Удальцов К.Р. Кибербезопасность в здравоохранении: стратегии защиты медицинских данных и оборудования// Международный журнал информационных технологий и энергоэффективности.– 2024. –
Т. 9 № 5(43) с. 18–22

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

КИБЕРБЕЗОПАСНОСТЬ В ЗДРАВООХРАНЕНИИ: СТРАТЕГИИ ЗАЩИТЫ МЕДИЦИНСКИХ ДАННЫХ И ОБОРУДОВАНИЯ

Удальцов К.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: 2003.06.10kr@gmail.com

Данная статья обсуждает важность кибербезопасности в здравоохранении и стратегии защиты медицинских данных и оборудования от киберугроз. В контексте цифровизации здравоохранения и увеличения угроз кибератак, обеспечение безопасности медицинских информационных систем становится критически важным для сохранности данных пациентов и непрерывности медицинского ухода. Статья охватывает рост угроз, защиту медицинских данных, безопасность медицинского оборудования, развитие стратегий кибербезопасности, будущие вызовы и важность сотрудничества между стейкхолдерами. Она подчеркивает необходимость инвестирования в кибербезопасность, обучения персонала, соблюдения законодательства и принятия инновационных решений для обеспечения безопасности и надежности здравоохранения в эпоху цифровой трансформации.

Ключевые слова: Кибербезопасность, здравоохранение, медицинские данные, медицинское оборудование, киберугрозы, защита данных, кризисное управление, обучение персонала, законодательство, сотрудничество, инновации, безопасность пациентов, цифровизация, угрозы, стратегии защиты.

CYBERSECURITY IN HEALTHCARE: STRATEGIES FOR PROTECTING MEDICAL DATA AND EQUIPMENT

Udaltsov K.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: 2003.06.10kr@gmail.com

This article discusses the importance of cybersecurity in healthcare and strategies for protecting medical data and equipment from cyber threats. In the context of digitalization of healthcare and increasing threats of cyber attacks, ensuring the security of medical information systems is becoming critically important for the safety of patient data and continuity of medical care. The article covers the growth of threats, the protection of medical data, the security of medical equipment, the development of cybersecurity strategies, future challenges and the importance of cooperation between stakeholders. She emphasizes the need to invest in cybersecurity, train staff, comply with legislation, and make innovative decisions to ensure the safety and reliability of healthcare in an era of digital transformation.

Keywords: Cybersecurity, healthcare, medical data, medical equipment, cyber threats, data protection, crisis management, staff training, legislation, cooperation, innovation, patient safety, digitalization, threats, protection strategies.

Введение

В эпоху цифровизации здравоохранения, когда медицинские данные переносятся в онлайн-среду и медицинское оборудование становится все более сетевым, вопрос кибербезопасности становится жизненно важным. [1] Защита медицинских данных и оборудования от киберугроз становится приоритетом для обеспечения непрерывности медицинского ухода и предотвращения возможных угроз для пациентов и организаций здравоохранения.

1. **Рост угроз в здравоохранении:**

С каждым годом случаи кибератак на медицинские учреждения увеличиваются. Злоумышленники могут нацелиться на медицинские данные пациентов, шантажировать организации здравоохранения или даже нарушить работу медицинского оборудования. [2] Это создает серьезные угрозы как для конфиденциальности данных, так и для безопасности пациентов.

2. **Защита медицинских данных:**

Одним из ключевых аспектов кибербезопасности в здравоохранении является защита медицинских данных. [3] Организации должны строго соблюдать нормы безопасности, шифровать данные, устанавливать системы мониторинга и обучать персоналу правилам работы с конфиденциальной информацией.

3. **Безопасность медицинского оборудования:**

С развитием Интернета вещей (IoT) медицинское оборудование становится более уязвимым для кибератак. [4] Взлом медицинских устройств может привести к серьезным последствиям, включая неправильное лечение пациентов. Производители медицинского оборудования должны уделять особое внимание кибербезопасности, внедряя защитные механизмы и обновления.

4. **Развитие стратегий кибербезопасности:**

Для эффективной защиты медицинских данных и оборудования необходимо разработать комплексные стратегии кибербезопасности. [5] Это включает в себя постоянное обновление систем безопасности, обучение персонала, аудит безопасности и сотрудничество с киберспециалистами.

5. **Будущее кибербезопасности в здравоохранении:**

С увеличением объема медицинских данных, использованием искусственного интеллекта в медицине и расширением интернета вещей, вопросы кибербезопасности станут только более актуальными. [6] В будущем необходимо ожидать новых вызовов, таких как квантовые вычисления и биометрическая аутентификация, которые потребуют новых стратегий защиты.

6. **Важность сотрудничества и обмена информацией:**

Для эффективной борьбы с киберугрозами в здравоохранении необходимо усилить сотрудничество между медицинскими учреждениями, государственными органами,

киберспециалистами и производителями медицинского оборудования. Обмен опытом и информацией поможет создать более устойчивые системы защиты.[7]

7. Подготовка персонала:

Одним из ключевых моментов в обеспечении кибербезопасности в здравоохранении является обучение персонала. Все сотрудники медицинских учреждений должны быть осведомлены о рисках кибератак и знать основные правила безопасности, чтобы минимизировать уязвимости систем.

8. Регулирование и законодательство:

Законы и нормативные акты в области кибербезопасности играют важную роль в защите медицинских данных. [8] Государства должны разрабатывать строгие правила и стандарты для организаций здравоохранения и производителей медицинского оборудования, чтобы обеспечить соответствие требованиям безопасности.

9. Кризисное управление:

Подготовка к кибератакам и разработка планов кризисного управления являются неотъемлемой частью стратегии кибербезопасности в здравоохранении. Организации должны иметь четкие инструкции по реагированию на инциденты безопасности, включая изоляцию уязвимостей, восстановление данных и устранение угроз.

10. Обучение пациентов:

Важным аспектом обеспечения кибербезопасности в здравоохранении является обучение пациентов основам безопасности данных. Пациентам следует быть осведомленными о рисках киберугроз и методах защиты своих медицинских данных, чтобы предотвратить возможные атаки на их личную информацию.

11. Инновации в области кибербезопасности:

Развитие новых технологий, таких как блокчейн и квантовые вычисления, открывает новые возможности для улучшения кибербезопасности в здравоохранении. Интеграция инновационных решений может повысить защиту медицинских данных и оборудования, делая системы более надежными и устойчивыми к угрозам.

Заключение

Кибербезопасность в области здравоохранения остается одним из наиболее актуальных и важных вопросов в современном мире. Защита медицинских данных и оборудования требует комплексного подхода, включающего в себя технологические инновации, сотрудничество между стейкхолдерами, обучение персонала и пациентов, а также строгое соблюдение законодательства. Только совместными усилиями можно обеспечить безопасность и надежность здравоохранения в цифровой эпохе.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018". – 2018. – С. 149-149.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 590-595.
4. Красов А. В. и др. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры.
5. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2020. – №. 2. – С. 86-94.
6. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных//Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
7. Волкогонов В. Н. и др. Анализ безопасности wi-fi сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 270-275.
8. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.

References

1. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks //Regional Informatics"RI-2018". – 2018. – pp. 149-149.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Kazantsev A. A. et al. Creating and managing a Security Operations Center for effective use in real-world environments//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 590-595.
4. Krasov A.V. et al. Software implementation of intrusion prevention tools and network infrastructure anomalies.
5. Sakharov D. V. et al. Using mathematical forecasting methods to assess the load on the computing power of the IOT network //Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia". - 2020. – No. 2. – pp. 86-94.
6. Gelfand A.M. Methods of choosing stegocontainers for data transmission//Regional informatics and information security. – 2020. – pp. 260-262.
7. Volkogonov V. N. et al. Wi-fi network Security Analysis//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 270-275.

8. Budarny G. S. and others. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.