УДК 004.056

АНАЛИЗ УРОВНЯ ОСВЕДОМЛЕННОСТИ О КИБЕРБЕЗОПАСНОСТИ СРЕДИ ИНОСТРАННЫХ СТУДЕНТОВ

Канте Д., **Эссака Н.К.Ш.**
Научный руководитель - Колегова О.А.
Университет ИТМО
dickokante86@gmail.com

Введение

Кибербезопасность становится критически значимой областью в условиях цифровизации образования и повсеместного распространения онлайн-сервисов. Иностранные студенты российских вузов находятся в группе повышенного риска: языковой барьер, незнание локальных схем мошенничества и отсутствие адаптированных инструкций создают условия для успешных фишинговых атак, взломов аккаунтов и финансовых потерь [1]. Установление связи между уровнем цифровой грамотности, реальным опытом инцидентов и запрашиваемыми форматами помощи имеет большое практическое значение, поскольку позволяет целенаправленно разрабатывать меры профилактики с учётом актуальных потребностей студентов. Изучение данной проблемы особенно важно в контексте роста числа цифровых сервисов и усиления требований к защите персональных данных [2].

Основная часть

Исследование базируется на результатах эмпирических данных, собранных путём опроса иностранных студентов Университета ИТМО (опрашивались студенты 1–3 курсов разных факультетов). Результаты опроса, во-первых, показывают реальную распространённость киберинцидентов. Установлено, что 59% респондентов лично сталкивались или знают о случаях взлома аккаунтов среди знакомых. Наиболее частыми каналами атак являются Telegram, ВКонтакте, фейковые сайты, фишинговые ссылки, а также телефонные звонки мошенников. При этом 85 % опрошенных не сообщали о случаях взлома в России, что косвенно указывает на отсутствие доверия к институциям или незнание порядка действий [1].

Во-вторых, была проанализирована самооценка уровня знаний в области кибербезопасности. Средний самооценочный уровень знаний составил 3,3 балла из 5, при этом 36 % респондентов оценили свои знания на 2 балла и ниже. Студенты младших курсов демонстрируют более низкие показатели по сравнению со старшекурсниками. В открытых вопросах респонденты предложили конкретные меры поддержки: проведение лекций с разбором реальных кейсов и звонков мошенников, создание памяток и чек-листов на русском и английском языке, обучение использованию менеджеров паролей и двухфакторной аутентификации, а также языковую поддержку.

Ссылаясь на данные опроса и литературу по изучаемой теме, мы предполагаем, что в том случае, когда причиной непонимания являются языковые и культурные барьеры, необходима адаптация контента и перевод инструкций на родные языки студентов [1]. Однако для повышения интереса к теме кибербезопасности наиболее эффективными представляются симуляции фишинговых атак, разбор реальных звонков мошенников и игровые чек-листы [2].

Выводы

Проведённый опрос, посвящённый анализу уязвимости иностранных студентов к киберугрозам, позволил выявить основные каналы атак и наиболее востребованные

форматы помощи. Разработанная методика оценки уровня осведомлённости позволила создать двухкомпонентную модель профилактики, сочетающую языковую адаптацию и практико-ориентированные тренинги.

Литература

1. Zhang K., Arunasalam A. International Students and Scams: At Risk Abroad [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2510.18715 (Дата обращения 18.02.2026).

2. Lui A., Womack C., Orton P. Collaborative Online International Learning as a Third Space to Improve Students‘ Awareness of Cybersecurity // Journal of International Education. 2025.Vol. 12, no. 3. P. 45–62.