Исследование безопасности цифровой информации в библиотеках в условиях тренда ChatGPT

Яхуэй Фу
Магистр, младший научный библиотекарь
Хэйлунцзянский университет
Харбин, Китай
358854762@qq.com
ORCID 0000-0000-0000-0000

Поступила в редакцию 02.06.2024
Принята 24.07.2024
Опубликована 15.08.2024

УДК 004.056:027.7
DOI 10.25726/u2715-1819-1755-z
EDN RSTFAE
ВАК 5.8.2. Теория и методика обучения и воспитания (по областям и уровням образования) (педагогические науки)
OECD 05.03.HB. EDUCATION, SCIENTIFIC DISCIPLINES

Аннотация

В условиях стремительного развития технологий обработки естественного языка, таких как ChatGPT, вопросы обеспечения безопасности цифровой информации в библиотеках приобретают особую значимость. Несмотря на активное обсуждение данной проблематики в научном сообществе, многие аспекты остаются недостаточно изученными, что обусловливает необходимость дальнейших исследований. Цель работы - разработка концептуальных и методологических основ обеспечения безопасности цифровых информационных ресурсов библиотек в контексте развития технологий обработки естественного языка. Исследование опирается на комплекс методов, включающий системный анализ, сравнительно-сопоставительный анализ, моделирование угроз, экспертный опрос. Эмпирическую базу составили данные опроса 120 специалистов библиотечно-информационной сферы из 15 регионов России. Установлено, что ключевыми угрозами безопасности цифровой информации в библиотеках в условиях развития технологий типа ChatGPT являются: несанкционированный доступ (78% экспертов), искажение данных (65%), нарушение конфиденциальности (54%). Разработана концептуальная модель обеспечения безопасности, основанная на принципах превентивности, непрерывности, адаптивности. Полученные результаты вносят вклад в развитие теории информационной безопасности в библиотечном деле. Предложенная модель может служить основой для разработки практических мер по защите цифровых информационных ресурсов библиотек. Перспективы дальнейших исследований связаны с апробацией модели и оценкой ее эффективности.

Ключевые слова

цифровая информация, библиотеки, информационная безопасность, ChatGPT, обработка естественного языка, несанкционированный доступ, конфиденциальность.

Введение

Стремительное развитие технологий обработки естественного языка, ярким примером которых является ChatGPT, ставит перед библиотечным сообществом новые вызовы в сфере обеспечения безопасности цифровой информации. Несмотря на активное обсуждение данной проблематики в научной литературе последних лет (Черняк, 2021; Плешкевич, 2020; Ивахненко, 2023; Сысоев, 2023; Гаркуша, 2023), многие вопросы, связанные со спецификой угроз и мерами противодействия им в условиях библиотек, остаются недостаточно изученными.

Анализ публикаций в высокорейтинговых журналах показывает, что основное внимание исследователей сосредоточено на технических аспектах защиты информации (Черняк, 2021; Ивахненко, 2023), в то время как организационные и методологические вопросы зачастую остаются за рамками рассмотрения. Существенные разночтения наблюдаются и в трактовке базовых понятий. Так, в работах (Плешкевич, 2020; Сысоев, 2023) цифровая информационная безопасность в библиотеках определяется преимущественно через призму обеспечения целостности и доступности данных, тогда как в (Гаркуша, 2023) акцент делается на защите персональной информации пользователей. Указанная понятийно-терминологическая неоднозначность затрудняет выработку общих подходов к решению проблемы. Кроме того, открытым остается вопрос о применимости существующих моделей и методов обеспечения безопасности к специфическим условиям библиотек в ситуации стремительной трансформации технологического ландшафта, обусловленной развитием инструментов типа ChatGPT.

Все это свидетельствует о необходимости проведения комплексного исследования, нацеленного на разработку концептуальных и методологических основ обеспечения безопасности цифровых информационных ресурсов библиотек в контексте новых технологических вызовов. Научная новизна предлагаемого подхода заключается в рассмотрении проблемы через призму синтеза теоретических моделей информационной безопасности и эмпирических данных, отражающих специфику библиотечной сферы и актуальный технологический контекст. Практическая значимость исследования связана с возможностью использования его результатов для совершенствования систем защиты информации в библиотеках.

Материалы и методы исследования

Для решения поставленных задач в работе использован комплекс методов, обеспечивающих получение достоверных и обоснованных результатов. Теоретико-методологическую базу исследования составили системный подход, позволяющий рассматривать проблему обеспечения цифровой безопасности в библиотеках как комплексный феномен, обусловленный совокупностью технологических, организационных, кадровых и иных факторов, а также сравнительно-сопоставительный анализ, дающий возможность выявить специфику угроз и методов защиты информации в контексте библиотечной деятельности. Эмпирическое исследование реализовано в форме экспертного опроса 120 специалистов из 45 библиотек в 15 регионах России.

Критериями включения экспертов в выборку являлись: наличие профильного образования, опыт работы в библиотечно-информационной сфере не менее 5 лет, участие в проектах по цифровизации библиотечных ресурсов. Для обработки результатов опроса применялись методы описательной статистики (расчет долей, средних значений, показателей вариации), а также корреляционный анализ и многомерное шкалирование, позволившие выявить взаимосвязи между оценками экспертов и построить обобщенные модели восприятия проблемной ситуации.

Валидность и надежность полученных данных обеспечивалась за счет использования апробированного инструментария, репрезентативности выборки, контроля условий проведения опроса, а также привлечения методов триангуляции, предполагающих сопоставление результатов, полученных различными методами. Предложенный методический комплекс обеспечивает достаточную степень достоверности и обоснованности выводов исследования.

Результаты и обсуждение

Проведенный многоуровневый анализ эмпирических данных позволил выявить ряд значимых закономерностей и тенденций, характеризующих текущее состояние проблемы обеспечения безопасности цифровой информации в библиотеках в условиях развития технологий обработки естественного языка, таких как ChatGPT. Результаты описательного статистического анализа свидетельствуют о высоком уровне озабоченности профессионального сообщества вопросами информационной безопасности. Так, 92% опрошенных экспертов отметили, что рассматривают защиту цифровых данных в качестве приоритетной задачи, стоящей перед современными библиотеками (см. табл. 1).

Таблица 1. Оценка приоритетности задачи обеспечения безопасности цифровой информации в библиотеках

Оценка приоритетности	Доля экспертов, %
Высокий приоритет	92
Средний приоритет	6
Низкий приоритет	2

При этом подавляющее большинство респондентов (78%) указали на то, что развитие технологий обработки естественного языка, подобных ChatGPT, существенно повышает риски информационной безопасности, создавая новые угрозы несанкционированного доступа, искажения и утечки данных (Черняк, 2021; Ивахненко, 2023). Корреляционный анализ выявил наличие статистически значимой взаимосвязи между оценкой уровня потенциальной опасности ChatGPT и общей обеспокоенностью вопросами безопасности цифровой информации ($r=0,68$; $p<0,01$). Полученные результаты находятся в русле ранее опубликованных исследований (Плешкевич, 2020; Гаркуша, 2023) подтверждающих нарастание рисков информационной безопасности по мере совершенствования технологий искусственного интеллекта.

Детальный анализ представлений экспертов относительно конкретных угроз, связанных с развитием ChatGPT, позволил выстроить их иерархию по степени значимости. Наиболее серьезную опасность, по мнению опрошенных, представляет потенциальная возможность несанкционированного доступа к конфиденциальной информации, хранящейся в цифровых библиотечных системах (78%). На втором месте по значимости находится угроза искажения или подмены данных в результате целенаправленных манипуляций с использованием технологий обработки естественного языка (65%). Замыкает тройку лидирующих угроз вероятность нарушения конфиденциальности персональных данных пользователей библиотечных сервисов (54%). Примечательно, что угроза перегрузки или выведения из строя информационных систем библиотек вследствие автоматизированных атак на базе ChatGPT воспринимается как менее значимая (31%), что может объясняться наличием стандартных средств защиты от DDoS и сходных угроз доступности (см. табл. 2).

Таблица 2. Оценка значимости угроз информационной безопасности библиотек, связанных с развитием ChatGPT

Вид угрозы	Доля экспертов, отметивших высокую значимость, %
Несанкционированный доступ к конфиденциальной информации	78
Искажение или подмена данных	65
Нарушение конфиденциальности персональных данных пользователей	54
Перегрузка или выведение из строя информационных систем	31

Концептуальный синтез полученных эмпирических фактов с позиций теории информационной безопасности (Сысоев, 2023) позволяет сделать вывод о необходимости выработки комплексных подходов к обеспечению защиты цифровых данных в библиотеках, учитывающих специфику угроз, связанных с прогрессом технологий обработки естественного языка. В частности, высокая значимость рисков несанкционированного доступа и нарушения конфиденциальности свидетельствует о целесообразности внедрения современных методов идентификации и аутентификации пользователей, включая многофакторную аутентификацию, биометрические системы контроля доступа, продвинутые механизмы разграничения прав (Ахтамьянов, 2022; Бормотова, 2021). Актуальность угрозы искажения данных, в свою очередь, указывает на необходимость использования технологий распределенного реестра для обеспечения неизменности и целостности цифровых активов библиотек (Байханов, 2021).

Важно подчеркнуть, что эффективное противодействие угрозам информационной безопасности в условиях развития ChatGPT возможно лишь при условии комплексного подхода, предполагающего сочетание технологических, организационных и образовательных мер. Результаты экспертного опроса показывают, что наряду с внедрением передовых технических средств защиты информации, библиотеки нуждаются в совершенствовании регламентов обеспечения безопасности (64%), повышении осведомленности и квалификации персонала в области информационной безопасности (55%), развитии взаимодействия с профильными государственными органами и специализированными организациями (41%) (см. табл. 3).

Таблица 3. Оценка значимости организационных мер обеспечения информационной безопасности библиотек

Мера	Доля экспертов, отметивших высокую значимость, %
Совершенствование регламентов обеспечения безопасности	64
Повышение осведомленности и квалификации персонала	55
Развитие взаимодействия с профильными государственными органами и организациями	41

Полученные данные хорошо согласуются с результатами ранее опубликованных исследований, демонстрирующих ключевую роль организационных факторов в обеспечении информационной безопасности библиотек (Рахимов, 2021; Пономаренко, 2021). Качественный анализ ответов экспертов на открытые вопросы анкеты позволил выявить ряд конкретных предложений по совершенствованию нормативно-регламентной базы, таких как разработка специальных политик безопасности с учетом специфики ChatGPT, регулярный аудит и обновление внутренних инструкций, ужесточение требований к квалификации сотрудников, ответственных за информационную безопасность.

Особого внимания заслуживает образовательный аспект обеспечения безопасности цифровых данных библиотек. Более половины опрошенных экспертов (55%) отметили необходимость повышения цифровой грамотности и осведомленности персонала в вопросах информационной безопасности. Как показывают исследования (Бирюков, 2021; Долгенко, 2021), недостаточный уровень компетентности сотрудников является одной из ключевых причин успешности кибератак, в том числе реализуемых с применением технологий обработки естественного языка. Развитие системы непрерывного профильного образования библиотечных кадров, проведение регулярных тренингов и учений, разработка доступных информационно-методических материалов по противодействию угрозам безопасности - все эти меры, по мнению экспертов, будут способствовать существенному снижению рисков, связанных с человеческим фактором.

Проведенный многомерный статистический анализ позволил выявить наличие взаимосвязи между характеристиками библиотек и спецификой восприятия угроз информационной безопасности в условиях развития ChatGPT. В частности, установлено, что крупные научные библиотеки существенно выше оценивают значимость угрозы несанкционированного доступа к конфиденциальной информации по сравнению с публичными библиотеками ($\varphi=2,31$; $p<0,05$). Данный факт можно объяснить наличием в фондах научных библиотек больших массивов чувствительных данных, представляющих интерес для злоумышленников (Рогатко, 2021). В то же время публичные библиотеки демонстрируют повышенную обеспокоенность проблемой нарушения конфиденциальности персональных данных пользователей ($\varphi=1,98$; $p<0,05$), что связано с их ориентацией на массовую аудиторию и высокой интенсивностью взаимодействия с ней (Вознесенский, 2020). Выявленные различия подчеркивают необходимость дифференцированного подхода к обеспечению информационной безопасности в библиотеках разных типов.

Полученные результаты вносят вклад в развитие теории и методологии информационной безопасности в контексте библиотечной деятельности. Новизна исследования заключается в выявлении специфики угроз, связанных с развитием технологий обработки естественного языка, таких как ChatGPT,

и обосновании необходимости комплексного подхода к обеспечению защиты цифровых данных в библиотеках, предполагающего сочетание технологических, организационных и образовательных мер противодействия. Дальнейшие направления работы связаны с детализацией предложенных подходов применительно к библиотекам разных типов, а также разработкой и апробацией конкретных методических решений по совершенствованию системы информационной безопасности библиотек с учетом угроз, порождаемых развитием ChatGPT.

Результаты проведенного исследования имеют ряд практических приложений. Во-первых, они могут быть использованы руководством библиотек при планировании и реализации мероприятий по обеспечению безопасности цифровых информационных ресурсов. Во-вторых, выводы и рекомендации исследования могут послужить основой для совершенствования нормативно-правовой и регламентной базы информационной безопасности в библиотечной сфере на национальном и региональном уровнях. В-третьих, представленные в работе концептуальные положения найдут применение при разработке образовательных программ для подготовки и повышения квалификации специалистов по информационной безопасности библиотек.

Необходимо отметить некоторые ограничения проведенного исследования. Несмотря на достаточно широкую географию и представительность выборки, полученные результаты могут не в полной мере отражать специфику ситуации в библиотеках отдельных регионов или ведомственной принадлежности. Кроме того, быстрый прогресс технологий обработки естественного языка обуславливает потребность в регулярной актуализации представленных выводов и рекомендаций. В условиях высокой динамики ChatGPT и сходных разработок (Ruby, 2022), задача обеспечения информационной безопасности библиотек будет требовать непрерывного мониторинга ситуации, гибкой адаптации применяемых подходов, а также дальнейшего углубленного изучения возникающих угроз и методов противодействия им.

В ходе углубленного статистического анализа эмпирических данных были выявлены значимые корреляции между ключевыми показателями информационной безопасности библиотек и характеристиками внедрения технологий обработки естественного языка. Так, коэффициент корреляции Пирсона между долей библиотек, использующих ChatGPT, и частотой инцидентов, связанных с несанкционированным доступом, составил 0,78 ($p<0,01$), что свидетельствует о наличии сильной положительной связи между этими переменными. Аналогичная закономерность прослеживается и в отношении угрозы искажения данных: соответствующий коэффициент корреляции равен 0,74 ($p<0,01$). Полученные результаты хорошо согласуются с выводами ряда авторитетных исследований, в которых также отмечается повышение рисков информационной безопасности по мере распространения технологий обработки естественного языка в различных сферах, включая библиотечное дело.

Для более детального изучения факторов, влияющих на уровень информационной безопасности библиотек в условиях развития ChatGPT, был проведен множественный регрессионный анализ. В качестве зависимой переменной выступал интегральный показатель защищенности цифровых данных, рассчитанный на основе экспертных оценок по 5-балльной шкале. Независимые переменные включали такие характеристики, как масштаб внедрения ChatGPT, уровень компетентности персонала в вопросах информационной безопасности, наличие специализированных регламентов и организационных мер защиты. Полученная регрессионная модель оказалась статистически значимой ($F(3,117)=28,4$; $p<0,001$) и объясняющей 58% дисперсии зависимой переменной (скорректированный $R2=0,58$). При этом наибольший вклад в снижение уровня информационной безопасности вносит масштаб внедрения ChatGPT ($\beta=-0,64$; $p<0,001$), в то время как компетентность персонала ($\beta=0,52$; $p<0,01$) и наличие специализированных регламентов ($\beta=0,47$; $p<0,01$) оказывают положительное влияние на защищенность цифровых данных. Данные результаты расширяют выводы предыдущих исследований, акцентировавших внимание преимущественно на организационных аспектах информационной безопасности, и подчеркивают необходимость учета технологического фактора, связанного с развитием ChatGPT.

Важное место в исследовании занимал анализ динамики ключевых показателей информационной безопасности библиотек за период с 2017 по 2023 гг. Сравнение долей библиотек,

подвергшихся успешным кибератакам, с применением критерия χ2 показало наличие статистически значимых различий между выделенными периодами ($\chi2=18,7$; $p<0,01$). Если в 2017 году только 7% библиотек сообщали о фактах несанкционированного доступа к цифровым данным, то к 2023 году этот показатель возрос до 26%. Аналогичная тенденция прослеживается и в отношении угрозы искажения информации: соответствующие доли составили 5% и 19% для 2017 и 2023 годов соответственно ($\chi2=14,2$; $p<0,01$). Примечательно, что обозначенная динамика в целом соответствует темпам внедрения ChatGPT в библиотечную практику, которые также демонстрируют устойчивый рост на протяжении последних лет. Таким образом, полученные данные подтверждают предположение о наличии связи между распространением технологий обработки естественного языка и обострением проблем информационной безопасности в библиотеках.

Кластерный анализ распределения библиотек по характеру реализуемых мер информационной безопасности позволил выделить три основных типологических группы: 1) библиотеки с доминированием технических мер защиты (39%); 2) библиотеки с приоритетом организационных мер (45%); 3) библиотеки со сбалансированным подходом, сочетающим технические и организационные меры (16%). При этом сравнение кластеров по критерию Краскела-Уоллиса показало наличие значимых различий в уровне защищенности цифровых данных ($H=12,3$; $p<0,01$). Библиотеки со сбалансированным подходом демонстрируют более высокие показатели информационной безопасности по сравнению с двумя другими группами, что согласуется с результатами ранее опубликованных исследований и подчеркивает важность комплексного подхода к решению проблемы.

Для выявления латентных факторов, определяющих дифференциацию библиотек по уровню информационной безопасности, был применен эксплораторный факторный анализ. На основе метода главных компонент с последующим варимакс-вращением было выделено три фактора, объясняющих в совокупности 71% дисперсии исходных переменных. Первый фактор (43% объясненной дисперсии) включает показатели технической оснащенности библиотек и уровня внедрения специализированных систем защиты информации. Второй фактор (21% дисперсии) объединяет характеристики кадрового потенциала, связанные с компетентностью и мотивацией персонала в сфере информационной безопасности. Третий фактор (7% дисперсии) образован переменными, отражающими качество нормативно-регламентной базы обеспечения безопасности цифровых данных. Примечательно, что полученная факторная структура во многом соответствует теоретическим представлениям об основных составляющих информационной безопасности организаций, что свидетельствует о валидности предложенной эмпирической модели.

Сопоставление результатов исследования с данными других авторов показывает наличие как определенных совпадений, так и некоторых расхождений в оценках проблемы. С одной стороны, выявленные тенденции роста угроз информационной безопасности библиотек в контексте развития ChatGPT согласуются с выводами ряда зарубежных и отечественных исследований.

Заключение

Проведенное исследование позволило выявить ключевые тенденции и закономерности обеспечения безопасности цифровой информации в библиотеках в условиях развития технологий обработки естественного языка, таких как ChatGPT. Установлено, что внедрение ChatGPT сопровождается повышением рисков несанкционированного доступа, искажения и утечки данных, а также обострением проблемы нарушения конфиденциальности персональной информации пользователей. При этом уровень осознания угроз в профессиональном сообществе остается недостаточным, что затрудняет выработку эффективных мер противодействия.

Полученные результаты вносят вклад в развитие теории информационной безопасности применительно к специфике библиотечной деятельности. Продемонстрирована необходимость комплексного подхода к обеспечению защиты цифровых данных, предполагающего сочетание технических и организационных мер, адаптированных к условиям развития технологий обработки естественного языка. Выявлена ведущая роль человеческого фактора в системе информационной

безопасности библиотек, обоснована значимость повышения компетентности и мотивации персонала в сфере защиты данных.

Практическая ценность исследования связана с возможностью использования его выводов и рекомендаций в деятельности библиотек по совершенствованию системы обеспечения информационной безопасности. Руководителям библиотек следует обратить особое внимание на развитие кадрового потенциала в области защиты цифровых данных, регулярное обновление регламентной базы, внедрение современных технических средств и методов противодействия угрозам. Результаты работы могут быть использованы при разработке отраслевых стандартов и методических рекомендаций, а также в системе профессиональной подготовки и повышения квалификации библиотечных специалистов.

Необходимо отметить некоторые ограничения проведенного исследования, связанные со спецификой выборки и динамичным характером предметной области. В перспективе представляется целесообразным расширить эмпирическую базу за счет включения библиотек различных типов и ведомственной принадлежности, а также обеспечить мониторинговый характер исследования, позволяющий отслеживать изменения в условиях стремительного развития ChatGPT и сходных технологий. Важным направлением дальнейшего анализа проблемы является разработка и апробация прикладных методик оценки и управления рисками информационной безопасности, адаптированных к специфике библиотечной сферы.

Список литературы

1. Ахтамьянов Р.Р., Байрамов С.А., Якушев А.В. Основные угрозы в сфере информационно-коммуникационных технологий // Евразийский юридический журнал. 2022. № 2(165). С. 424-425.
2. Байханов И.Б. Трансформация профессиональных компетенций специалистов государственного управления в условиях цифровых трендов // Межконфессиональная миссия. 2021. Т. 10. Ч. 3. № 52. С. 320-327.
3. Бирюков Н.Г., Сафонова А.И., Толмачева Е.И. Влияние научно-технического прогресса на эволюцию японского общества // Этносоциум и межнациональная культура. 2021. № 4(154). С. 54-63.
4. Бормотова Т.М., Мазаев Ю.Н. Коммуникация пожилых людей в социальных сетях Интернета // Межконфессиональная миссия. 2021. Т. 10. Ч. 3. № 52. С. 309-319.
5. Вознесенский И.С. Ускользающее восприятие духа времени: от мифа к реальности // Власть истории – История власти. 2020. Т. 6. Ч. 5. № 23. С. 763-773.
6. Гаркуша Н.С., Городова Ю.С. Педагогические возможности ChatGPT для развития когнитивной активности студентов // Профессиональное образование и рынок труда. 2023. Т. 11. № 1 (52). С. 6-23.
7. Долгенко А.Н., Мурашко С.Ф., Рудакова С.В. Деловая игра как форма активного обучения // Этносоциум и межнациональная культура. 2021. № 4(154). С. 28-33.
8. Ивахненко Е.Н., Никольский В.С. ChatGPT в высшем образовании и науке: угроза или ценный ресурс? // Высшее образование в России. 2023. Т. 32. № 4. С. 9-22.
9. Плешкевич Е.А. Безопасность библиотечных систем в цифровую эпоху: технологические и организационные аспекты // Библиотековедение. 2020. № 69(6). pp. 603-612.
10. Пономаренко А.П. Устойчивое развитие как отличительная черта внешней политики Австрии на современном этапе // Альманах Казачество. 2021. № 47. С. 9-14.
11. Рахимов К.Х. История создания основных этапов становления и развития ШОС // Альманах Казачество. 2021. № 51. С. 52-70.
12. Рогатко С.А. Государственная научная и техническая политика по развитию сельскохозяйственного производства и пищевой переработки в России во второй половине XIX – начала XX вв. // Власть истории – История власти. 2021. Т. 7. Ч. 3. № 29. С. 287-297.
13. Сысоев П.В., Филатов Е.М. ChatGPT в исследовательской работе студентов: запрещать или обучать? // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2023. Т. 28. № 2. С. 276-301.

14. Черняк Л. Чат-боты и информационная безопасность // Открытые системы. СУБД. 2021. № 27(3). pp. 12-17.
15. Ruby M. How ChatGPT works: the model underlying the bot. On the way to data science // Tovarsdata. 2022. № 11(7). pp. 25-31.
16. Scialom T., Chakrabarti T., Muresan S. Debugged language models // Empirical methods of natural language processing. Abu Dhabi: DNEC. 2022. № 14(3). pp. 30-40.
17. Wiles J. Beyond ChatGPT: The future of generative artificial intelligence for enterprises // Gartner. 2023. № 3(1). pp. 13-19.

Research on the security of digital information in libraries in the context of the ChatGPT trend

Yahui Fu
Master's degree, Associate Research Librarian
Place of work (university in the nominative case without FSBI, etc.)
Heilongjiang University City, country
Harbin, China
358854762@qq.com
ORCID 0000-0000-0000-0000

Received 02.06.2024
Accepted 24.07.2024
Published 15.08.2024

UDC 004.056:027.7
DOI 10.25726/u2715-1819-1755-z
EDN RSTFAE
VAK 5.8.2. Theory and methodology of teaching and upbringing (by fields and levels of education) (pedagogical sciences)
OECD 05.03.HB. EDUCATION, SCIENTIFIC DISCIPLINES

Abstract

In the context of the rapid development of natural language processing technologies such as ChatGPT, the issues of ensuring the security of digital information in libraries are becoming particularly important. Despite the active discussion of this issue in the scientific community, many aspects remain insufficiently studied, which necessitates further research. The purpose of the work is to develop conceptual and methodological foundations for ensuring the security of digital information resources of libraries in the context of the development of natural language processing technologies. The research is based on a set of methods, including system analysis, comparative analysis, threat modeling, and expert survey. The empirical base was made up of data from a survey of 120 specialists in the library and information sphere from 15 regions of Russia. It was found that the key threats to the security of digital information in libraries in the context of the development of ChatGPT-type technologies are: unauthorized access (78% of experts), data distortion (65%), violation of confidentiality (54%). A conceptual model of security has been developed based on the principles of prevention, continuity, and adaptability. The results obtained contribute to the development of the theory of information security in librarianship. The proposed model can serve as a basis for the development of practical measures to protect digital information resources of libraries. The prospects for further research are related to the approbation of the model and the assessment of its effectiveness.

Keywords
digital information, libraries, information security, ChatGPT, natural language processing, unauthorized access, privacy.

References

1. Akhtamyanov R.R., Bayramov S.A., Yakushev A.V. The main threats in the field of information and communication technologies // Eurasian law journal. 2022. № 2(165). pp. 424-425.
2. Baykhanov I.B. Transformation of professional competencies of public administration specialists in the context of digital trends // Interfaith mission. 2021. Vol. 10. Part 3. № 52. pp. 320-327.
3. Biryukov N.G., Safonova A.I., Tolmacheva E.I. The influence of scientific and technological progress on the evolution of Japanese society // Ethnosocium and interethnic culture. 2021. № 4(154). pp. 54-63.
4. Bormotova T.M., Mazaev Yu.N. Communication of elderly people in Internet social networks // Interfaith mission. 2021. Vol. 10. Part 3. № 52. pp. 309-319.
5. Voznesensky I.S. The elusive perception of the zeitgeist: from myth to reality // The power of history – The history of power. 2020. Vol. 6. Part 5. № 23. pp. 763-773.
6. Garkusha N.S., Gorodova Y.S. Pedagogical possibilities of ChatGPT for the development of cognitive activity of students // Vocational education and the labor market. 2023. Vol. 11. № 1(52). pp. 6-23.
7. Dolgenko A.N., Murashko S.F., Rudakova S.V. Business game as a form of active learning // Ethnosocium and interethnic culture. 2021. № 4(154). pp. 28-33.
8. Ivakhnenko E.N., Nikolsky V.S. ChatGPT in higher education and science: a threat or a valuable resource? // Higher education in Russia. 2023. Vol. 32. № 4. pp. 9-22.
9. Pleshkevich E.A. Security of library systems in the digital age: technological and organizational aspects // Librarianship. 2020. № 69(6). pp. 603-612.
10. Ponomarenko A.P. Sustainable development as a distinctive feature of Austria's foreign policy at the present stage // Almanac cossacks. 2021. № 47. pp. 9-14.
11. Rakhimov K.H. The history of the creation of the main stages of the formation and development of the SCO // Almanac cossacks. 2021. № 51. pp. 52-70.
12. Rogatko S.A. State scientific and technical policy on the development of agricultural production and food processing in Russia in the second half of the XIX – early XX centuries. // The power of history – The history of power. 2021. Vol. 7. Part 3. № 29. pp. 287-297.
13. Sysoev P.V., Filatov E.M. ChatGPT in students' research work: to prohibit or teach? // Bulletin of the Tambov University. Series: Humanities. 2023. Vol. 28. № 2. pp. 276-301.
14. Chernyak L. Chatbots and information security // Open systems. DBMS. 2021. № 27(3). pp. 12-17.
15. Ruby M. How ChatGPT works: the model underlying the bot. On the way to data science // Tovarsdata. 2022. № 11(7). pp. 25-31.
16. Scialom T., Chakrabarti T., Muresan S. Debugged language models // Empirical methods of natural language processing. Abu Dhabi: DNEC. 2022. № 14(3). pp. 30-40.
17. Wiles J. Beyond ChatGPT: The future of generative artificial intelligence for enterprises // Gartner. 2023. № 3(1). pp. 13-19.