БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ЗДРАВООХРАНЕНИИ

Кузьмина П.О., студентка 4 курса,

Хало Л.А., к.э.н., доцент,

Волгоградский государственный медицинский университет, г. Волгоград, Россия

Аннотация. Кибербезопасность в сфере здравоохранения представляет собой крайне важный аспект для эффективного функционирования региональной и муниципальной экономики. Рост количества кибератак на медицинские учреждения, стремительное развитие технологий и увеличение объемов электронных медицинских данных создают новый вызов для защиты конфиденциальности и безопасности пациентов. В ходе исследования анализируются уязвимости медицинских организаций к киберугрозам и предлагаются меры по улучшению информационной безопасности.

Ключевые слова: кибербезопасность, здравоохранение, цифровые технологии, защита данных, уязвимость .

Кибербезопасность в здравоохранении играет важную роль, поскольку она обеспечивает защиту конфиденциальной информации пациентов и предотвращает несанкционированный доступ к электронным медицинским данным. Увеличение

объемов таких данных, а также внедрение новых технологий в медицинскую практику создают благоприятные условия для кибератак, которые могут привести к серьезным последствиям, включая компрометацию личной информации, финансовые потери и даже вред для здоровья пациентов. Кроме того, атаки на медицинские учреждения могут нарушить работу критически важных систем, что ставит под угрозу оказание медицинских услуг. Поэтому надежная киберзащита становится неотъемлемой частью функционирования здравоохранения, способствуя не только сохранению доверия пациентов, но и обеспечению безопасности и эффективности медицинской помощи в целом.

Чтобы оценить уровень киберугроз в секторе здравоохранения, в исследовании была собрана информация из различных источников: отчеты о кибератаках, публикации научных журналов, специализированные издания и исследования последних лет. Были учтены случаи хакерских атак, направленных на больницы и другие медицинские учреждения в разных странах, включая детали о времени, методах проведения атак и их последствиях. Обработанные данные позволили выявить определенные тенденции и составить представление о текущем уровне угроз в области кибербезопасности в здравоохранении.

Анализ текущей ситуации показывает, что кибератаки на медицинские учреждения участились, и 2021 год стал особенно показателен в этом плане. Многие из этих атак направлены на кражу личных данных пациентов и мошенничество с медицинской информацией. События, подобные атаке WannaCry, заставили многие организации пересмотреть свои подходы к киберзащите, и, согласно исследованиям, 75% опрошенных медицинских организаций решили увеличить свои инвестиции в эту сферу.

Однако проблема не ограничивается только кражей данных. Существуют и другие виды атак, такие как программы-вымогатели, DDoS-атаки и фишинг. Эти угрозы могут вызвать серьезные сбои в работе медицинских учреждений [1]. Например, террористическая атака на систему электронного здравоохранения в Ирландии в 2021 году продемонстрировала, какой хаос может возникнуть, если доступ к медицинским данным окажется под угрозой. В результате этой атаки многие больницы и клиники столкнулись с трудностями в предоставлении медицинской помощи [2].

Анализ последующих событий показывает, что кибератаки на медицинские организации продолжаются в 2023 году. Например, в США произошло значительное вторжение в систему электронных медицинских записей, которое затронуло миллионы пациентов. Доклады о данном инциденте подчеркивают, что были скомпрометированы не только личные данные, но и финансовая информация, что может иметь далеко идущие последствия для здоровья пациентов. В ответ на рост киберугроз некоторые организации начали внедрять технологии искусственного интеллекта для более эффективного обнаружения и предотвращения атак, что значительно повысило уровень защиты данных.

Прогнозы на 2024 год в области кибербезопасности в здравоохранении не внушают оптимизма. Количество атак на медицинские учреждения продолжает расти, и киберпреступники все чаще применяют сложные методы социальной инженерии для получения доступа к системам. Эксперты настоятельно рекомендуют сосредоточить внимание на обучении сотрудников, так как человеческий фактор остается одной из основных причин утечек данных. Кризис в кибербезопасности в здравоохранении требует не только внедрения новых технологий, но и изменения культуры безопасности внутри организаций [3]. Это необходимо для обеспечения надежной защиты личных и медицинских данных пациентов, что является приоритетом для современных медицинских учреждений.

В результате проведенного анализа текущих угроз и уязвимостей в системе кибербезопасности медицинских учреждений становится очевидным, что внедрение специфических мер по улучшению защиты данных является крайне необходимым. Основная цель данных мер заключается в создании надежной системы безопасности, которая будет защищать личную информацию пациентов и минимизировать последствия потенциальных кибератак.

Ключевые рекомендации, представленные в таблице 1, служат основой для формирования более устойчивой системы защиты, что позволяет медицинским организациям обеспечивать безопасность данных и защищать интересы пациентов. Кро ме того, важно активизировать сотрудничество между государственными органами, медицинскими учреждениями и технологическими компаниями для обмена информацией о новых угрозах и методах защиты.

Таблица 1 - Рекомендации по обеспечению кибербезопасности

Рекомендации
Описание
Обучение сотрудников

Проведение регулярных обучающих мероприятий по кибербезопасности для всех сотрудников	

Внедрение искусственного интеллекта	

Использование технологий искусственного интеллекта для постоянного мониторинга и опера	

Аудит системы	

Реализация плановых проверок информационных систем с целью выявления уязвимых мест	

Многофакторная аутентификация	

Внедрение системы многофакторной аутентификации для повышения уровня защиты	

Политика безопасности данных	

Создание и внедрение	строгих	протоколов упр

Таким образом, интеграция предложенных мер не только усилит уровень киберзащиты

в медицинских учреждениях, но и обеспечит безопасное оказание медицинских услуг, что в конечном итоге будет способствовать доверию пациентов и устойчивости организаций.

Литература

1. Исрафилов А. Кибербезопасность в медицине: Защита электронных медицинских данных // Холодная наука. 2024. № 6. С. 59 – 67. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-v-meditsine-zaschita-elektronnyh-meditsinskih-dannyh (дата обращения: 20.11.2024).

2. Мур, Г., Хуршид, З., Макдоннелл, Т. Устойчивость рабочей силы: безопасность пациентов и реакция персонала на кибератаку на системы ИКТ Национальной службы здравоохранения Ирландии // BMC Health Services Research. 2023. № 1112. С. 1–7. URL: https://rdcu.be/d0Sjj (дата обращения: 20.11.2024).

3. Соболева, С.Ю., Голиков, В.В., Тажибов, А.А. Информационные технологии в здравоохранении: особенности отраслевого применения // E-Management. 2021. № 2. С. 37 - 43. URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-v-zdravoohranenii-osobennosti-otraslevogo-primeneniya (дата обращения: 20.11.2024).