KAZAN DIGITAL WEEK2023
20-22 СЕНТЯБРЯ

минцифры_

2023 ГОД НАЦИОНАЛЬНЫХ КУЛЬТУР И ТРАДИЦИЙ
МИЛЛИ МӘДӘНИЯТЛӘР ҺӘМ ГОРЕФ-ГАДӘТЛӘР ЕЛЫ

Тематическое направление: **«Цифровые технологии в здравоохранении и медицине»**

Thematic areas: **«Digital technologies in healthcare and medicine»**

Казань, 2023

KAZAN DIGITAL WEEK2023
20-22 СЕНТЯБРЯ

минцифры_

Дмитрий Кибенко
Dmitrii Kibenko

Директор ООО «Татарстан онлайн»
Эксперт в области информационной безопасности

CEO Tatarstan Online

Тема выступления: **Информационная безопасность и защита персональных данных в эпоху цифровизации в медицине**

Topic of the speech: **Information security and data protection in a medical organization**

10 Этических принципов в здравоохранении

- Соблюдение законов и нормативных актов
- Внесение позитивного вклада в общество
- Продвижение высоких стандартов качества
- Ответственное ведение бизнеса
- Бережное отношение к окружающей среде
- Защита прав пациентов
- Защита информации и ответственное использование данных
- Предотвращение дискриминации, домогательств и буллинга
- Защита и расширение прав и возможностей персонала
- Поддержка этических практик и предотвращение вреда

www.epihc.org/principles

Защита информации и ответственное использование данных

минцифры_

Обычные базовые требования включают:

• Получения явного, информированного и свободного письменного согласия на обработку данных.
• Гарантирования, что предоставление медицинских услуг не зависит от согласия на обработку данных.

Соблюдайте административные, технические и физические меры для:

• Сохранения точности, полноты и защиты записей, документов и отчетов, включая медицинскую информацию.
• Защиты информации от утери или неправомерного доступа через контролируемый доступ.
• Обеспечения конфиденциальности информации в соответствии с правовыми и этическими стандартами.

Обучение персонала должно быть непрерывно и включать:

• Обучение персонала не обсуждать состояние пациентов в общественных местах и соц.сетях.
• Запрет продажи или монетизации данных без явного согласия предоставителей данных, включая пациентов и поставщиков медицинских услуг.

Требования регуляторов к защите медицинских данных

1. Федеральный закон "О персональных данных" от 27.07.2006 №152-ФЗ

2. **Приказы ФСТЭК:** приказ ФСТЭК № 17 по ГИС, приказ ФСТЭК № 21 по ИСПДн, приказ ФСТЭК № 239 по ЗОКИИ

3. Письма, в том числе ограниченного доступа с рекомендациями ФСТЭК России, в том числе № 240/22/952, № 240/22/953, № 240/22/960, № 240/22/1549

4. Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"

Приказ 250.
Кто отвечает за кибербезопасность в ЛПУ?

Главный врач

- Назначает на заместителя полномочия по ИБ
- Создает подразделение по ИБ
- При необходимости принимает решение о привлечении внешних организаций — лицензиатов ФСТЭК или аккредитованных ФСБ организаций
- Несет персональную ответственность

Заместитель главного врача

- Курирует деятельность по обеспечению ИБ
- Взаимодействует с НКЦКИ
- Отвечает за согласование стратегии организации в части ИБ
- Согласовывает политику ИТ, ЦТ и цифровизации
- Осуществляет регулярный контроль
- Информирует руководство об инцидентах ИБ
- Руководит подразделением по ИБ
- Входит в коллегиальный орган

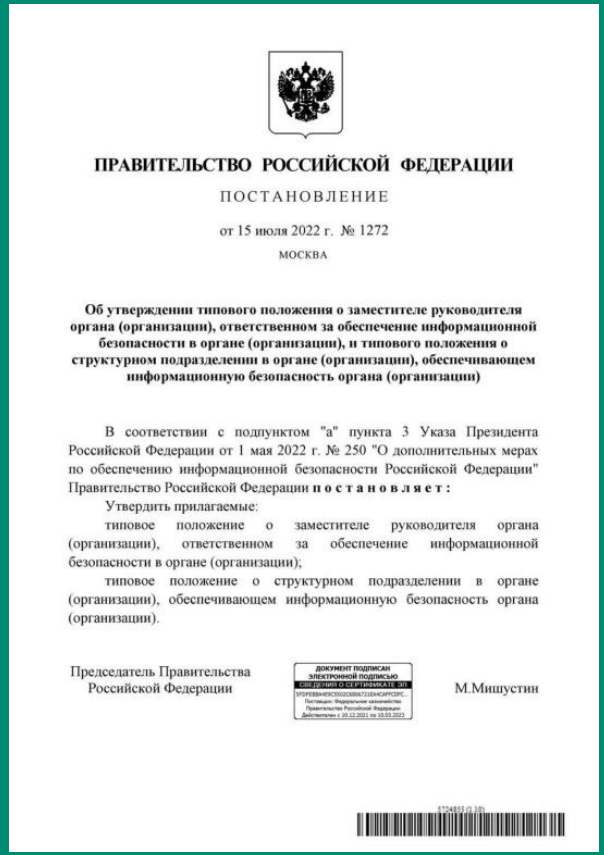
Подразделение по ИБ и/или подрядчик

- Планирует, организует, координирует и контролирует работы по ИБ
- Выявляет угрозы ИБ и уязвимости
- Предотвращает утечки информации
- Обеспечивает киберустойчивость

www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/ukaz-prezidenta-250.pdf

Постановление Правительства РФ № 1272

«Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 15 июля 2022 г. № 1272

МОСКВА

Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)

В соответствии с подпунктом "а" пункта 3 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" Правительство Российской Федерации **п о с т а н о в л я е т :**

Утвердить прилагаемые:

типовое положение о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации);

типовое положение о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации).

Председатель Правительства Российской Федерации — М.Мишустин

Ответственность

- **Дисциплинарная**

ст. 90 Трудового кодекса РФ лица, виновные в нарушении законодательства в области персональных данных, могут быть привлечены к дисциплинарной и материальной ответственности

- **Гражданская**

ч. 1 ст. 150 Гражданского кодекса Российской Федерации неприкосновенность частной жизни

- **Административная**

Разглашение информации с ограниченным доступом (ст. 13.14, ч. 1 ст. 28.4 КоАП РФ)

- **Уголовная**

Нарушение неприкосновенности частной жизни (ст. 137 УК РФ; пп. "а" п. 1 ч. 2 ст. 151 УПК РФ)

Реализовано в РТ

- Создано защищенное облако для размещения медицинских информационных систем
- Создан защищенный контур здравоохранения
- Используются новые ПК с защищенной ОС Альт 8 СП
- Внедряются средства защиты для существующего парка ПК

Часто задаваемые вопросы?

Какой должна быть длительность обучения заместителей руководителя?

- **Не менее 360 часов**

А можно топ-менеджеру не учиться 360 часов?

- **На текущий момент нет.**

Может ли заместитель руководителя организации по ИБ начать работу сразу и потом пойти учиться?

- **Да, сначала можно назначить ответственного, а потом уже учить его.**

А можно возложить все на существующее ИТ-подразделение?

- **Да, можно**

А можно не создавать подразделение ИБ и все переложить на подрядчика?

- **В случае нехватки специалистов возможно поручение данной задачи внешней организации, но контроль за соблюдением Указа 250 и контроль аутсорсера должны быть реализованы все равно**
- **Внешняя организация должна быть лицензиатом ФСТЭК России и ФСБ России**

www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/ukaz-prezidenta-250.pdf

Защита информации и план мероприятий от ChatGPT

- **Возложение на одного из заместителей обязанностей** по обеспечению информационной безопасности
- **Проведение анализа уязвимостей:** Оценка существующих информационных систем и выявление уязвимостей, которые могут стать точкой входа для злоумышленников.
- **Разработка политики безопасности:** Создание и утверждение документа, который определяет стандарты и правила обработки и хранения медицинских данных.
- **Обучение персонала:** Проведение обучающих курсов для сотрудников по правилам безопасности, включая осведомленность о социальной инженерии и фишинге.
- **Установка средств защиты:** Установка и регулярное обновление антивирусных программ, брандмауэров и других средств защиты на компьютерах и серверах.
- **Контроль доступа:** Введение системы управления доступом для ограничения прав доступа к медицинским данным в зависимости от роли сотрудника.
- **Аудит безопасности:** Регулярное проведение аудита информационной безопасности для выявления и устранения нарушений.
- **Резервное копирование данных:** Разработка и поддержание плана резервного копирования данных для обеспечения их доступности в случае инцидентов.
- **Мониторинг событий:** Установка системы мониторинга событий для реагирования на подозрительную активность в реальном времени.
- **Шифрование данных:** Применение шифрования для защиты данных в пути и в покое, особенно при передаче медицинской информации.
- **Обновление и согласование со стандартами:** Постоянное обновление мероприятий безопасности в соответствии с современными стандартами и законодательством в области медицинской информационной безопасности.

KAZAN DIGITAL WEEK2023
20-22 СЕНТЯБРЯ

минцифры_

2022 2031 десятилетие науки и технологий

2023 ГОД ПЕДАГОГА И НАСТАВНИКА

2023 ГОД НАЦИОНАЛЬНЫХ КУЛЬТУР И ТРАДИЦИЙ
МИЛЛИ МӘДӘНИЯТЛӘР ҺӘМ ГОРЕФ-ГАДӘТЛӘР ЕЛЫ

Благодарю за внимание!

Thank you for your attention!

Казань, 2023