Политика безопасности персональных данных, обрабатываемых в информационных системах персональных данных ГУЗ «Майнская районная больница»

Содержание

Перечень принятых сокращений и обозначений

Далее по тексту приняты следующие обозначения и сокращения:

АС - автоматизированная система:

ЗИ - защита информации;

ЛВС - локальная вычислительная сеть:

НСД - несанкционированный доступ к информации;

ОС - операционная система:

ПИБ - политика информационной безопасности;

ПДн - персональные данные:

ИСПДн - информационная система персональных данных;

ПО - программное обеспечение:

СВТ - средства вычислительной техники;

СЗИ НСД - система защиты от НСД к информации:

СКЗИ - средство криптографической защиты информации.

ВВЕДЕНИЕ

1. Назначение политики безопасности

Данный документ определяет требования по защите персональных данных, обрабатываемых на автоматизированных рабочих местах и серверах информационных систем персональных данных ГУЗ «Майнская районная больница» (далее ОРГАНИЗАЦИЯ).

2. Целевая аудитория

Политика безопасности обязательная для следующих сотрудников ОРГАНИЗАЦИИ:

- пользователей сети, выполняющие свои служебные обязанности, связанные с обработкой персональных данных (далее ПДн), на автоматизированных рабочих местах;

- системных администраторов, ответственных за эксплуатацию и сопровождение информационных систем обработки персональных данных (ИСПДн), а также за информационную безопасность информационных систем;

3. Полномочия

Главный врач совместно с лицами, ответственными за информационную безопасность в организации, уполномочен создать, внедрить и поддерживать данную политику в соответствии с требованиями федерального законодательства.

Сотрудники отдела АСУ несут ответственность за внедрение данной политики, мониторинг соответствия политике безопасности и реагирование на нарушения политики безопасности.

Отдел кадров несет ответственность за доведение данной политики до каждого сотрудника.

Сотрудники несут персональную ответственность за выполнение данной политики.

4. Срок действия

С 01 декабря 2015 года по 31 декабря 2016 года. В случае отсутствия приказов главного врача по прекращению действия настоящей политики или ее замене срок действия пролонгируется автоматически.

5. Исключения

Все отклонения от выполнения данной политики безопасности утверждаются главным врачом с отчётом о последствиях (согласием) сотрудников отдела АСУ.

6. Поддержка

По всем вопросам, связанным с политикой безопасности, необходимо обращаться в группу администраторов ИСПДн.

7. Пересмотр и обновление

Группа администраторов ИСПДн несет ответственность за пересмотр (обновление) политики безопасности в связи с изменением федерального законодательства или целями и задачами бизнеса.

Политика безопасности пересматривается по мере необходимости.

1. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

1.1. Учетные записи

Перечень учетных записей и прав этих записей в отношении ПДн, ИСПДн и средств защиты ИСПДн вводятся Порядком доступа сотрудников ГБУЗ "Стоматологическая поликлиника города Ульяновска" к информационным системам обработки персональных данных и программно-аппаратным средствам их защиты. В соответствии с данным документом вводятся следующие типы учетных записей:

– Руководитель организации, имеющий доступ к ПДн всех ИСПДн (пользователь ИСПДн) и использующий при этом соответствующие средства защиты информации (СЗИ).

– Руководитель структурного подразделения (пользователь ИСПДн), имеющий доступ к ПДн, обрабатываемым в рамках вверенного ему подразделения, и использующий при этом соответствующие средства защиты информации

– Сотрудник структурного подразделения (пользователь ИСПДн), имеющий доступ к ПДн, обрабатываемым в рамках его должностных обязанностей, и использующий при этом соответствующие средства защиты информации

– Администратор ИСПДн, выполняющий настройку и конфигурирование ИСПДн и имеющий в связи с этим к ПДн.

– Администратор СЗИ ИСПДн, выполняющий настройку и конфигурирование СЗИ ИСПДн.

– Администратор КСЗИ ИСПДн, выполняющий настройку и конфигурирование криптографических СЗИ ИСПДн и ответственный за хранение и использование криптографических ключей.

– Администратор антивирусных СЗИ ИСПДн, выполняющий настройку и конфигурирование антивирусных средств защиты ИСПДн.

– Администратор межсетевого экрана, выполняющий настройку и конфигурирование межсетевого экрана организации

– Администратор СЗИ ИСПДн от несанкционированного доступа, выполняющий настройку и конфигурирование СЗИ от НСД.

Учетная запись Администратора ИСПДн обладает правами локального администратора Windows. Допускается совмещение прав учетных записей. Права и обязанности пользователей и администраторов перечислены в соответствующих должностных инструкциях.

1.2. Идентификация и аутентификация

Идентификация и аутентификация в ИСПДн осуществляются на основе двухфакторной аутентификации (парольной и с использованием USB ключа) с использованием СЗИ от НСД идентификатор ruToken в соответствии с должностными инструкциями Пользователя и Администратора СЗИ ИСПДн НСД и инструкции по использованию идентификатора ruToken.

1.3. Парольная политика

Пароль должен содержать не менее 6 символов, состоящих из букв разных регистров, цифр и спецсимволов. Пароли должны меняться не реже чем раз в 3 месяца. Хранение пароля на открытом носителе не допускается.

1.4. Каталоги и файлы

Пользователям разрешен доступ ко всем каталогам и файлам используемых ими ИСПДн, кроме системных.

Администраторам разрешен доступ ко всем файлам и каталогам.

1.5. Инциденты

Все возможные инциденты и порядок действий для их разрешения описаны в соответствующих должностных инструкциях Пользователей и Администраторов.

2. ИСПОЛЬЗОВАНИЕ НОСИТЕЛЕЙ ИНФОРМАЦИИ

2.1. Носители информации

К использованию разрешены следующие носители информации:

– Флеш-карты
– CD и DVD диски

Все носители, содержащие ПДн, должны быть зарегистрированы в журнале учета съемных носителей информации.

Носители разрешается использовать только в служебных целях, использование носителей в личных целях, для переноса музыки, фильмов и т.п. не допускается.

2.2. Хранение

Все носители, содержащие ПДн, должны хранится в сейфе организации. Хранение носителей вне организации не допускается.

2.3. Подключение

При подключении съемного носителя информации в соответствии должностной инструкцией пользователя антивирусных СЗИ необходимо проверить его на наличие вирусов с помощью антивирусного ПО.

2.4. Уничтожение

Носители информации, содержащие ПДн, уничтожаются в присутствии специальной комиссии, отчет об уничтожении заносится в соответствующий акт.

2.5. Инциденты

Возможные инциденты и описание процедур реагирования на них описаны в должностных инструкциях Администратора ИСПДн и Администратора СЗИ ИСПДн.

3. РЕЗЕРВНОЕ КОПИРОВАНИЕ

3.1. Носители информации

В качестве носителей информации для резервного копирования данных, содержащих ПДн, в организации используются компакт-диски формата CD-R. Порядок учета, хранения и уничтожения определяются п. 2. настоящей Политики. Ответственность за резервное копирование несет Администратор ИСПДн.

3.2. Каталоги и файлы

Резервному копированию подлежат каталоги и файлы, содержащие исполняемые файлы ИСПДн, базы данных ИСПДн и конфигурационную

информацию СЗИ ИСПДн.

3.3. Приложения

Основными приложениями, использующимися для резервного копирования, являются программы WinZip (стандартная утилита операционной системы для архивирования данных) и explorer (в части переноса данных на компакт-диски)

3.4. Периодичность

Указанные в п.3.2. файлы и папки резервируются с периодичностью один раз в месяц.

3.5. Инциденты

В случае потери целостности файлов или папок, указанных в п.3.2. необходимо

- произвести анализ оставшейся информации и по возможности извлечь ее;
- восстановить функционирование ИСПДн
- в случае отсутствия части информации или полной невозможности ее восстановления используется последняя резервная копия, содержащая утраченные данные.

4. СЕТЕВОЙ ДОСТУП

4.1. Сетевые устройства

Коммутационные устройства организации, использующиеся для организации сетевого взаимодействия в рамках функционирования ИСПДн описаны в Техническом паспорте ИСПДн.

4.2. Сетевые приложения

Сетевые приложения организации, использующиеся для организации сетевого взаимодействия в рамках функционирования ИСПДн описаны в Техническом паспорте ИСПДн.

4.3. Учетные записи и сетевой доступ

Сетевой доступ в организации реализуется средствами операционной системы Windows. Разграничение доступа при этом осуществляется на уровне учетных записей операционной системы в соответствии с п.1.4 настоящей Политики.

4.4 Доступ в Интернет

Доступ пользователей в Интернет определяется Порядком доступа сотрудников Организации к информационным системам обработки персональных данных и программно-аппаратным средствам их защиты и приказами организации.

4.5. Межсетевой экран

Правила фильтрации трафика определяются должностной инструкцией Администратора межсетевого экрана.

5. ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ

5.1. Вредоносные программы

В рамках применения настоящей политики вредоносными программами являются программы и программные закладки, опубликованные на обновляемом ресурсе http://ru.norton.com Соответствие уровня защиты данному перечню обеспечивается своевременным обновлением баз антивирусных программ и выполнением должностных инструкций пользователя и администратора антивирусных средств защиты ИСПДн.

5.2. Приложения

Перечень приложений против вредоносных программ и правила доступа к настройкам этих программ определяются должностными инструкциями пользователя и администратора антивирусных средств защиты ИСПДн.