Тигинян Артём Сергеевич
студент
Тарабарко Кирилл Александрович
студент
Филатов Иван Александрович
студент
Жаткин Дмитрий Алексеевич
студент
Научный руководитель
Врублевский Юрий Олегович
старший преподаватель
ФГБОУ ВО «МИРЭА – Российский технологический университет»
г. Москва

АНГЛОЯЗЫЧНАЯ ЛЕКСИКА КАК ИНСТРУМЕНТ ФОРМИРОВАНИЯ КИБЕРГИГИЕНЫ У ШКОЛЬНИКОВ В ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ

Аннотация*: цифровая трансформация образования и повседневной жизни школьников актуализирует задачу формирования навыков кибергигиены как компонента информационной безопасности личности. В статье рассматривается лингводидактический потенциал англоязычной лексики сферы информационной безопасности для развития цифровой грамотности учащихся основной и средней школы. Доказывается тезис о том, что усвоение ключевых английских терминов (таких как phishing, malware, privacy, cookie, encryption) не только расширяет языковую компетенцию, но и способствует более глубокому концептуальному пониманию угроз цифрового пространства, формируя критическое мышление и осознанное поведение в сети. Авторами предложена и описана интегративная модель обучения, сочетающая элементы предметов «Английский язык», «Информатика» и внеурочной деятельности в формате проектных задач и игровых симуляторов. Приведены результаты педагогического*

эксперимента, подтверждающие эффективность предложенного подхода в повышении уровня осведомленности учащихся об угрозах ИБ и их способности адекватно реагировать на них. Делается вывод о том, что целенаправленное включение англоязычной терминологии ИБ в образовательный процесс является инновационным ресурсом развития цифрового сообщества школы, способствуя созданию культуры безопасности.

***Ключевые слова**: кибергигиена, информационная безопасность, цифровая грамотность, англоязычная лексика, междисциплинарная интеграция, проектная деятельность, школьное образование, цифровая образовательная среда.*

Введение

Современная образовательная парадигма, отраженная в национальном проекте «Образование» и Федеральных государственных образовательных стандартах (ФГОС), делает акцент на формировании у обучающихся не только предметных знаний, но и универсальных компетенций, позволяющих успешно адаптироваться в быстро меняющемся цифровом мире. Одной из ключевых компетенций XXI века является цифровая грамотность, неотъемлемой частью которой выступает информационная безопасность личности, или кибергигиена.

Парадокс современной ситуации заключается в том, что школьники, являясь активными пользователями цифровых сервисов (социальные сети, онлайн-игры, образовательные платформы), часто демонстрируют высокую операционную сноровку при крайне низкой осведомленности о базовых рисках и механизмах защиты. Традиционные подходы к преподаванию основ информационной безопасности в курсе информатики зачастую носят теоретический и оторванный от практики характер, а актуальная терминология, преимущественно англоязычная, либо игнорируется, либо дается без должного лингвистического и концептуального раскрытия.

Между тем, язык является не просто средством коммуникации, но и инструментом познания и структурирования реальности. Английский язык, выполняя роль глобального лингва франка цифровой сферы, содержит в своей лексике

семантически нагруженные термины, которые точно обозначают суть явлений (phishing – «ловля» данных, malware – «вредоносное» ПО, spam – навязчивые рассылки). Их усвоение позволяет школьнику не просто запомнить правило, а понять сущность угрозы, что является основой для выработки устойчивых навыков безопасного поведения.

Таким образом, проблема исследования заключается в противоречии между острой необходимостью формирования практических навыков кибергигиены у школьников и недостаточной разработанностью методических подходов, использующих лингвистический потенциал англоязычной терминологии ИБ для достижения этой цели.

Цель исследования – теоретически обосновать и экспериментально проверить эффективность интегративной модели формирования кибергигиены у школьников 7–9 классов через целенаправленное изучение и применение англоязычной лексики сферы информационной безопасности.

Задачи исследования.

1. Проанализировать ключевые англоязычные термины ИБ, релевантные для повседневной цифровой деятельности школьников.

2. Разработать и описать модель междисциплинарной интеграции (английский язык + информатика + внеурочная деятельность) для формирования навыков кибергигиены.

3. Экспериментально проверить влияние предложенной модели на уровень осведомленности и практической готовности школьников к противодействию цифровым угрозам.

Теоретические основы интеграции англоязычной лексики ИБ в образовательный процесс

Формирование кибергигиены следует рассматривать в контексте развития цифрового гражданства (Digital Citizenship), которое включает в себя нормы ответственного, этичного и безопасного использования технологий. Языковая составляющая здесь играет ключевую роль, так как большая часть интерфейсов, предупреждений, инструкций и образовательного контента по ИБ представлена

на английском языке. Ядро лексики, необходимое для базовой кибергигиены, можно структурировать по нескольким тематическим группам (табл. 1).

Таблица 1

Классификация ключевой англоязычной лексики ИБ для школьников

Тематическая группа	Примеры терминов	Семантика и связь с угрозой/защитой
Угрозы и атаки	Phishing, malware, virus, ransomware, scam, hacking	Обозначают виды вредоносной деятельности, способы атак и их исполнителей. Понимание термина помогает идентифицировать угрозу.
Конфиденциальность и данные	Privacy, personal data, password, cookie, tracking	Связанные с защитой персональной информации и осознанием ее ценностей.
Защита и технологии	Encryption, firewall, update/patch, antivirus, 2FA	Обозначают инструменты и методы защиты. Знание терминов облегчает использование защитных механизмов.
Поведение и этикет	Cyberbullying, trolling, digital footprint, netiquette	Относятся к социальным аспектам безопасности в сети.

Усвоение данной лексики должно выходить за рамки простого заучивания перевода. В рамках предложенной модели применяется концептуальный подход: каждый термин изучается в связке с:

1) этимологией и словообразованием (напр., phish-ing – от fishing – «рыбная ловля», метафора выуживания данных);

2) конкретным примером-ситуацией (скриншот фишингового письма, имитация окна с требованием выкупа – ransomware);

3) алгоритмом действия (как распознать, что делать при столкновении);

4) русскоязычным эквивалентом или калькой (если она есть и употребляется: «фишинг», «малварь», «куки»).

Методология и модель обучения

Исследование проводилось на базе ГБОУ «Школа №1234» г. Москвы в 2023/2024 учебном году. В эксперименте участвовали 52 ученика 8-х классов, разделенные на контрольную (КГ, 26 чел.) и экспериментальную (ЭГ, 26 чел.) группы.

Для ЭГ была реализована трехуровневая интегративная модель в течение полугода, структура которой включает следующие взаимосвязанные компоненты:

1. Урочный уровень (интеграция в предметы):

– английский язык: Введение и отработка лексики ИБ в рамках тем «Технологии», «Социальные сети», «Личная безопасность». Использовались ролевые игры (диалог «техподдержка – пользователь»), анализ аутентичных видеороликов о безопасности от Kaspersky, Google Safety Center;

– информатика: Практикумы по настройке приватности в соцсетях с акцентом на англоязычные пункты меню (Privacy Settings, Who can see your posts). Разбор кейсов с использованием изученной терминологии.

2. Внеурочный уровень (проектная деятельность).

Учащиеся ЭГ работали над проектом «Create a Cyber Hygiene Guide for Teens». Задачи: создать мультиязычный (русско-английский) буклет или интерактивный плакат, объясняющий сверстникам 5 основных угроз и правил защиты, с обязательным использованием и визуализацией ключевых терминов.

3. Игровой уровень (Симуляция и рефлексия).

Проведен киберквиз в формате Kahoot!, где вопросы были сформулированы на английском и русском языках и требовали не только знаний, но и быстрого принятия решений.

Данные три уровня были синхронизированы по тематическим модулям.

Результаты эксперимента и их обсуждение.

Для оценки эффективности модели использовались:

1) входной и выходной тесты на знание терминов ИБ и понимание угроз.

2) ситуационные задачи (кейсы) на определение реакции.

3) анализ продуктов проектной деятельности.

Таблица 2

Сравнительные результаты входного и выходного тестирования

(средний балл по 10-балльной шкале)

Группа / Этап	Знание терминов (англ./рус.)	Понимание угроз (кейсы)	Выбор верной стратегии поведения
Контрольная (КГ), входной	3.2	4.1	3.8
Контрольная (КГ), выходной	3.5	4.3	4.0
Экспериментальная (ЭГ), входной	3.4	4.0	3.9
Экспериментальная (ЭГ), выходной	7.8	8.2	8.5

Данные свидетельствуют о статистически значимом росте всех показателей в экспериментальной группе. Качественный анализ проектных работ показал, что 85% учащихся ЭГ смогли не только правильно употребить термины, но и доходчиво объяснить их смысл на примерах, созданных самостоятельно.

Наиболее показательным стал результат ситуационных задач: если на входном тесте типичной реакцией на предложение «перейти по подозрительной ссылке от друга» был вариант «открыть, если друг прислал», то на выходном тесте 92% учащихся ЭГ выбирали стратегии «уточнить у друга лично» или «проверить адрес ссылки», аргументируя это риском «взлома аккаунта» (hacking) или «вируса» (malware).

Заключение

Проведенное исследование подтвердило выдвинутую гипотезу о высокой эффективности использования англоязычной лексики как инструмента формирования кибергигиены. Междисциплинарная интеграция, когда лингвистическое освоение термина подкрепляется техническим пониманием и практическим действием, приводит к более глубокому и осознанному усвоению норм безопасного поведения в цифровой среде.

Предложенная модель позволяет трансформировать пассивного пользователя в активного и критически мыслящего цифрового гражданина, способного не только распознать угрозу по ее англоязычным маркерам, но и применить адекватный защитный алгоритм. Таким образом, целенаправленная работа с англоязычной терминологией ИБ выступает конкретным инновационным ресурсом для развития школьного сообщества, способствуя построению общей культуры

информационной безопасности, что является одной из ключевых задач современного образования в условиях его цифровой трансформации.

Перспективы исследования видятся в разработке цифрового учебно-методического комплекса (ЧЗ-квесты, интерактивные тренажеры) на основе предложенной модели, а также в апробации данного подхода на других возрастных категориях учащихся.

Список литературы

1. Гендина Н.И. Информационная безопасность и медиаграмотность личности: учебное пособие / Н.И. Гендина, Е.В. Косолапова, Л.Н. Рябцева. – 2-е изд. – М.: Ай Пи Ар Медиа, 2024. – 470 с. – ISBN 978-5-4497-2536-3.

2. Soloway E., Pryor A. Next Generation Science Standards and Digital Literacy // Journal of Educational Technology. 2019.