УДК 004.056

Ахметова А.Ф.,
студент,
1 курс, специальность «Реклама и связи с общественностью»
Казанский государственный энергетический университет
Россия, г. Казань
Шевко Н.Р.,
кандидат экономических наук, доцент,
доцент кафедры «Информационные технологии и интеллектуальные системы»
Казанский государственный энергетический университет
Россия, г. Казань

ФЕНОМЕН ЛОЖНОЙ ЦИФРОВОЙ КОМПЕТЕНТНОСТИ В КОНТЕКСТЕ КИБЕРГИГИЕНЫ СОВРЕМЕННОГО СТУДЕНТА

Аннотация: *В данной статье рассматриваются особенности кибербезопасности и кибергигиены студентов. Автор анализирует противоречие между высоким уровнем технической грамотности студентов и их уязвимостью перед современными киберугрозами. Вводится и раскрывается понятие «ложной цифровой компетентности» как одного из главных факторов риска при применении методов социальной инженерии. На основе проведенного мини-опроса выделяются типичные ошибки поведения студентов в сети и предлагаются пути повышения культуры информационной безопасности.*

Ключевые слова: *кибербезопасность, кибергигиена, студенты, цифровая грамотность, социальная инженерия, ложная компетентность.*

Annotation: *This article examines the features of cybersecurity and cyber hygiene among student youth. The author analyzes the contradiction between the high level of technical literacy of students and their vulnerability to modern cyber threats. The concept of "false digital competence" is introduced and explored as one of the primary risk factors in the application of social engineering methods. Based on a conducted mini-survey, typical behavioral errors of students online are identified, and methods to enhance information security culture are proposed.*

Keywords: *cybersecurity, cyber hygiene, students, digital literacy, social engineering, false competence.*

В условиях тотальной цифровизации многих жизненных сфер, особенно высшего образования, кибербезопасность приобретает статус базового навыка жизнедеятельности. Переход учебных процессов в онлайн-формат, использование облачных сервисов для хранения студенческих работ и популярность безналичных расчетов делают студенческую среду одной из наиболее привлекательных мишеней для киберпреступников. Согласно Федеральному закону № 149-ФЗ «Об информации...» [2], защита информации является обязанностью всех субъектов информационных отношений. Однако на практике защищенность конечных пользователей - студентов, остается на критически низком уровне.

Центральным понятием в данном контексте выступает кибергигиена. Под кибергигиеной понимается совокупность регулярно выполняемых пользователем правил и привычек, направленных на минимизацию рисков утечки данных, заражения вредоносным ПО и потери контроля над личными аккаунтами. В отличие от узкоспециализированной информационной безопасности (ИБ), кибергигиена доступна и обязательна для каждого человека. Современные первокурсники относятся к поколению Z, которое в социологии часто называют «Digital Natives» (цифровыми аборигенами). Студенты не представляют своей жизни без гаджетов, проводя в смартфонах и

компьютерах значительную часть дня. В связи с этим в студенческой среде формируется тезис №1: высокий уровень технической грамотности (умение быстро пользоваться приложениями и находить информацию) не равен высокому уровню культуры информационной безопасности.

Это противоречие порождает феномен ложной цифровой компетентности. Студенты уверены: если они способны самостоятельно установить сложную программу или настроить VPN, то они автоматически защищены от угроз. Возникающая психологическая самоуверенность приводит к снижению когнитивного контроля (внимательности).

К основным киберугрозам, с которыми сталкивается молодежь, относятся:

- Фишинг (поддельные сайты вузов, стипендиальных программ, интернет-магазинов);

- Кража аккаунтов в мессенджерах и социальных сетях;

- Утечки конфиденциальных данных в открытый доступ (согласно ФЗ № 152 «О персональных данных» [1], биометрические и паспортные данные требуют особой защиты).

Здесь подтверждается тезис №2: основным вектором атак на студентов является социальная инженерия, эксплуатирующая эмоциональные триггеры. Студенты - эмоционально восприимчивая группа, часто находящаяся в условиях нехватки времени и стресса (сессия, дедлайны). Преступники манипулируют чувством FOMO (страх упущенной выгоды) - например, предлагая «сливы ответов на экзамен» или фейковые гранты за быстрый переход по ссылке. В состоянии спешки студент совершает ошибку. Классические работы по ИБ (например, В.А. Галатенко [3] и В.Ф. Шаньгин [4]) всегда подчеркивали главенствующую роль «человеческого фактора» в системе защиты. Чтобы оценить уровень кибергигиены на практике, в рамках исследования был проведен анонимный мини-опрос среди студентов 1 курса (в выборку вошли 30 человек).

Приведём данные опроса. Из 30 первокурсников 70 % (21 из 30) используют один пароль (или слегка изменённый) для почты, учебного портала и соцсетей. 85 % (26 из 30) подключаются к открытому WI-FI в кафе или вузе и при этом заходят в личные кабинеты и банковские приложения. Лишь 35 % (11 из 30) включили двухфакторную аутентификацию везде, где это возможно. Полученные цифры подтверждают тезис о ложной компетентности: чем привычнее студент обращается с гаджетами, тем менее осторожным он становится. Эту самоуверенность можно назвать «цифровой смелостью». Для противодействия этим угрозам необходим комплекс мер. Технические способы известны: менеджеры паролей, антивирус на телефоне, двухфакторная аутентификация. Но сами по себе они проблему не решают. Нужно развивать у студентов критическое мышление - умение проверить ссылку, не открывать подозрительный файл. Обычные памятки на стенах и брошюры почти не работают, что подтверждает практика преподавания. Студенту мало прочитать правило - его надо вовлечь. Вуз может проводить учебные фишинговые рассылки (конечно, в образовательных целях), квесты, игровые сценарии, форумы, вовлекать студентов через различные учебные практики. Тогда кибергигиена станет такой же рутинной привычкой, как мытьё рук. Следует отметить ограничения проведённого исследования. Выборка составила 30 человек, опрашивались только студенты первого курса одного вуза. Полученные результаты носят предварительный характер и не могут быть распространены на всех студентов, однако они указывают на устойчивую тенденцию, требующую внимания.

Итог таков: связь между «цифровой самоуверенностью» и реальной незащищённостью прослеживается чётко. Студент отлично владеет программами и настройками, но оказывается беспомощным перед психологическим давлением и социальной инженерией. Выход - не в пересказе правил, а в систематических практических занятиях, которые тренируют внимательность и самоконтроль.

Использованные источники:

1. Российская Федерация. Законы. О персональных данных : Федеральный закон № 152-ФЗ : принят Государственной Думой 8 июля 2006 года : одобрен Советом Федерации 19 июля 2006 года. – Москва, 2006. – 15 с.

2. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ : принят Государственной Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года. – Москва, 2006. – 21 с.

3. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко ; под редакцией В. Б. Бетелина. – Москва : ИНТУИТ, 2012. – 264 с.

4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. – Москва : Форум : ИНФРА-М, 2014. – 416 с.

5. Азанбаева, А. Б. Кибербезопасность / А. Б. Азанбаева, А. А. Беспалова // Потенциал российской экономики и инновационные пути его реализации : материалы Всероссийской научно-практической конференции студентов и аспирантов, Омск, 17–18 апреля 2023 года. В 2 частях. Часть I / под редакцией Т. В. Ивашкевич, А. И. Ковалева, О. В. Фрик, О. Г. Конюковой. – Омск : Омский государственный технический университет, 2023. – С. 15–18.

6. Артамонов, В. А. Кибербезопасность в условиях цифровой трансформации социума / В. А. Артамонов // Цифровая социология. – 2022. – Т. 5, № 2. – С. 44–51. – DOI: 10.26425/2658-347X-2022-5-2-44-51.

7. Салганова, Е. И. Цифровая грамотность студентов: компетентностный подход / Е. И. Салганова, Л. Б. Осипова // Экономические и социальные перемены: факты, тенденции, прогноз. – 2023. – Т. 16, № 1. – С. 227–240. – DOI: 10.15838/esc.2023.1.85.12.

8. Брусенцева, В. А. Проблемы обеспечения безопасности детей и подростков в сети Интернет / В. А. Брусенцева, Е. В. Шаповалов //

Информационная безопасность регионов. – 2021. – № 2 (43). – С. 31–35. – URL: https://www.elibrary.ru/item.asp?id=46573456 (дата обращения: 08.05.2026).