УДК 004.05

ОЦЕНКА УРОВНЯ ОСВЕДОМЛЕННОСТИ СТУДЕНТОВ О КИБЕРУГРОЗАХ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кряжева Е. В.,

к.псих.н., доцент,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Ларин С. Э.,

студент,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Суходольский А. В.,

студент,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Аннотация.

В статье рассматривается проблема информационной безопасности. Анализируются возможные киберугрозы: программы-вымогатели, дипфейки, фишинговые сообщения, рассылка вредоносных файлов через мессенджеры. Рассматриваются нормативно-технические акты РФ, в которых отражены основные определения и термины по информационной безопасности. Авторами разработан опросник, который позволяет оценить уровень осведомленности студентов вуза об основных аспектах информационной безопасности. В конце представлены выводы по проделанной работе.

Ключевые слова: информационная безопасность, киберугрозы, фишинг, двухфакторная аутентификация, защита данных.

ASSESSMENT OF STUDENTS' AWARENESS OF CYBER THREATS AND INFORMATION SECURITY

Kryazheva E. V.,
Candidate of Psychological Sciences, Associate Professor,
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia
Larin S.E.
student,
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia
Sukhodolsky A.V.
student,
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia

Annotation.
The article discusses the problem of information security. Possible cyber threats are analyzed: ransomware, deepfakes, phishing messages, sending malicious files via instant messengers. The normative and technical acts of the Russian Federation, which reflect the main definitions and terms of information security, are considered. The authors have developed a questionnaire that allows you to assess the level of awareness of university students about the main aspects of information security. At the end, conclusions on the work done are presented.
Keywords: information security, cyber threat, phishing, two-factor authentication, data protection.

В эпоху стремительного развития цифровых технологий нельзя не упомянуть о вызовах, которые встают перед пользователями в области информационной безопасности. На сегодняшний день тенденция к росту

цифровизации практически во всех сферах жизни сопровождается увеличением рисков, связанных с угрозами. Автоматизация процессов и повышение удобства повседневной жизни открывают новые возможности для злоумышленников и порождают новые киберугрозы. Недостаточная осведомленность пользователей об актуальных интернет-угрозах может привести к негативным последствиям.

На 2024 год одной из наиболее значимых угроз в сфере кибербезопасности в России остаются атаки с использованием программ-вымогателей [5]. Также активно применяется искусственный интеллект для создания более убедительных фишинговых сообщений и дипфейков, что существенно усложняет их распознавание [6]. Такие угрозы особенно опасны для пользователей с низким уровнем цифровой грамотности.

Перед изучением терминологии, затрагивающей информационную безопасность, следует отметить, что в Российской Федерации использование информационных технологий и обеспечение информационной безопасности регламентируются основными законодательными и нормативно-правовыми актами [7].

Перейдем к более подробному изучению понятия информационной безопасности и дадим его определение. Информационная безопасность – совокупность мер, направленных на защиту информации от утечек и несанкционированного доступа. Рассмотрим определения согласно ГОСТ Р 50922—2006 «Защита информации. Основные термины и определения» [3]:

Защита информации представляет собой комплекс мер, ориентированный на предотвращение утечек защищаемой информации. Защита информации от утечки направлена на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа.

Безопасность информации – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность. Ключевые понятия информационной безопасности определены в ГОСТ Р

50.1.056–2005 «Техническая защита информации. Основные термины и определения» [2]. Также одним из ведущих стандартов является ГОСТ Р ИСО/МЭК 27002-2021 Информационные технологии. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИИ. Свод норм и правил применения мер обеспечения информационной безопасности. Стандарт является руководством для организаций по разработке и внедрению мер информационной безопасности. После изучения всех необходимых определений установленных ГОСТ, рассмотрим, что из себя представляют современные интернет-угрозы.

Сейчас одной из самых актуальных угроз в сфере информационной безопасности стала новая схема мошенничества, связанная с рассылкой вредоносных файлов через мессенджеры. МВД России предупредило пользователей о том, что фотографии не могут иметь формат исполняемых файлов APK и ни в коем случае такие файлы скачивать нельзя [4]. Данный вид угрозы направлен на то, чтобы принудить пользователя открыть и установить вредоносный файл. Это создает риск утечки конфиденциальной информации, несанкционированного доступа к устройству и последующего использования в мошеннических действиях.

Современные интернет-угрозы демонстрируют не только хитрость методов злоумышленников, но и важность осведомленности пользователей о своевременных мерах защиты от подобных угроз. С этой целью было проведено исследование, направленное на изучение практических вопросов и оценку уровня осведомленности студентов КГУ им. К.Э. Циолковского о ключевых аспектах информационной безопасности и их отношения к интернет-угрозам. В рамках исследования был разработан и проведен опросник, направленный на изучение отношения обучаемых к данной проблеме и уровня их подготовки к противодействию интернет–угрозам. Выборка включала 65 респондентов, гендерные предпочтения не учитывались. При анализе полученных результатов использовался частотный анализ.

Опрос включал 14 вопросов, направленных на оценку:

1. уровня знаний об основных угрозах в информационной безопасности;
2. используемых мер защиты (пароли, антивирусы, двухфакторная аутентификация);
3. частоты случаев утраты данных или взлома аккаунтов.

Инструменты для анализа: Microsoft Excel для обработки и визуализации данных.

Основной блок опроса был направлен на оценку знаний респондентов по тематике информационной безопасности, а также их практик в области защиты информации.

Для более компактного представления результатов все 14 диаграмм с вопросами были систематизированы в три ключевых блока:

1. осведомленность об угрозах;
2. используемые методы защиты;
3. опыт инцидентов.

Рисунки 1–3, представленные ниже, иллюстрируют результаты по этим блокам.

Рис. 1 – Уровень знаний студентов об основных правилах информационной безопасности (составлено авторами)

Из рисунка 1 видно, что большинство студентов (71%) заявили, что знают основные правила информационной безопасности. Еще 26% знакомы в общих чертах и лишь 3% не владеют знаниями.

Рис. 2 – Какие меры принимают студенты чаще всего (составлено авторами)

Из рисунка 2 видно, что 49% студентов используют антивирусное программное обеспечение, а 44% применяют двухфакторную аутентификацию. Лишь 7% указали что не предпринимают никаких мер для защиты своих данных.

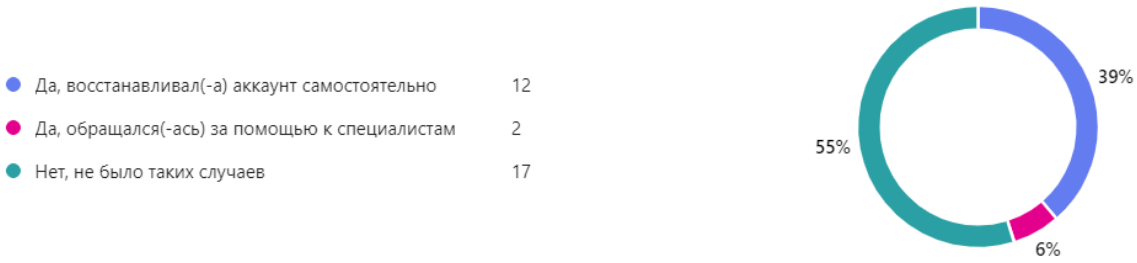

Рис. 3 – Опыт потери личной информации и взлома у студентов (составлено авторами)

На рисунке 3 видно, что большинство студентов (55%) не сталкивались с потерей личной информации или взломом, что свидетельствует о высоком уровне безопасности их аккаунтов. Однако 39% отметили, что им приходилось

самостоятельно восстанавливать свои аккаунты, а 6% обращались за помощью к специалистам.

Все полученные результаты свидетельствуют о необходимости повышения уровня знаний студентов о способах предотвращения киберугроз, а также фокусировки на формирование навыков, направленных на предотвращение подобных инцидентов в будущем.

Библиографический список:

1. Баланов, А. Н. Комплексная информационная безопасность: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 400 с. — ISBN 978-5-507-49250-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/414947 (дата обращения: 03.12.2024).
2. ГОСТ Р 50.1.056–2005 – «Техническая защита информации. Основные термины и определения»: [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200044768
3. ГОСТ Р 50922–2006 – «Защита информации, Основные термины и определения. Общие положения о защите информации»: [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200058320
4. МВД предупредило о рассылке вирусов под видом фотографий через Telegram // rbc URL: https://www.rbc.ru/technology_and_media/20/10/2024/67143c4e9a794720531cbc74 (дата обращения: 06.12.2024).
5. Названа главная киберугроза для российских компаний в 2024 году // газета.ru URL: https://www.gazeta.ru/social/news/2024/02/06/22273669.shtml (дата обращения: 30.11.2024).
6. Новогодние обещания: как сделать 2024 год безопасным // kaspersky daily URL: https://www.kaspersky.ru/blog/cybersecurity-resolutions-2024/36782/ (дата обращения: 30.11.2024).
7. Справочник законодательства РФ в области информационной безопасности // Хабр URL: https://habr.com/ru/articles/432466/ (дата обращения: 06.12.2024).

Оригинальность 77%