие интересы могут быть нарушены при неправильном использовании данных. Параметры безопасности отражают ценности и интересы, их иерархические приоритеты, что позволяет определить потенциальное поле для защитных мероприятий.

B. Нейросетевые технологии и обработка данных пользователей

Субъекты обеспечения информационной безопасности, в первую очередь, включают самих пользователей, они защищены системами онлайн-коммуникации, вплоть до запрета действий, опасных для их данных. Примером попытки сохранения пользователем анонимности при одновременном раскрытии им информации служит ввод адресов почты (например, «annaivanova1998@email.nn») и номеров мобильных телефонов, которые идентифицируют человека, поскольку гражданин РФ (и ряда других стран) может купить сим-карту только при наличии паспорта.

Платформы обязаны спрашивать у пользователей их согласие на сбор данных пользователей. Тем не менее, огромные объемы информации собираются без согласия пользователя, Google и Facebook несколько раз заплатили штрафы за утечку или некорректное обращение с данными клиентов. Объем структурированных переплетенных данных превосходит возможности человеческого анализа, машинные алгоритмы позволяют подбирать функции, описывающие процесс совершения выбора человеком. Перечисленные причины объясняют, почему машинное обучение на основе нейросетевых технологий выступает наиболее подходящим инструментом для формирования содержания ответов чат-ботов.

C. Вопросы безопасности в нейронных сетях

Выделим три элемента, касающиеся безопасности:

- Данные пользователей включают, прежде всего, угрозу раскрытия информации у истока самими пользователями. Часто пользователи, заполняя форму на сайте или в разговоре с ботом, выдают набор данных, однозначно идентифицирующих их.
- Платформы занимаются сбором данных с согласия пользователей и без такового. Закон регулирует торговлю обезличенными записями, но систематические расследования выявляют случаи неправильного использования личной информации.
- Данные пользователей могут быть объединены из разных источников и обработаны алгоритмами, непонятными для человека или предвзятыми по определенной причине (например, полиция в США создала прогностическую систему, которая интерпретирует грустное лицо как признак потенциального преступника, а веселых людей идентифицирует как добросовестных граждан); распознавание лиц позволило в Южной Корее во время пандемии автоматически приглашать для проведения тестов всех контактных лиц, находившихся рядом с заболевшими в общественном транспорте, на улице, и т. д.).

Эти примеры проблемных областей информационной безопасности не исчерпывают, но очерчивают проблематику адекватного и корректного, внимательного отношения к данным. В то же время в основе опасений по поводу обработки машинных данных с помощью нейронных технологий лежат культурные и этические проблемы.

III. Социокультурная и информационная безопасность

Культура – это социальный механизм передачи сущности идентичности во времени с передачей знаний.

A. Социокультурная система как основа устойчивости сообщества

Этические вопросы включают, как правило, вопрос об ограничении частной жизни людей. Вместе с тем, социокультурная безопасность шире, она касается права сообщества воспроизводить и развивать себя как систему символического содержания, включающую ценностно-смысловую шкалу приоритетов, видение мира как репрезентативную схему истолкования фактов в рамках набора значений. Например, социально-профессиональное сообщество использует специфический язык, в котором слова имеют иное значение и произношение, отличное от значения и произношения населения в целом.

Обычные люди также образуют особую категорию, чем объясняется устойчивость и сопротивляемость этносов любым попыткам разрушить их автономию. Маркетологи нередко работают с лидерами мнений, но для эффективного анализа используют образ типичного «обычного» клиента. Расширение глобальных цепочек поставок и транснациональный бизнес показали силу местных традиций, маркетинговые коммуникации учитывают местные особенности, даже макдональдизация как пример глобальной продуктовой стратегии включает специфическую национальную кухню в странах, где локализованы рестораны данной сети [9].

Социокультурная безопасность отражает защиту культурных элементов, формирующих идентичность сообщества. Риски для социокультурной идентичности включают в себя ложную информацию о национальных или региональных, этнических или религиозных действиях, ценностях, намерениях, оценках и поддерживаемых личностных чертах, модус операнди («способах действия»), которые характерны для членов сообщества и ценятся населением этого сообщества. Эта логика применима к национальным государствам, цивилизациям, региональным и локальным обществам, организационно-корпоративным единицам, социально-профессиональным сообществам.

B. Информационная и социокультурная безопасность в ситуациях конфликтов и соперничества

Информационная и социокультурная безопасность отражает защиту сообщества от продвижения привлекательных образов и репрезентаций другой группы людей, конкурентов в борьбе за редкие ресурсы (как социальную категорию) или конкурентов за долю рынка как бизнеса. Согласно концепции диффузии инноваций, новое предпочтение будет распространяться, как круги по воде, и чем более привлекательна иллюзия, тем больше будет объем распространяющихся волн.

Культура включает глубинные регуляторы, которые остаются не осознанными до момента встречи одной социальной группы с другой, сопоставление привычек и обычаев описывается как «культурный шок» из-за понимания многообразия и, в то же время, является моментом, когда человек осознает собственные встроенные регулятивные опоры, которые управляют его поведением. Культурный шок состоит в сравнении ранее единственно возможной нормальной модели поведения с новыми вариантами, которые ранее были невообразимы. Информационная война представляет стратегии одного сообщества по навязыванию своих ценностей и норм другому, продвигая привлекательные иллюзии, показывая положительные результаты, но не упоминая о стоимости их достижения, о цене, которую придётся за них заплатить.

Социально-культурная и информационная безопасность как система включает в себя следующие компоненты:

- Механизм обнаружения выявляет потенциальные атаки и риски, исследует их возможные формы и источники. Для социокультурной безопасности источником риска является предпочтение референтным лицом элемента чужой культуры.
- Механизм контроля определяет санкции, которые применяются к субъектам, несущим риски информационной и социокультурной безопасности. Обычно смысл любой санкции состоит в том, чтобы не дать акторам действовать неприемлемым образом: если игрок знает последствия своих действий, он сам выберет наиболее подходящую модель действий, чтобы больше получить и меньше потерять. В цифровой среде контроль опирается на вездесущий мониторинг цифровых следов.
- Механизм регулирования включает ожидаемые последствия и, при необходимости, реализацию социальных санкций, в первую очередь, отчуждения и неодобрения, вплоть до штрафов и лишения свободы в качестве фиксированных и «материализованных» форм эксклюзии (лишение ресурсов, в случае уплаты штрафа и ограничения контактов с обществом при заключении в тюрьму).
- Социокультурная безопасность представляет собой баланс легитимности. Общество одобряет санкции против своих членов, если нормы, которые были ими нарушены, воспринимаются как существенные, значимые и ценные. Бунты возникают в моменты, когда общество вырабатывает новую ценностную шкалу, а реализация «старой» нормативно-ценностной системы воспринимается массами населения как нецелесообразная и неактуальная.

Последний пункт представляет интересный компонент для нейронных сетей, реализованных в машинно-человеческом общении, поскольку анализ предыдущих фактов поведения и краткосрочной динамики выбора пользователей не дает четкого измерения степени принятия выбора (приоритет ценности, суждение о норме поведения, новом видении мира).

C. Механизмы социокультурной безопасности

Оперативное планирование любой акции военные эксперты описывают как восстановление баланса между настроением и ожиданиями широкого населения (с их повседневной жизнью и простыми целями, такими как купить хлеб и дать образование детям) и стратегиями действий национального развития с учетом располагаемых ресурсов, поскольку в противном случае, если военное решение встретит сопротивление, то затраты на контроль территории будут превышать выигрыш от её захвата.

Социокультурная безопасность представляет собой основу для такого планирования, например, в рыночной конкуренции между компаниями, ориентированными на прибыль, взвешивание различных ценностей (таких, как набор из 18 ценностей, инструментальных и терминальных в теории М. Рокича, или 8 уровней мотивации по А. Маслоу), норм поведения и представлений о том, как устроен мир, является латентным процессом, когда в личности действуют глубинные культурные основания.

Задача регулирования состоит в том, чтобы в любой момент выяснить состояние этого баланса. В вопросах безопасности эксперты пристрастны, потому что они тоже люди со своими культурными правилами и устоями; специалисты профессиональных групп – носители своего культурного бэкграунда, что объясняет, например, различия в удобстве использования программ и платформ для восточных и западных пользователей, отличия социальных сетей (российского вК и американского Fb), расхождение русского и западного инстаграма (русский сектор этой соцсети требует гораздо больше текста, чем европейский или американский сектора), а структура и организация Вичата адаптированы под специфику норм восприятия, характерных для китайских пользователей.

Противоречие состоит в том, что нейронная сеть анализирует предыдущие факты и не имеет средств для своевременного выявления смены настроений, нейронной сети для анализа требуются заранее квалифицированные единицы в качестве оценочного суждения, но машинные средства не в состоянии предсказать изменение оценочных суждений, даже если они способны распознать знак (положительный/отрицательный); в то же время специалисты, будучи людьми, являются носителями социокультурных регуляторов, усвоенных в детстве, а люди обычно не осознают своих интериоризированных регуляторов как предубеждений при суждениях.

Экспертное машинное обучение («обучение с учителем») помогает выявить динамику шкалы ценностей в случаях заранее известных ценностей и приоритетов, когда эти степени и шкалы выражены. Но машинное обучение не способно предсказать человеческое суждение перед действительно важным стратегическим решением, настроение массового населения можно обнаружить только экспериментально, тестовым способом, что иногда является политическим провалом. Известны многие неудачные примеры, такие как пенсионная реформа в России в июле 2018 года, которая толком не решила экономических задач и способствовала нарушению «крымского консенсуса», подъема патриотизма с 2014 г.; или продажа более дешевых автомобилей Jaguar в 2008-2009 годах на рынках во время мирового финансового коллапса, когда нижние сегменты не приняли этот роскошный автомобиль как популярный продукт, а верхние сегменты рынка посчитали это предвестником краха компании и сократили спрос.

IV. Разработка чат-ботов и проблематизация социокультурной безопаности

Чат-боты представляют собой общение между машиной и человеком, в котором эффективно используются технологии нейронных сетей для развития диапазона реакций на действия человека.

A. Чат-боты и вопросы безопасности

Применительно к чат-ботам с нейронными сетями обычно выделяют следующие группы проблем, связанных с обеспечением безопасности:

- Вежливость и этикет в общении человек-человек (h2h) отличается от типа человек-машина (h2m): в обыденном восприятии люди заслуживают вежливого обращения, а машины – нет, люди ведут себя по отношению к машинам более грубо, чем к людям. Если робот использует опыт разговора с людьми, чтобы учиться на используемых предложениях и словах, и попытается скопировать их и ответить теми же фразами, чат-бот очень скоро будет отключен за неуместную манеру общения. Ожидается, что роботы и чат-боты будут более вежливыми и ответственными, чем люди.
- Закреплённая дискриминация при выборе связана с анализом ботами предыдущего распределения человеческих ресурсов (HR), включая гендерные, возрастные и расовые стереотипы («молодая блондинка-секретарша» – нейронная сеть сделает вывод, что чат-бот должен отказать мужчине старше 40 лет на вакансию секретаря). Эту проблему отбора с неэффективной дискриминацией можно решить с помощью системного вмешательства человека, экспертного машинного обучения, когда HR-специалисты изучают алгоритмы отбора чат-ботов и вычищают из них эйджизм, сексизм и расизм как унаследованные из истории, но неоптимальные критерии выбора.
- Сбалансированность эмоций чат-ботов – проблема человеческого восприятия общения, которое должно быть богато аффективными нюансами, в то же время отвращение к тому, что машина притворяется человеком, вызывает необходимость четко различать, что говорит человек к машине, поэтому излишняя эмоциональность неприемлема.

HR-специалисты также отмечают нормативные рамки законодательства, которые ограничивают возможности использования чат-ботов для сбора персональных данных: в соответствии с правовыми процедурами пользователь должен подписать соглашение об обработке персональных данных, прежде чем предоставлять какие-либо персональные данные, но с чат-ботом уже происходит персонифицированное общение. Это означает замкнутый круг общения, начинающегося при данном согласии. Эту процедуру можно решить с помощью кнопки «принять файлы cookie», тем не менее, система управления персоналом учитывает проблемные области, связанные с безопасностью персональных данных.

Социокультурная безопасность информационной системы уязвима для людей как пользователей (которые могут иметь собственное видение моделей поведения в контексте общения с чат-ботом и совершать необдуманные поступки с собственными персональными данными), так и специалистов (уже стал анекдотом пример неопытного HR-менеджера, который искал механика 4-го разряда до 40 лет). Иногда организации или сообщества сталкиваются с проблемами, происходящими от собственных сотрудников или лиц, ответственных за хранение данных, за кибербезопасность или цифровое регулирование (согласно Указу Президента РФ от 1 мая 2022 №250, системные предприятия должны формировать собственную службу информационной безопасности, начиная с 2025 г. [10]). Можно привести пример банковского сектора, где по статистике большинство утечек персональных данных являются незаконными сделками со стороны сотрудники; самые известные скандалы вокруг компаний также устраивают инсайдеры, которые предоставляют внутренние корпоративные данные посторонним, журналистам или просто публикуют информацию в своих профилях в социальных сетях.

Специалисты по кибербезопасности упоминают вопрос правового регулирования в сфере фейковых новостей, ложной информации или ссылки на запрещенный источник (например, иностранного агента или террористическую организацию), которые могут быть представлены на онлайн-ресурсах компании или местного, регионального сообщества или топ-менеджера.

Эти вопросы социокультурной и информационной безопасности можно классифицировать в таблице:

ТАБЛИЦА I ПРОБЛЕМЫ СОЦИОКУЛЬТУРНОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ ЧАТ-БОТА

Сфера	**Инструменты безопасности**		
	Проблемы безопасности	***Источники риска***	***Вариант решения***
Разглашение данных	Люди редко осознают возможности машинных средств объединять данные из разных источников и делать выводы о различных вариантах выбора пользователей	Сетевая культура пользователя	Развитие правил и процедур, ограничивающих действия
Утечки данных	Специалисты, отвечающие за хранение данных, недостаточно удовлетворенные в сообществе, могут посчитать данные пользователей как источник роста своих доходов. Опасен приоритет корыстного интереса	Недооценка мотивов инсайдеров	Оценка шкалы ценностей, анализ поведения
Публикации	Противоречащие закону публикации в условиях прозрачности цифрового онлайн-мира связаны с соблазном для некоторых людей произвести вау-эффект, для этого они публикуют материалы, разрушающие идентичность сообщества	Члены организации, участники сообщества, сотрудники	Экспертные нейросети способны выявлять таких агентов
Разнообразие ценностей	Социокультурная система воспроизводит общество в символическом универсуме восприятий и идентичностей. Конкуренция между сообществами за доступ к ресурсам выражается в соперничестве за выбор смысла	Субъекты, задающие стратегии	Эксперты ставят задачи, нейросетевой анализ выявляет признаки

[a] Составлено автором

Стратегия эволюции социокультурного разнообразия и естественного отбора включает в себя попытку завоевать лояльность участников чужого сообщества и трансформировать их идентичность, заменить её своей. Символический мир является полем соперничества ценностно-смыслового семантического картирования [11], но сиюминутные ситуативно привлекательные идеи часто противоречат долгосрочным глубинным культурным основаниям идентичности. Стратегия распространения иллюзорных мнений о жизнедеятельности сообществ (вплоть до расчеловечивания людей, принадлежащих к иному сообществу, клану, государству, отрасли или бизнесу), эффективна в тот момент, когда разрушен прежний идентифицирующий миф и ещё только реконструируется новый, но глубокие корни культурной идентичности будут способствовать взращиванию нового социокультурного «дерева» ценностей и норм. Так, Цейлон сохранил ланкийскую культуру (насчитывающую более двух с половиной тысяч лет) вопреки голландскому и затем британскому владычеству и вернул социальную ткань, создав в 1972 г. независимое государство Демократическую социалистическую республику Шри-Ланка. Корпоративная история идентичности может быть прослежена на примере ПАО «Газпром», сохранившего за 30 лет самоопределение и модус операнди советского министерства газовой промышленности, включая ведомственную социальную инфраструктуру для сотрудников и роль компании в геополитической и геоэкономической позиции страны.

V. ЗАКЛЮЧЕНИЕ

Механизм выявления угроз и рисков социокультурной и информационной безопасности исследует потенциальную опасность поведенческих актов людей, вовлеченных в функционирование цифровых инструментов, в т. ч. чат-ботов – пользователей, специалистов, программистов. Намерения можно прогнозировать на основе мониторинга шкалы приоритетов интересов и мотиваций человека, а защитить пользователя от его собственных ошибочных (часто в силу недостаточной цифровой компетентности) решений может совершенствование процедур. Эксперты, привлеченные к анализу критериальных моделей в алгоритмах нейронных сетей, могут помочь адаптировать правила и процедуры к требованиям закона и рискам осознанного потенциально опасного поведения.

В отличие от узкого понимания кибербезопасности, социокультурная защищенность в цифровой среде является сложной областью для защиты и требует тонкого сочетания человеческих и технологических решений и итеративного их тестирования. Система культурной трансмиссии, передачи знаний и образования и воспитания должна быть понятна гражданам и строиться таким образом, чтобы поддерживать идентичность национального общества, регионального или профессионального сообщества.

СПИСОК ЛИТЕРАТУРЫ

[1] Wiener N. The human use of human beings : cybernetics and society. Boston: Houghton Mifflin, 1950.

[2] Wiener N. Cybernetics; or, Control and communication in the animal and the machine. Paris: Hermann & Cie; Cambridge, Massachusets, US: MIT Press, 1948.

[3] Pokrovskaia N.N. Tax, financial and social regulatory mechanisms within the knowledge-driven economy. Blockchain algorithms and fog computing for the efficient regulation // Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017. N.Y.: IEEE, 2017. doi: 10.1109/SCM.2017.7970698.

[4] Slobodskoi A.L., Terebkova T.A., Garin A.K. Digital education and the new technological generation: Demand for new content in learning // Наука о данных: мат. межд. научно-практ. конф., Санкт-Петербург, 5–7 февраля 2020 / СПбГЭУ, СПб., 2020. С. 287–289.

[5] Pokrovskaia N.N. Global and Local Regulating Approach for Sustainable Development // Sustainable Manufacturing, 2012. С. 287-292. doi: 10.1007/978-3-642-27290-5_45.

[6] Arrow K.J. Social Choice and Individual Values. New Haven and London: Yale University Press, 1951.

[7] Brusakova I. Cognitive Technologies Of Information Managements Of Business Processes Of The Digital Enterprises // Int. J. Adv. Inf. Sci. Technol. 2016. №5 (1). С. 73–76.

[8] Cappelli L., D'Ascenzo F., Ababkova M. Yu., Leontyeva V. L., Pokrovskaia N. N. Digital communication tools and knowledge creation processes for enriched intellectual outcome – experience of short-term E-learning courses during pandemic // Future Internet. 2021. Vol. 13 (2). doi: 10.3390/fi13020043.

[9] Ababkova M. Yu., al Haj Bara B. The impact of branding on consumer awareness // PR and advertising technologies in modern society. Engineers of senses: Transformation of competencies and global challenges of the communication industry, 2021. СПб.: СПбПУ, 2021. С. 14–18.

[10] Указ Президента РФ от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности РФ". http://publication.pravo.gov.ru/Document/View/0001202205010023

[11] Ababkova M.Yu., Leontieva V.L. Metaphor-Based Research For Studying Russian And Chinese Students' Perception Of The University // Europ. Proc. Soc. Behavioural Sc. EpSBS. 2020. Vol. 98. С. 89–98.