**Мошарова Анастасия Сергеевна,**
преподаватель кафедры частного права,
ФКОУ ВО Пермский институт ФСИН РОСИИ,
г. Пермь

# ЗАЩИТА МЕДИЦИНСКИХ ДАННЫХ

**Аннотация:** в цифровую эпоху информационная безопасность- актуальная проблема любой организации, в том числе медицинской. Медицинские центры подвержены таким угрозам, как взлом, утечка данных, вирусные атаки.

**Ключевые слова:** информационная безопасность, медицинская организация, защита

В современном мире все чаще упоминается такая проблема как хакерская атака, ее цель- проникновение внутрь сети организации с целью сбора финансовой, технической информации, персональных данных, логинов и паролей от личных кабинетов сотрудников. С помощью полученной информации злоумышленники далее могут производить террористические действия.

Медицинские организации являются довольно привлекательными для киберпреступников, так как личные данные пациентов, контакты и медицинские сведения, корпоративные и коммерческие данные представляют не малый интерес для злоумышленников. Медицинская информационная система – это информационная система персональных данных, которая содержит специальные категории персональных данных о состоянии здоровья [1, С.51]. Медицинская организация – это юридическое лицо, которое в качестве основного вида деятельности осуществляет медицинскую деятельность на основании лицензии. К таким организациям приравниваются индивидуальные предприниматели, которые занимаются медицинской деятельностью.

Медцентр – это полноценная медицинская организация, где предоставляют квалифицированное лечение и услуги на основе диагноза по назначению врача. Медицинская организация – более общее понятие, а медцентр – конкретный вид медицинской организации.

На сегодняшний день существует довольно большое количество путей проникновения в информационную базу организации, это может быть осуществлено и с помощью подбора связки логина и пароля, уязвимости приложений из-за их несвоевременного обновления или закрытия, фишинга или через отправку вредоносных писем, либо сообщений с ссылками на вредоносный код (вирус).

Фишинг-это вид интернет-мошенничества, при котором злоумышленники пытаются получить доступ к конфиденциальной информации других людей, например их учётным записям и данным банковских карт [2]. Фишинг может быть голосовой, почтовый, смс-фишинг и веб- фишинг. В 2024 году было обезврежено 560800 тревог повышенного уровня, при этом 14652 угрозы могли быть получены сотрудниками по электронной почте [3, С.4].

Любое письмо с просьбами открыть приложение или файл, перейти по ссылке должно вызывать подозрение.

Медицинские центры находятся в двояком положении: «с одной стороны, нам нужно упрощать и делать более прозрачным обмен медицинскими данными- это требование времени, с другой- внедрять средства защиты данных, устройств и сетей от утечек и хакерских атак. Поэтому принимаются комплексные меры: это и использование сертифицированных межсетевых экранов, взаимодействие с центром информационных технологий, внедрение сервисов виртуальной частной сети с методами шифрования и др.» [3, С.4].

Информационная безопасность- важное приоритетное направление государственной политики в РФ. Информационная безопасность Российской Федерации (далее – информационная безопасность) – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства [4]. Информационная безопасность медицинских организаций требует особо пристального внимания ввиду большого количества пациентов, базы их персональных данных, достаточно большого штата сотрудников, необходимостью отображения всех медицинских действий в информационной базе.

В современном мире важно придерживаться строгих методов обеспечения безопасности. Важно начать с соблюдения самых простых правил, таких как: пароль нельзя хранить рядом с компьютером, должно быть минимальное использование съемных носителей, важна внимательность при получении писем, проверка адреса отправителя, ни в коем случае нельзя переходить по сомнительным ссылкам и открывать подозрительные файлы.

*Список литературы:*

1.Гулиев Я.И., Цветков А.А. Обеспечение информационной безопасности в медицинских организациях// защита персональных данных. 2016.№6. С.49- 61.

2. Фишинг: что это такое? как распознать и защитится?. Электронный ресурс. URL: https://www.unisender.com/ru/glossary/chto-takoe-fishing-i-kak-ot-nego-zashchititsya/ (дата обращения 15.03.2025)

3. Это личное: как защищают медицинские данные // Газета тюменского кардиоцентра. 03.2025. №68. С.4- 5.

4. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. N 646 // Собрание законодательства Российской Федерации от 12 декабря 2016 г. N 50 ст. 7074.