

УДК 004.056

***ОСВЕДОМЛЁННОСТЬ СТУДЕНТОВ МЕДИЦИНСКИХ ВУЗОВ О
КИБЕРБЕЗОПАСНОСТИ В МЕДИЦИНЕ.***

Яньшина Ю. В.,

студентка,

ФГБОУ ВО «Ижевская государственная медицинская академия»,

Ижевск, Россия

Шигаева К. А.,

студентка,

ФГБОУ ВО «Ижевская государственная медицинская академия»,

Ижевск, Россия

Толмачёв Д.А.,

д.м.н., доцент,

ФГБОУ ВО «Ижевская государственная медицинская академия»,

Ижевск, Россия

Аннотация. Статья посвящена исследованию уровня осведомлённости студентов медицинских вузов о защите данных пациентов и кибербезопасности в медицине. Основной целью исследования является определение текущего уровня знаний студентов о важных аспектах защиты данных и киберугрозах, с которыми они могут столкнуться в будущей профессиональной деятельности. Для достижения этой цели было проведено анкетирование, включающее 15 вопросов, направленных на оценку общего уровня осведомлённости, понимания технических аспектов кибербезопасности и осознания этических проблем. Полученные результаты показывают существующие пробелы в знаниях студентов, что подчёркивает важность повышения осведомлённости студентов о вопросах кибербезопасности. В заключение статьи представлены рекомендации по развитию навыков и знаний студентов в области защиты данных пациентов и кибербезопасности.

Ключевые слова: кибербезопасность, защита данных, студенты, медицина, анкетирование, этика.

***STUDENT AWARENESS
MEDICAL UNIVERSITIES ON PATIENT DATA PROTECTION AND
CYBERSECURITY IN MEDICINE.***

Yanshina Yu. V.,

student,

Izhevsk State Medical Academy,

Izhevsk, Russia

Shigaeva K. A.,

student,

Izhevsk State Medical Academy,

Izhevsk, Russia

Tolmachev D.A.,

MD, Associate Professor,

Izhevsk State Medical Academy,

Izhevsk, Russia

Annotation. The article is devoted to the study of the level of awareness of medical university students about patient data protection and cybersecurity in medicine. The main purpose of the study is to determine the current level of knowledge of students about important aspects of data protection and cyber threats that they may encounter in their future professional activities. To achieve this goal, a questionnaire was conducted, including 15 questions, aimed at assessing the general level of awareness, understanding of technical aspects of cybersecurity, and awareness of ethical issues. The results show the existing gaps in students' knowledge, which underlines the importance of raising students' awareness of cybersecurity issues. The article concludes with recommendations for developing students' skills and knowledge in patient data protection and cybersecurity.

Key words: cybersecurity, data protection, students, medicine, questionnaires, ethics.

Актуальность. В условиях активного внедрения цифровых технологий в медицину, включая использование электронных медицинских карт, телемедицины и дистанционных консультаций, вопросы защиты персональных данных пациентов и обеспечения кибербезопасности приобретают особую актуальность [1, 10].

Конфиденциальная информация пациентов включает в себя персональные данные, историю болезни, результаты анализов и другие сведения, которые необходимо защищать. Утечка такой информации или её несанкционированное использование могут привести к серьёзным последствиям, затрагивающим права пациентов, репутацию медицинских учреждений и безопасность данных в целом [2, 3].

Рост числа киберинцидентов в сфере здравоохранения подчёркивает необходимость разработки и соблюдения чётких стандартов кибербезопасности. В последние годы частота таких инцидентов увеличивается, и медицинская информация становится одной из самых привлекательных целей для киберпреступников, поскольку утечка данных может повлечь за собой как репутационные, так и юридические риски для медицинских учреждений [4, 5].

В этом контексте особенно важно обеспечить надлежащую подготовку будущих специалистов в области медицины, чтобы минимизировать угрозы кибератак и повысить уровень защиты данных [9].

Цель. Проанализировать осведомленность студентов медицинских вузов о кибербезопасности в медицине.

Материалы и методы. Исследование основано на анкетировании 175 студентов 4-го курса Ижевской государственной медицинской академии для оценки уровня их осведомлённости в области защиты данных пациентов и кибербезопасности. Анкета из 15 вопросов охватывает три ключевых направления: общий уровень осведомлённости, технические аспекты

Дневник науки | www.dnevniknauki.ru | СМИ Эл № ФС 77-68405 ISSN 2541-8327

кибербезопасности и этические вопросы. Вопросы были представлены в виде закрытых вариантов ответов, что позволило оценить как знания, так и уверенность студентов в своих знаниях. Анкетирование проводилось в формате онлайн-опроса, что обеспечило анонимность и широкую выборку. Для анализа использовались методы описательной статистики, что позволило выявить средние значения и наиболее распространённые ответы, а также провести сравнительный анализ по каждой тематической категории для последующей разработки рекомендаций.

Полученные результаты. В ходе исследования было выявлено, что 85,0% респондентов считают защиту данных пациентов в своей будущей профессиональной деятельности крайне важной задачей, тогда как 10,0% респондентов отметили, что это скорее важно, и лишь 5,0% не считают защиту данных приоритетным аспектом. Эти результаты свидетельствуют о высокой степени осведомлённости студентов о важности обеспечения конфиденциальности данных пациентов как фундаментального элемента их будущей медицинской практики. Более того, такое распределение мнений подчёркивает преобладание среди студентов этического и профессионального подхода к вопросам кибербезопасности, что имеет ключевое значение в условиях цифровизации здравоохранения и растущих угроз нарушения конфиденциальности.

В результате анализа уровня знаний о конфиденциальных данных было установлено, что 60,0% опрошенных студентов уверены в том, какие именно сведения относятся к категории конфиденциальных в медицине. 30,0% студентов указали, что имеют лишь частичное представление об этом, а 10,0% затруднились ответить на вопрос, что может свидетельствовать о недостаточной осведомлённости в данной области. Уровень осведомлённости студентов в вопросах, касающихся конфиденциальных данных может повлиять на их готовность соблюдать высокие стандарты кибербезопасности в условиях растущих цифровых рисков и угроз.

Исследование осведомлённости студентов о санкциях за нарушение конфиденциальности данных пациентов показало, что только 28,0% респондентов полностью осведомлены о мерах ответственности, предусмотренных за такие нарушения. 40,0% студентов указали, что имеют лишь частичное представление о санкциях, а 32,0% вообще не знакомы с возможными юридическими и профессиональными последствиями. Эти данные подчёркивают существующий пробел в подготовке студентов к вопросам юридической ответственности в сфере медицины и кибербезопасности. Недостаток знаний о санкциях может снизить значимость соблюдения конфиденциальности в глазах будущих специалистов, особенно в условиях, когда нарушения безопасности данных могут привести к серьёзным последствиям для пациента и подорвать доверие к медицинскому учреждению.

Интересно отметить, что 75,0% респондентов оценивают вероятность утечки данных пациентов как высокую, 18,0% считают риски умеренными, и лишь 7,0% считают их низкими. Эти результаты указывают на высокую степень осознания студентами серьёзности проблемы защиты данных в условиях цифровизации и частых кибератак на медицинские учреждения. Такое восприятие рисков отражает не только осведомлённость студентов о потенциальных угрозах, но и их готовность подходить к этой проблеме с должным вниманием, что является важной предпосылкой для формирования более безопасной практики в будущем.

Что касается уровня информированности студентов о киберрисках в области медицины показало, что 40,0% опрошенных хорошо осведомлены о таких опасностях, как вирусы, хакерские атаки и другие виды угроз информационной безопасности, которые могут повлиять на защиту данных пациентов и работу медицинских организаций. 30,0% респондентов заявили, что имеют лишь общее представление о киберугрозах, а ещё 30,0% признались, что совсем не разбираются в этой теме. Эти результаты указывают на необходимость более глубокого изучения вопросов кибербезопасности и возможных рисков в Дневник науки | www.dnevniknauki.ru | СМИ Эл № ФС 77-68405 ISSN 2541-8327

процессе обучения медицинских специалистов. Понимание потенциальных киберугроз в медицине играет ключевую роль для будущих специалистов, поскольку цифровизация здравоохранения и рост объёма электронных данных повышают уязвимость системы к кибератакам и несанкционированному доступу. Недостаточный уровень осведомлённости может привести к тому, что молодые специалисты будут хуже подготовлены к предотвращению и быстрому реагированию на инциденты, связанные с информационной безопасностью [7].

Также в ходе исследования был задан вопрос: «Насколько вы оцениваете уровень защищённости медицинских компьютерных систем?», и результаты распределились следующим образом: 35,0% студентов оценили защищённость медицинских компьютерных систем как высокую, 40,0% считают, что уровень защиты находится на среднем уровне, и 25,0% респондентов считают, что системы не защищены должным образом. Эти данные свидетельствуют о том, что значительная часть студентов ощущает наличие рисков и недостатков в защите медицинских компьютерных систем. Несмотря на то, что треть опрошенных считает уровень безопасности удовлетворительным, каждый четвёртый студент указывает на потенциальные угрозы из-за недостаточной защиты данных.

Наиболее частыми кибератаками, по мнению респондентов, являются утечки данных и фишинговые сайты (54,5%). Это отражает понимание студентами того, что персональная информация пациентов и данные медицинских учреждений наиболее уязвимы для внешних угроз, направленных на получение конфиденциальной информации.

При этом 30,0% респондентов отметили угрозу вирусных атак, включая вредоносное ПО и трояны, которые могут нарушить работу медицинских систем и привести к потере или компрометации данных. Остальные 15,5% указали на другие виды кибератак, такие как атаки типа «отказ в обслуживании» (DDoS), которые могут парализовать доступ к медицинским данным, что критически важно в условиях лечебного процесса.

Кроме того, респондентов спросили, какие методы защиты данных им известны. Наиболее известными методами оказались шифрование информации (45,0%) и использование надёжных паролей (40,0%). Меньшая часть опрошенных (15,0%) упомянула брандмауэры и антивирусное ПО как важные инструменты защиты. Эти данные подчёркивают необходимость более глубокого изучения различных методов защиты, особенно таких, как двухфакторная аутентификация (2FA) и регулярное обновление программного обеспечения, чтобы расширить знания студентов о комплексной защите медицинских данных [6].

Анализ значимости соблюдения этических норм при работе с данными пациентов показал, что 78,0% респондентов отметили высокую важность этического подхода к защите конфиденциальной информации, 15,0% оценили значимость как среднюю, а 7,0% не придали этому большого значения. Полученные результаты показывают, что большинство респондентов воспринимают защиту данных пациентов не только как техническую, но и как этическую задачу, демонстрируя осознание своей будущей моральной ответственности за сохранность конфиденциальной информации.

По вопросу о целях соблюдения конфиденциальности мнения респондентов распределились следующим образом: 50,0% студентов отметили, что главным является защита прав пациентов, подчеркнув важность сохранения личной информации в интересах их безопасности и доверия к медицинской организации. При этом 30,0% участников назвали соблюдение законодательства основной причиной сохранения конфиденциальности, что указывает на их понимание юридических обязательств, регулирующих сферу здравоохранения. 20,0% выбрали другие причины, такие как соблюдение профессиональной этики и создание безопасной рабочей среды. Эти результаты свидетельствуют о том, что студенты осознают многогранность значимости конфиденциальности, включая как моральные, так и правовые аспекты [8].

Вывод. В ходе исследования была проведена оценка уровня информированности студентов о значимости защиты персональных данных пациентов и кибербезопасности в их будущей медицинской практике. Результаты опроса показали, что респонденты в целом осознают важность обеспечения конфиденциальности информации, однако были выявлены пробелы в знаниях о возможных санкциях за нарушения и киберугрозах. Студенты продемонстрировали готовность к этичному обращению с данными, но необходимость повышения уровня знаний о методах защиты остаётся актуальной. В условиях продолжающейся цифровизации здравоохранения и роста числа кибератак на медицинские учреждения важно, чтобы будущие специалисты не только обладали теоретическими знаниями, но и умели применять их на практике для защиты данных.

Рекомендуется внедрять специализированные курсы и семинары, посвящённые вопросам конфиденциальности, юридической ответственности и этики. Регулярные тренинги и доступные информационные ресурсы о киберугрозах и методах защиты данных помогут сформировать у студентов ответственное отношение к информации. Обсуждение реальных случаев нарушения конфиденциальности позволит развивать критическое мышление и понимание серьёзности проблемы. Установление партнёрских отношений между образовательными учреждениями и медицинскими организациями для обмена опытом и передовыми практиками может значительно улучшить подготовку студентов к реальным вызовам в области защиты данных.

Библиографический список:

1. Айдынлар, А., Мави, А., Кютюкчу, Э. и др. Осведомленность и уровень цифровой грамотности среди студентов, получающих медицинское образование / А. Айдынлар, А. Мави, Э. Кютюкчу, и др. // BMC Med Educ 24, 38 (2024). [Электронный ресурс]. — Режим доступа — URL: <https://rdcu.be/dY0AB> (Дата обращения: 04.11.2024)

2. Гусев А.С. О проекте «Цифровое здравоохранение» / А.С. Гусев // [Электронный ресурс]. — Режим доступа — URL: <http://www.kmis.ru/blog/o-proekte-tsifrovoye-zdravookhranenie> (Дата обращения: 04.11.2024)
3. Ибрафиллов А. КИБЕРБЕЗОПАСНОСТЬ В МЕДИЦИНЕ: ЗАЩИТА ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ ДАННЫХ / А. Ибрафиллов // Холодная наука. 2024. №6. URL: <https://cyberleninka.ru/article/n/kiberbezopasnost-v-meditsine-zaschita-elektronnyh-meditsinskih-dannyh> (Дата обращения: 04.11.2024).
4. Лебедев Г.С., Шадеркин И.А., Фомина И.В. Эволюция интернеттехнологий в системе здравоохранения / Г.С. Лебедев, И.А. Шадеркин, И.В. Фомина // Журнал телемедицины и электронного здравоохранения. 2017. № 2. С. 64–78
5. Леванов В.М., Куцик Е.А. Информированность и мотивационные установки студентов медицинского вуза в отношении цифровой медицины – пятилетний тренд / В.М. Леванов, Е.А. Куцик // Медицинский альманах. 2019. № 1(58). С. 14-18.
6. Любаева Д. Ю. Правовые аспекты защиты персональных данных в медицинских учреждениях / Д.Ю. Любаева // Контентус. 2022. №9 (122). С. 57-63.
7. Малинина Е.В., Дубинкин В.А., Маркова Н.Ю., Кичко И.С. ПРИМЕНЕНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПРАКТИЧЕСКОМ ЗДРАВООХРАНЕНИИ / Е.В. Малинина, В.А. Дубинкин, Н.Ю. Маркова, И.С. // Вестник новых медицинских технологий. Электронное издание. 2024. №2. [Электронный ресурс]. — Режим доступа — URL: <https://cyberleninka.ru/article/n/primenenie-tsifrovyyh-tehnologiy-v-prakticheskom-zdravookhraneni> (дата обращения: 03.11.2024).
8. Минниханова, А. А., Гайсина Г. Ф., Толмачев Д. А. Влияние средств массовой информации на подрастающее поколение / А. А.

Минниханова, Г. Ф. Гайсина, Д. А. Толмачев // Colloquium-Journal. – 2019. – № 9-3(33). – С. 64-65.

9. Островик М.О., Кавешников А.В., Серебрякова В.Н. Информированность и отношение студенческой молодежи к цифровой медицине / М.О. Островик, А.В. Кавешников, В.Н. Серебрякова / Сибирский журнал клинической и экспериментальной медицины. 2020. № 35(3). С. 141-150
10. Рашитов Д.Р., Ибрагимов Д.И., Толмачев Д.А. ОСВЕДОМЛЕННОСТЬ СТУДЕНТОВ МЕДИЦИНСКИХ ВУЗОВ О ВЛИЯНИИ ЦИФРОВОЙ МЕДИЦИНЫ И ТЕЛЕМЕДИЦИНЫ НА СИСТЕМУ ЗДРАВООХРАНЕНИЯ / Д.Р. Рашитов, Д.И. Ибрагимов, Д.А. Толмачев / Медицинские науки – №10 – 2024. [Электронный ресурс]. — Режим доступа — URL: https://dnevniknauki.ru/images/publications/2024/10/medicine/Rashitov_Ibragimov_Tolmachev2.pdf (Дата обращения: 04.11.2024).

Оригинальность 75%