УДК 346.7

Афонин Алексей Николаевич, к.э.н., доцент,
Первый Санкт-Петербургский государственный медицинский
университет им. акад. И.П. Павлова,
КТМУ Санкт-Петербургского государственного
университета технологии и дизайна,
Санкт-Петербург
Afonin Alexey Nikolaevich,
First St. Petersburg State Medical University
named after I.P. Pavlov. I.P. Pavlov
KTMU of St. Petersburg State University
of Technology and Design

Киселева Наталья Николаевна,
независимый эксперт,
Санкт-Петербург
Kiseleva Natalia Nikolaevna,
independent expert

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЗДРАВООХРАНЕНИИ, АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ИХ РЕШЕНИЯ
INFORMATION SECURITY IN HEALTHCARE, CURRENT PROBLEMS AND THEIR SOLUTIONS

Аннотация: Данная работа посвящена проблемам обеспечения информационной безопасности в здравоохранении, подготовке и проведению различных организационных, программных и технических мер, направленных на защиту цифровых данных в медицинской организации.

Absract: This paper is devoted to the problems of information security in healthcare, preparation and implementation of various organisational, software and technical measures aimed at protecting digital data in a medical organisation.

Ключевые слова: информационная безопасность, здравоохранение, цифровые технологии.

Keywords: information security, healthcare, digital technologies.

Информационная безопасность в здравоохранении является комплексом организационных, программных и технических мер, направленных на защиту цифровых данных медицинской организации (далее – МО), обеспечение их конфиденциальности, целостности и доступности. МО, в силу специфики своей деятельности, сталкиваются в работе с большим объемом персональных данных пациентов и медицинского персонала. Помимо персональных данных, медицинские информационные системы (далее – МИС) МО содержат информацию, которая является врачебной тайной: данные о состоянии здоровья пациентов, сведения по оказанию медицинской помощи, особенностями диагностики и лечения. Такие сведения необходимо хранить, обрабатывать, передавать и уничтожать, учитывая их специфику и требования действующего законодательства.

Следует отметить, что действующее законодательство Российской Федерации (далее – РФ) защищает права граждан в части нераспространения персональных данных, врачебной

тайны и прочей конфиденциальной информации. Реализация конституционного принципа неприкосновенности частной жизни, личной и семейной тайны содержится в ч. 1 ст. 23, ч. 1 ст. 24 Конституции РФ [1]. За нарушение норм, регулирующих различные действия с персональными и медицинскими данными пациентов, предусмотрена:

– дисциплинарная (ст. 90, ст. 192 Трудового кодекса РФ);

– административная (ст. 13.11 Кодекса об административных правонарушениях РФ);

– гражданско-правовая (ст. 15, ст. 151 Гражданского кодекса РФ);

– уголовная (ст. 137 Уголовного кодекса РФ) ответственность в соответствии с федеральным законодательством [2; 3; 4; 5].

Развитие информационных технологий привели к цифровизации всей системы здравоохранения РФ. Требования к МИС установлены Приказом Минздрава РФ от 24.12.2018 г. № 911н и содержаться в Постановлении Правительства РФ от 16.11.2015 г. № 1236 [6, 7]. МИС предназначены для сбора, хранения, обработки и представления информации, необходимой для оказания медицинской помощи и информационной поддержки медицинского персонала. Информация, содержащаяся в МИС, подлежит защите в соответствии с законодательством о защите персональных данных. Согласно Федеральному закону от 26.07.2017 г. № 187-ФЗ если МО является субъектом критической информационной инфраструктуры (далее – КИИ), или одной из ее ИС присвоена категория значимости объекта КИИ, возникают дополнительные требования к информационной безопасности (далее – ИБ), которые устанавливает Приказ ФСТЭК от 25.12.2017 г. № 239 [8, 9]. Таким образом, безопасность МО должна соответствовать функциональным требованиям ИБ, предъявляемых ФСТЭК:

– средства защиты должны быть сертифицированы ФСТЭК;

– ПО или программно-аппаратные средства защиты должны быть включены в реестр отечественного ПО Минкомсвязи.

К угрозам ИБ в здравоохранении относится:

– вредоносное ПО;

– фишинговые атаки;

– DDoS;

– различные уязвимости МИС.

Обеспечение ИБ в МО предполагает комплексный подход. К методам защиты ИБ в здравоохранении можно отнести:

– управленческие (организационные), включают в себя разработку и внедрение инструкций и регламентов по обработке и хранению данных МО, аудит ИБ;

– юридические (правовые), предусматривают ответственность за нарушение правил и требований ИБ;

– программно-аппаратные, программное и аппаратное ПО, необходимое для противодействия угрозам ИБ;

– методы обеспечения физической безопасности, контроль доступа в помещения, где находятся серверы и документация МО.

Таким образом, в соответствии с действующем законодательством в здравоохранении необходимо наличие повышенных требований к защите IT-инфраструктуры, что является критически важным аспектом в обеспечении ИБ МО. Современные угрозы, такие как вредоносное ПО, фишинговые атаки, DDoS и различные уязвимости МИС ставят под угрозу конфиденциальность персональных и медицинских данных в МО. Выполнение необходимых требований и усиление ИБ способствует защите данных, улучшению качества медицинского обслуживания и повышению эффективности управления здравоохранением в целом.

Список литературы:

1. Конституция РФ [Электронный ресурс]. URL: https://www.garant.ru/ (дата обращения: 30.01.2025).
2. Трудовой кодекс РФ [Электронный ресурс]. URL: https://www.garant.ru/ (дата обращения: 30.01.2025).
3. Кодекс об административных правонарушениях РФ [Электронный ресурс]. URL: https://www.garant.ru/ (дата обращения: 30.01.2025).
4. Гражданский кодекс РФ [Электронный ресурс]. URL: https://www.garant.ru/ (дата обращения: 30.01.2025).
5. Уголовный кодекс РФ [Электронный ресурс]. URL: https://www.garant.ru/ (дата обращения: 30.01.2025).
6. Приказ Минздрава РФ от 24.12.2018 г. № 911н [Электронный ресурс]. URL: https://www.garant.ru/ (дата обращения: 30.01.2025).
7. Постановление Правительства РФ от 16.11.2015 г. № 1236 [Электронный ресурс]. URL: https://www.garant.ru/ (дата обращения: 30.01.2025).
8. Федеральный закон от 26.07.2017 г. № 187-ФЗ [Электронный ресурс]. URL: https://www.garant.ru/ (дата обращения: 30.01.2025).
9. Приказ ФСТЭК от 25.12.2017 г. № 239 [Электронный ресурс]. URL: https://www.garant.ru/ (дата обращения: 30.01.2025).