

- использовать сложные уникальные пароли и двухфакторную аутентификацию;
- регулярно менять пароли;
- не открывать подозрительные ссылки и вложения;
- использовать только служебные электронные адреса для работы;
- блокировать компьютер при уходе с рабочего места;
- не копировать персональные данные пациентов на личные устройства;
- своевременно обновлять операционные системы и антивирусное программное обеспечение.
- Защита персональных данных пациентов

Медицинская информация относится к конфиденциальной информации. Ее незаконное распространение может повлечь дисциплинарную, административную и уголовную ответственность в соответствии с законодательством Республики Казахстан.

Каждый сотрудник обязан соблюдать требования информационной безопасности при работе с медицинскими информационными системами.

Действия при подозрении на кибератаку

При обнаружении подозрительной активности необходимо:

- Немедленно прекратить выполнение подозрительных действий.
- Не передавать никакие коды подтверждения.
- Сообщить системному администратору или специалисту по информационной безопасности.
- При наличии признаков мошенничества обратиться в полицию по номеру 102.
- Если затронут банковский счет — немедленно связаться с банком для блокировки операций.
- Государственные меры по борьбе с киберпреступностью

В Казахстане:

действует Департамент по противодействию киберпреступности МВД; проводится блокировка мошеннических интернет-ресурсов; ведется профилактическая работа среди населения и работников организаций; совершенствуется законодательство в сфере цифровой безопасности; развивается международное сотрудничество по борьбе с транснациональной киберпреступностью.

Заключение