Государственное бюджетное учреждение здравоохранения Самарской области «Чапаевская центральная городская больница» (ГБУЗ СО «ЧЦГБ»)

ПРИКАЗ

«26» 03 2021г. **Чапаевск** № 96.3

Об утверждении Положения о защите персональных данных в информационных системах персональных данных в государственном бюджетном учреждении здравоохранения Самарской области «Чапаевская центральная городская больница»

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в целях обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных и совершенствования системы защиты информации в информационных системах персональных данных ГБУЗ СО «ЧЦГБ»,

ПРИКАЗЫВАЮ:

1. Утвердить «Положение О защите персональных данных в информационных системах персональных данных в ГБУЗ СО «ЧЦГБ».
2. Приказ довести до исполнителей, заместителей главного врача, руководителей структурных подразделений под роспись.
3. Контроль за исполнением настоящего Приказа оставляю за собой.

Главный врач _____/ Н.С. Юрицин

УТВЕРЖДАЮ

Главный врач

ГБУЗ СО «ЧЦГБ»

_____ / Н.С. Юрицин

«___»_____2021г.

ПОЛОЖЕНИЕ

О защите персональных данных
в информационных системах персональных данных в Государственном бюджетном учреждении здравоохранения Самарской области «Чапаевская центральная городская больница»

1. Общие положения

Настоящее «Положение о защите персональных данных в информационных системах персональных данных в Государственном бюджетном учреждении здравоохранения Самарской области «Чапаевская центральная городская больница» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012г., методическими рекомендациями ФСТЭК России и ФСБ России. Положение разработано в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений при их обработке, порядок обучения персонала практике работы в ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

2. Порядок предоставления допуска пользователей к работе в ИСПДн

Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

Первоначальный допуск пользователей к работе в ИСПДн осуществляется на основании приказа, который издаётся Главным врачом (далее Руководитель Государственного бюджетного учреждения здравоохранения Самарской области «Чапаевская центральная городская больница» (далее – ГБУЗ СО «ЧЦГБ»). В приказе определяется список работников, допущенных к работе в ИСПДн.

С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации и выполнения необходимых мероприятий по обеспечению безопасности в ИСПДн руководителем назначается администратор безопасности.

С целью соблюдения принципа персональной ответственности за свои действия каждому работнику, допущенному к работе в ИСПДн, должно быть сопоставлено персональное уникальное имя (учётная запись пользователя), под которым он будет регистрироваться и работать в ИСПДн.

Использование несколькими работниками при работе в ИСПДн одного и того же имени пользователя ***запрещено.***

В дальнейшем, процедура регистрации (создания учётной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой.

В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учётной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);
- должность (с полным наименованием отдела), фамилия, имя и отчество работника;
- имя пользователя (учётной записи) данного работника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путём указания решаемых пользователем задач в ИСПДн).

Заявку рассматривает и визирует руководитель, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного работника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем заявка передаётся администратору безопасности для внесения необходимых изменений в списки пользователей ИСПДн.

На основании заявки администратор безопасности производит необходимые операции по созданию (удалению) учётной записи пользователя, присвоению ему начального значения пароля, а также регистрацию персонального идентификатора и другие необходимые действия, указанные в заявке.

После внесения изменений в списки пользователей администратор безопасности должен обеспечить настройки средств защиты соответствующие требованиям безопасности указанной ИСПДн.

Работнику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное значение пароля, которое он обязан сменить при первом же входе в систему.

Исполненная заявка хранится у администратора безопасности.

Она может впоследствии использоваться:

- для восстановления полномочий пользователей после возникновения внештатных ситуаций;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;
- для проверки работниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

3. Порядок работы пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн

Пользователь имеет право в отведённое ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

Пользователь несёт ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

Перед началом работы в ИСПДн, работники учреждения, допущенные к работе с ПДн, принимают под роспись обязательство о неразглашении персональных данных.

Вход пользователя в систему должен осуществляться по выдаваемому ему электронному идентификатору и по персональному паролю.

Запись информации, содержащей ПДн, должна осуществляться только на машинные носители информации, соответствующим образом учтённые в Журнале учёта защищаемых носителей информации. Ответственным за ведение Журнала учёта является администратор безопасности.

При работе со съёмными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

Каждый работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несёт персональную ответственность за свои действия и ***обязан***:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;
- хранить в тайне свой пароль (пароли). В соответствии с п. 7.5. данного Положения и с установленной периодичностью менять свой пароль (пароли);
- хранить установленным порядком своё индивидуальное устройство идентификации (ключ) и другие реквизиты в недоступном для посторонних месте;
- выполнять требования Положения по организации антивирусной защиты в полном объёме;
- немедленно известить администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:
  - фактов совершения попыток несанкционированного доступа (далее - НСД) к ИСПДн;
  - несанкционированных изменений в конфигурации программных или аппаратных средств ИСПДн;
  - отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;
  - некорректного функционирования установленных на компьютеры технических средств защиты;
  - непредусмотренных отводов кабелей и подключённых устройств.

Пользователю категорически ***запрещается***:

- использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить ПДн на неучтённых машинных носителях информации;

- оставлять включённым без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте или где бы то ни было своё персональное устройство идентификации, машинные носители и распечатки, содержащие ПДн;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению конфиденциальности ПДн;

- размещать средства отображения информации (монитор, принтер и т.п.) таким образом, чтобы с них существовала возможность визуального считывания информации посторонними лицами.

Администратор безопасности **обязан**:

- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;
- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищённых СВТ и других устройствах;
- производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:
- реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);
- вводить описания пользователей ИСПДн в информационную базу системы разграничения доступа в ИСПДн;
- своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;
- проводить инструктаж работников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;
- контролировать своевременное (не реже чем один раз в течение 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;
- обеспечивать постоянный контроль выполнения работниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;

- осуществлять контроль порядка создания, учёта, хранения и использования резервных и архивных копий массивов данных;
- настраивать и сопровождать подсистемы регистрации и учёта действий пользователей при работе в ИСПДн;
- организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учёта бумажных носителей информации;
- периодически тестировать функции СЗИ от НСД с использованием специальных средств анализа защищённости, особенно при изменении программной среды и полномочий исполнителей;
- восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;
- вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;
- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования;
- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание персональных данных на носителях информации);
- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;
- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

4. Порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных, защищаемой информации и средств защиты информации

1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.
2. К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные в Журнале учёта носители.

3. Администратор безопасности ***обязан*** осуществлять периодическое резервное копирование персональных данных.

4. Носители информации, предназначенные для создания резервной копии и хранения персональных данных, выдаются установленным порядком администратором безопасности. По окончании процедуры резервного копирования электронные носители сдаются на хранение администратору безопасности, или руководителю.

5. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

6. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

7. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и(или) защищаемой информации в результате сбоев в сети электропитания.

8. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных.

9. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся у администратора безопасности. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

10. Ответственность за проведение резервного копирования, мероприятий по восстановлению работоспособности технических средств, мероприятий по восстановлению средств защиты информации возлагается на администратора безопасности.

5. Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных

1. Перед началом работы в ИСПДн пользователи должны ознакомиться с требованиями настоящего Положения под роспись.

2. Пользователи должны продемонстрировать администратору безопасности наличие необходимых знаний и умений для выполнения требований настоящего Положения.
3. Ответственным за организацию обучения и оказание методической помощи в учреждении является администратор безопасности.

6. Правила антивирусной защиты

Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения, компьютерных вирусов и устанавливает ответственность руководителя и работников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение.

7. К использованию на компьютерах допускаются только лицензионные антивирусные средства;
8. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности;
9. Администратор безопасности осуществляет периодическое обновление антивирусных средств и контроль их работоспособности;
10. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы;
11. Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров;
12. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съёмных носителях (флэш-накопителях, магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съёмной носитель);
13. Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль;
14. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором безопасности должна быть выполнена антивирусная проверка ИСПДн;

15. На компьютеры пользователей запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации;

16. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов пользователь **обязан**:

- приостановить обработку данных в ИСПДн;
- немедленно поставить в известность о факте обнаружения заражённых вирусом файлов администратора безопасности, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем заражённых вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение заражённых файлов.

17. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора безопасности;

18. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

7. Правила парольной защиты

1. Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора безопасности.

3. При доступе пользователя в систему должна осуществляться идентификация и проверка подлинности по идентификатору и паролю, а также с использованием электронных идентификаторов.

4. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями самостоятельно с учетом следующих требований:

- пароль должен быть длиной не менее шести буквенно-цифровых символов;
- символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущих;
- пользователь не имеет права сообщать личный пароль другим лицам.

5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 360 дней.
6. Удаление учётной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри учреждения и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой, на основании указания руководителя или начальника отдела кадров.
7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри учреждения и другие обстоятельства) администратора безопасности.
8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по изменению его пароля.
9. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности.

8. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

1. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

2. Право на установку, обновление и модификацию общесистемного и прикладного программного обеспечения компьютеров ИСПДн предоставляется администратору безопасности.
3. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме администратора безопасности ***запрещено***.
4. Заявку на внесение изменений в конфигурацию аппаратно-программных средств защищённых рабочих мест ИСПДн, рассматривает руководитель, визирует её, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

   После чего заявка передаётся администратору безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке.
5. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.
6. Установка и обновление ПО (системного, прикладного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.).
7. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие опасных функций.
8. После установки (обновления) ПО, администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки.
9. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, администратор безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

9. Порядок контроля обеспечения защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления.

1. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения техни-

ческих средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

2. Основными задачами контроля являются:
   - проверка организации выполнения мероприятий по защите информации в учреждении, учёта требований по защите информации в разрабатываемых плановых и распорядительных документах;
   - выявление демаскирующих признаков объектов ИСПДн;
   - уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
   - проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
   - проверка выполнения требований по защите ИСПДн от несанкционированного доступа;
   - проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;
   - проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;
   - оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;
   - разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

10.Порядок охраны и допуска посторонних лиц в помещения ИСПДн

1. В учреждении должна быть предусмотрена физическая охрана технических средств ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надёжных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации.
2. В помещениях должна быть установлена охранная и пожарная сигнализация.

3. Серверное и коммутационное оборудование ИСПДн должно находиться под надёжным замком, в отдельном помещении или запирающемся шкафу, ключ должен храниться у администратора безопасности.
4. Вскрытие и закрытие помещений осуществляется работниками, работающими в данных помещениях.
5. Список работников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения утверждается руководителем и передаётся на пост охраны.
6. При закрытии помещений и сдачей их под охрану работники, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации на которых содержатся персональные данные, убираются для хранения в запираемый ящик стола или сейф.
7. При обнаружении повреждения замков, дверей или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и(или) ответственному за защиту информации.
8. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или ответственному за защиту информации, или руководителю, или администратору безопасности.

11.Заключительные положения

1. Требования настоящего Положения обязательны для всех работников, обрабатывающих персональные данные.
2. Нарушение требований настоящего Положения влечёт за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.