УДК 339.138

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ ЗДРАВООХРАНЕНИЯ

Н. И. Шандора

старший преподаватель, Белорусский государственный университет, г. Минск, Беларусь, shandoranatasha@tut.by

Данная статья посвящена важности роли информационной безопасности в сфере здравоохранения; выявлены основные особенности медицинской информации. В статье рассматриваются ключевые направления информационной безопасности в учреждениях, предоставляющих медицинские услуги, так как несанкционированный доступ к конфиденциальным данным пациентов может привести к серьезным последствиям. Определены основные факторы риска и угрозы информационной безопасности медицинских информационных систем, а также даны рекомендации по информационной безопасности в сфере здравоохранения.

Ключевые слова: информация; информационная безопасность; медицинские учреждения; программное обеспечение (ПО); медицинская информационная система (МИС); эшелонированная защита.

TOOLS TO PROMOTE A MEDICAL ORGANIZATION IN SOCIAL MEDIA

N. I. Shandora

senior lecturer, Belarusian State University, Minsk, Belarus, shandoranatasha@tut.by

This article is devoted to the importance of the role of information security in the field of healthcare, the main features of medical information are identified. The article discusses the key areas of information security in institutions providing medical services, as unauthorised access to confidential patient data can lead to serious consequences. The main risk factors and threats to information security of medical information systems are identified, and recommendations on information security in healthcare are given.

Keywords: information; information security; medical institutions; software; medical information system (MIS); echeloned security.

В условиях информатизации общества важным аспектом функционирования современной национальной информационной политики является обеспечение информационной безопасности и защиты субъектов информационных отношений.

Информационная безопасность в сфере здравоохранения является ключевым моментов в медицинской отрасли на современном этапе. Она предполагает комплекс мер по защите организаций от внешних и внутренних кибератак и обеспечению доступности медицинских услуг, правильной эксплуатации медицинских систем и оборудования, сохранения конфиденциальности и целостности данных пациентов, а также соблюдения отраслевых норм. Информационная безопасность в медицинском учреждении представляет собой целенаправленную деятельность персонала по достижению защищенности информационной среды учреждения.

Безопасная работа в области информационных технологий в медицинских организациях может быть достигнута только при помощи комплексного подхода применения различных мер, таких как организационные, программные и технические [1].

Выделяют основные направления кибербезопасности:

- сохранность целостности данных;
- конфиденциальность информации;
- обеспечение доступности.

Особенность медицинских данных сделали кибербезопасность в здравоохранении уникальной проблемой, так как большая часть персональных данных попадает под категорию врачебной тайны и имеют свою специфику:

- информация находится в распоряжении пациента;
- обработка медицинской документации должна происходить оперативно;
- различные сегменты медицинской информации чаще всего обрабатываются разными людьми (регистратор, медсестра, врач и т. д.) и др.

Еще одной проблемой создания некого единого подхода безопасности данных является то, что многие медицинские учреждения имеют неоднородную инфраструктуру, свою специализацию, используют различные цифровые комплексы.

Наиболее вероятными нарушениями информационной безопасности в сфере здравоохранения являются:

- нарушение конфиденциальности (утечка данных);
- доступ к базе данных (полный или частичный);
- потеря данных (разрушен носитель информации, информация стерта);
- незапланированное изменение данных;
- отказ функционала системы;
- система функционирует некорректно и др. [2].

Можно выделить основные рекомендации информационной безопасности в сфере здравоохранения:

- физическая безопасность (контроль периметра, где располагается медицинское оборудование, система контроля доступа на объект, достаточность мер по ограничению доступа, учет доступа);
- сетевая безопасность;
- реальный менеджер паролей (сложность, уникальность, сменяемость, второй фактор аутентификации, ответственность);
- уровень доступа к компонентам системы (профилирование уровня доступа, только необходимый для выполнения обязанностей, при необходимости выполнения операции в системе, которая не предусмотрена тем или иным профилем, могут быть разработаны различные сценарии однократного выполнения как самого сотрудника, так и с помощью удаленного вмешательства);
- персональная ответственность (вовлечение команд и сотрудников в процессы информационной безопасности, работа с персоналом, постоянное обучение персонала).

Информатизация системы здравоохранения тесно связана с внедрением медицинских информационных систем (МИС) в учреждениях здравоохранения. МИС предназначена для автоматизации деятельности лечебно-профилактических учреждений при совокупности информационных, организационных, программных и технических средств. В данных системах объединены наиболее важные аспекты медицинской организации: финансовая, организационная и административная информация; электронные медицинские данные пациентов, данные исследований, мониторинги и др. МИС направлена на повышение качества обслуживания пациентов, сокращения ошибок при заполнении отчетной документации, быстрый доступ к медицинской информации больших объемов и др. Одним из главных блоков любой МИС должен быть блок защиты персональных данных [3].

Можно выделить некоторые факторы риска, касающихся МИС:

- использование распространенных (и более уязвимых) операционных систем (ОС) и систем управления базами данных (СУБД);
- работа в открытых сегментах сети с персональных компьютеров (ПК) пользователей;
- доступ через интернет (удаленные пользователи и использование личного кабинета (ЛК), телемедицинские консультации);

- администрирование в рамках общей IT инфраструктуры (виртуальная среда, центр обработки данных (ЦОД) заказчика).

Основные угрозы безопасности медицинских информационных систем:

- угрозы от действия вредоносных программ (вирусов);
- угрозы утраты ключей и атрибутов доступа.

Для защиты от этих угроз рекомендуется создание эшелонированной защиты, которая включает в себя множество технических средств и организационных мероприятий, направленных на минимизацию получения несанкционированного доступа к системе и установке или запуска вредоносного программного обеспечения, а также нарушению целостности информации:

- применение надежных паролей и политика управления учетными записями (необходимо тщательно проверять);
- демилитаризованные зоны (DMZ) и защита периметра для сети сайта;
- брандмауэры (защитный экран между глобальным интернетом и локальной сетью учреждения) в сети;
- предотвращение доступа в интернет;
- системы обнаружения вторжений в сеть и защита от таких вторжений;
- анализ сетевого трафика;
- анализ журналов и др. [4].

Необходимо отметить, что использование антивирусного ПО не всегда является панацеей в безопасности МИС. Возникают определённые риски в виде:

- сканирование в режиме реального времени, влияющее на производительность системы;
- появление ложных срабатываний;
- помещение в карантин клинических данных, случайно совпавших с сигнатурой вируса;
- антивирусное ПО само по себе является объектом атаки;
- поддержка антивирусного ПО на протяжении всего жизненного цикла МИС (поддержка операционной системы и обновление вирусных сигнатур и библиотек). И как правило антивирусное ПО не поставляется вместе с МИС. Таким образом заказчик несет ответственность за приобретение, установку и обслуживание антивирусного ПО и файлов антивирусных определений. Рекомендуется как можно скорее устанавливать в системы последние обновления безопасности операционных систем и браузеров.

В виду того, что в условиях эксплуатации медицинское оборудование и информационные технологии со временем меняются как в результате технологического, так и по причине нормативной базы все рекомендации нуждаются в регулярной внутренней и внешней оценке. Однако, необходимо отметить, что именно обучение и вовлечение персонала в процессы обеспечения информационной безопасности является краеугольным камнем построение системы информационной безопасности в любой организации.

Библиографические ссылки

1. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends [Electronic resourse]. URL: https://www.sciencedirect.com/science/article/pii/S2772918423000048 (date of access: 05.02.2024).

2. Информационная безопасность МИС: как не допустить утечки данных пациентов [Электронный ресурс]. URL: https://archimed.pro/blog/informatsionnaya-bezopasnost-mis-kak-ne-dopustit-utechki-dannykh-patsientov/?sphrase_id=5133 (дата обращения: 01.02.2024).

3. *Плащевая Е. В.* Медицинские информационные системы [Электронный ресурс]. URL: https://www.amursma.ru/upload/iblock/a94/Vvedenie_v_medicinskuyu_informatiku._Koncepciya_informatizacii_Zdravooxraneniya_Rossii_i_Amurskoj_oblasti.pdf (дата обращения: 02.02.2024).

4. Эшелонированная защита от DDos и ботов [Электронный ресурс]. URL: https://servicepipe.ru/blog/defense-in-depth (дата обращения: 02.02.2024).