ЧĂВАШ РЕСПУБЛИКИН
СЫВЛĂХА СЫХЛАС ЁÇ
МИНИСТЕРСТВИ

П Р И К А З

29.03.2019 422 №

Шупашкар хули

**МИНИСТЕРСТВО
ЗДРАВООХРАНЕНИЯ
ЧУВАШСКОЙ РЕСПУБЛИКИ**

П Р И К А З

29.03.2019 № 422

г. Чебоксары

Об утверждении Положения по обеспечению защиты информации в Министерстве здравоохранения Чувашской Республики

В соответствии с требованиями Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указа Президента Российской федерации от 06 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера», введенным в действие приказом Председателя Государственной технической комиссии при Президенте Российской Федерации от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» и в целях эффективного обеспечения информационной безопасности Министерства здравоохранения Чувашской Республики п р и к а з ы в а ю:

1. Утвердить Положение по обеспечению защиты информации в Министерстве здравоохранения Чувашской Республики (далее – Положение).

2. Заместителям министра, руководителям структурных подразделений Министерства здравоохранения Чувашской Республики обеспечить строгое соблюдение требований Положения всеми сотрудниками Министерства здравоохранения Чувашской Республики.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Министр В.Н. Викторов

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ ЧУВАШСКОЙ РЕСПУБЛИКИ
ЧĂВАШ РЕСПУБЛИКИН СЫВЛĂХА СЫХЛАС ЁÇ МИНИСТЕРСТВИ
КАНЦЕЛЯРИЯ

УТВЕРЖДЕНО
приказом Министерства здравоохранения
Чувашской Республики
от «29» 03 2019 г. № 422

ПОЛОЖЕНИЕ
по обеспечению защиты информации в Министерстве здравоохранения Чувашской Республики

1. Общие положения

1.1. В настоящем Положении используются следующие основные понятия:

автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

антивирусная программа (антивирус) - программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики - предотвращения заражения файлов или операционной системы вредоносным кодом;

аппаратные средства - это технические средства, используемые для обработки данных. Сюда относятся: Персональный компьютер (комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач);

безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;

вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению;

доступ к информации - возможность получения информации и ее использования;

защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

идентификация - присвоение субъектам и объектам доступа идентификатора и / или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

информация - сведения (сообщения, данные) независимо от формы их представления;

информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позво-

ляющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных;

носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;

обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и / или осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования;

правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

средства защиты информации - это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации;
(в целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

- ***технические*** (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации.
- ***программные*** средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др.
- ***смешанные*** аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.
- ***организационные*** средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия));

технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах;

уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

1.2. Настоящее Положение по обеспечению защиты информации министерства (далее - Положение) разработано в соответствии с требованиями Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указа Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера», введенным в действие приказом Председателя Государственной технической комиссии при Президенте Российской Федерации от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)».

Положение является основным руководящим документом в области обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, обязательным для выполнения всеми сотрудниками Министерства здравоохранения Чувашской Республики (далее – Министерство), преследует цель оказать помощь должностным лицам в практической реализации установленных мер защиты информации при эксплуа-

тации различных средств вычислительной техники.

1.3. Информация, циркулирующая в Министерстве, связанная с персональными данными и сведениями конфиденциального характера подпадает под действие федеральных законов, направленных на обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных.

1.4. Защите подлежат:

- информационные ресурсы, содержащие сведения, отнесенные к конфиденциальной информации, представленные в виде бумажных носителей, носителей на магнитной и оптической основе, информационных массивов и баз данных;
- информационное содержание имеющихся баз данных;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы);
- программные средства (операционные системы и системы управления базами данных, другое общесистемное и прикладное программное обеспечение);
- автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные, телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемые для обработки информации, содержащие сведения, отнесенные к конфиденциальной информации;
- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается (передается) информация, содержащая сведения, отнесенные к конфиденциальной информации, а также сами помещения.

2. Обязанности должностных лиц

2.1. Практическая реализация мероприятий по защите информации и контроль за соблюдением безопасности информации в Министерстве возлагается на ответственное должностное лицо за выполнение мероприятий по обеспечению защиты информации, назначенного приказом Министерства здравоохранения Чувашской Республики от 19 февраля 2018 г. № 229 «Об ответственных лицах за организацию и обеспечение мероприятий по защите информации, не содержащей сведений, составляющих государственную тайну, в Министерстве здравоохранения Чувашской Республики» (далее – специалист, ответственный по защите информации).

2.2. На специалиста, ответственного по защите информации, возлагается:

- разработка проектов приказов, распоряжений и инструкций по обеспечению защиты информации и осуществление контроля за выполнением требований указанных документов;
- взаимодействие по вопросам обеспечения безопасности и защиты информации с субъектами информационного обмена и контролирующими органами;
- руководство работой специалиста по информационной безопасности;
- анализ состояния работ по обеспечению защиты информации и выработка предложений по ее совершенствованию;
- выявление конфиденциальной информации и документальное оформление в виде перечня сведений, подлежащих защите;
- внедрение программного обеспечения, разрабатываемого в Министерстве с учетом требований защиты информации и настоящего Положения;
- совместно со специалистом по информационной безопасности с исполь-

зованием программных и технических средств и закрепление их за пользователями;

- осуществление контроля за сменой паролей в установленное время;
- контроль за хранением машинных носителей с общим программным обеспечением и пакетов прикладных программ, предназначенных для тиражирования;
- разработка Списка сотрудников, имеющих право обработки на средствах вычислительной техники конфиденциальной информации, по заявкам руководителей структурных подразделений Министерства;
- инструктаж и консультирование сотрудников по вопросам обеспечения защиты информации;
- участие в проведении расследований по фактам нарушения безопасности информации в Министерстве;
- организация учета и хранения съемных накопителей информации.

2.3. На специалиста по информационной безопасности возлагается:

- контроль за выполнением специальных требований по размещению технических средств, прокладке кабельных трасс и инженерных систем;
- обеспечение монтажа и генерации локальных вычислительных сетей в соответствии с требованиями установленного класса защищенности информационных систем;
- организация антивирусной защиты средств вычислительной техники;
- внедрение технических средств информационной системы персональных данных, с учетом требований защиты информации и настоящего Положения;
- выбор технических средств, удовлетворяющих требованиям настоящего Положения;
- резервное копирование баз данных и информации с сервера;
- своевременное создание и ведение баз эталонных копий программного обеспечения автоматизированных и информационных систем;
- организация хранения эталонных машинных носителей с программным обеспечением и пакетов прикладных программ, предназначенных для тиражирования;
- опечатывание (опломбирование) системных блоков персональных компьютеров, на которых обрабатывается конфиденциальная информация.
- участие в проведении расследований по фактам нарушения безопасности информации в Министерстве.

2.4. Ответственность за выполнение мероприятий по обеспечению защиты информации в структурных подразделениях Министерства возлагается на руководителей структурных подразделений Министерства.

2.5. Персональную ответственность за обеспечение безопасности информации на своем рабочем месте несет сотрудник Министерства, который должен руководствоваться Инструкцией пользователя (оператора) по обеспечению защиты информации при работе на персональном компьютере (Приложение № 1 к настоящему Положению).

3. Ввод в эксплуатацию программных средств обработки конфиденциальной информации

3.1. Установка программного обеспечения и средств защиты информации осуществляется специалистом, ответственным за информационную безопасность.

3.2. Прием и ввод в эксплуатацию программного обеспечения и средств защиты информации осуществляется решением технической комиссии по вопро-

сам защиты информации, утвержденной приказом Министерства здравоохранения Чувашской Республики от 5 сентября 2017 г. № 1181 «О создании технической комиссии по вопросам защиты информации Министерства здравоохранения Чувашской Республики».

3.3. Установка и эксплуатация программного обеспечения, не принятого в эксплуатацию технической комиссией по вопросам защиты информации, не допускается.

4. Организация резервного копирования информации

4.1. Организация резервного копирования информации является необходимой составной частью комплексной системы защиты информации.

4.2. Ответственность за резервное копирование информации возлагается на специалиста по информационному обеспечению.

4.3. При возникновении нештатных ситуаций (сбой программного обеспечения, отключение электричества, выход из строя сервера и т.п.) может произойти потеря и (или) разрушение данных. В этом случае специалист по информационному обеспечению производит восстановление программного обеспечения и (или) данных из последней резервной копии.

4.4. Организация резервного копирования информации производится в соответствии с Инструкцией по организации резервного копирования информации (Приложение № 2 к настоящему Положению).

5. Учет и обращение с жесткими магнитными дисками

5.1. Жесткие магнитные диски являются основными носителями информации в информационных системах и подлежат обязательной защите от несанкционированного доступа.

5.2. Требования по учету и обращению с жесткими магнитными дисками устанавливаются Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы (Приложение № 3 к настоящему Положению).

6. Учет, хранение и обращение со съемными накопителями информации

6.1. Порядок учета, хранения и обращения со съемными накопителями информации устанавливается Инструкцией о порядке обращения со съемными накопителями информации (Приложение № 4 к настоящему Положению).

6.2. Поступившие в любое структурное подразделение Министерства съемные накопители информации, содержащие прикладное программное обеспечение или средства защиты информации, подлежат в обязательном порядке учету и регистрации в соответствии с настоящим Положением.

7. Организация антивирусной защиты

7.1. Антивирусная защита программных и аппаратных средств автоматизированной системы является необходимой составной частью комплексной системы защиты информации.

7.2. Защита от вирусов (компьютерных, программных) производится в соответствии с Инструкцией по организации антивирусной защиты (Приложение № 5 к настоящему Положению).

8. Организация парольной защиты информации

8.1. Система парольной защиты информации является основой комплексной системы защиты от несанкционированного доступа к информационным ресурсам.

8.2. Парольная система защиты информации организуется в соответствии с Инструкцией по организации парольной защиты информации (Приложение № 6 к настоящему Положению).

9. Порядок размещения и установки средств вычислительной техники по обработке конфиденциальной информации в помещениях

9.1. Помещения, в которых осуществляется обработка защищаемой информации, относятся к категории защищаемых. Вход в помещения лиц, не имеющих отношение к работе с персональными данными, должен быть ограничен.

9.2. Размещение и установка средств вычислительной техники в помещениях, где обрабатывается защищаемая информация, должны исключать возможность хищения устройств вычислительной техники и предотвращать бесконтрольное использование и визуальный просмотр обрабатываемых сведений лицами, не имеющими к ним отношения в соответствии с порядком разрешительного доступа сотрудников Министерства к АРМ с установленным СКЗИ, утвержденный председателем технической комиссии по защите информации от 18 декабря 2015 г.

9.3. Допуск представителей для ремонта и уборки помещений, где размещены средства вычислительной техники, осуществляется в присутствии одного из сотрудников данного помещения.

Приложение № 1
к Положению по обеспечению
защиты информации в
Министерстве здравоохранения
Чувашской Республики

Инструкция
пользователя (оператора) по обеспечению защиты информации
при работе на персональном компьютере

1. Общие обязанности сотрудников Министерства по обеспечению информационной безопасности при работе с информационной системой

Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационной системы, несет персональную ответственность за свои действия и обязан:

- строго соблюдать правила, установленные настоящим Положением, при работе со средствами вычислительной техники;
- выполнять правила работы со средствами защиты информации, установленными на его рабочей станции;
- в соответствии с Инструкцией по организации парольной защиты информации (Приложение № 6 к настоящему Положению) хранить в тайне свой пароль (пароли) и с установленной периодичностью принять меры по замене своего пароля (паролей);
- при работе со средствами криптозащиты информации, в случае предоставления ему права защиты (подтверждения подлинности и авторства) документов, передаваемых по технологическим цепочкам в информационной системе, при помощи электронной цифровой подписи, руководствоваться:

1) инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152.

2) правилами обмена электронными документами и использования электронной цифровой подписи, утвержденными постановлением Кабинета Министров Чувашской Республики от 15 августа 2014 г. № 276 «О концепции информатизации Чувашской Республики».

- выполнять требования Инструкции по организации антивирусной защиты (Приложение № 5 к настоящему Положению) в части касающейся действий пользователей рабочей станции в информационной системе;
- немедленно вызывать специалиста, ответственного по защите информации, и ставить в известность руководителя структурного подразделения Министерства в случае подозрения компрометации личных ключей и паролей, а также при обнаружении:

1) нарушений целостности пломб (наклеек) на аппаратных средствах рабочей станции;

2) несанкционированных (произведенных с нарушением установленного порядка) действий по изменению конфигурации программных или аппаратных средств рабочей станции;

3) отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции;

4) некорректного функционирования установленных на рабочей станции технических средств защиты;

- присутствовать при работах по внесению изменений в программные и аппаратные средства, закрепленной за ним рабочей станции в структурном подразделении Министерства.

2. Сотрудникам Министерства запрещается

- использовать средства вычислительной техники в неслужебных целях;
- передавать сведения конфиденциального характера по незащищенным каналам связи (факс, электронная почта и т.п.);
- несанкционированно копировать, распространять, изменять, использовать документы конфиденциального характера;
- самовольно вносить какие-либо изменения в конфигурацию программного обеспечения и аппаратных средств или устанавливать дополнительно любые программные обеспечения и аппаратные средства, не предусмотренные карточкой рабочего места;
- осуществлять обработку конфиденциальной информации в присутствии посторонних, не допущенных к данной информации, лиц;
- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра свою рабочую станцию, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было персональное устройство идентификации, машинные носители и распечатки, содержащие персональные данные.

Приложение № 2
к Положению по обеспечению
защиты информации в
Министерстве здравоохранения
Чувашской Республики

ИНСТРУКЦИЯ
по организации резервного копирования информации

1. Периодичность резервного копирования данных

1.1. Резервное копирование данных должно производиться в соответствии с графиком резервного копирования.

1.2. График резервного копирования должен быть составлен для каждого вида информации, подлежащей периодическому резервному копированию.

1.3. Специалист по информационной безопасности должен отслеживать исправность средств резервного копирования, возникновение различных нештатных ситуаций, плановые и неплановые отключения электроэнергии, другие события, наступление которых может привести к потере информации.

2. Порядок резервного копирования данных

2.1. Резервное копирование информации производится в соответствии с документацией на используемое программное обеспечение.

2.2. Резервное копирование информации должно производиться с исключением любых рисков потери информации.

3. Хранение резервных копий данных

3.1. Резервные копии данных должны храниться вместе с инструкцией по восстановлению данных из резервных копий.

3.2. Хранение резервных копий данных должно быть организовано в отдельном помещении от используемых данных.

3.3. Хранение резервных копий данных должно быть организовано с соблюдением правил, исключающих несанкционированный доступ к данным.

4. Восстановление данных после сбоя

Восстановление данных из резервной копии производится в соответствии с документацией на используемое программное обеспечение, с составлением при необходимости акта и уведомлением руководителя структурного подразделения Министерства.

Приложение № 3
к Положению по обеспечению
защиты информации в
Министерстве здравоохранения
Чувашской Республики

Инструкция
по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы

Настоящей инструкцией регламентируется взаимодействие структурных подразделений Министерства по обеспечению защиты конфиденциальной информации при проведении модификаций программных обеспечений, технического обслуживания средств вычислительной техники.

Право внесения изменений в конфигурацию аппаратных средств информационной системы предоставляется специалисту, ответственному по защите информации, и специалисту по информационному обеспечению согласно их должностных инструкций. Изменение программного обеспечения может быть произведено специалистом БУ «Медицинский информационно-аналитический центр» Министерства здравоохранения Чувашской Республики по согласованию со специалистом, ответственным по защите информации, или специалистом по информационному обеспечению.

Изменение программного обеспечения и конфигурации аппаратных средств информационной системы кем-либо, кроме вышеперечисленных специалистов запрещено.

Процедура внесения изменений в конфигурацию аппаратных и программных средств информационной системы инициируется заявкой руководителя структурного подразделения Министерства (приложение № 1 к настоящей инструкции).

В заявках могут указываться следующие виды необходимых изменений:

- установка нового оборудования (рабочей станции, сервера, средства связи, телекоммуникаций);
- замена оборудования;
- изъятие оборудования;
- добавление устройства (узла, блока) в состав оборудования;
- замена устройства (узла, блока) в составе оборудования;
- изъятие устройства (узла, блока) из состава оборудования;
- установка программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи);
- обновление (замена) программных средств, необходимых для решения определенной задачи;
- удаление программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи).

В заявке указываются условные наименования рабочей станции, серверов, средств связи, телекоммуникаций.

Заявка передается специалисту, ответственному по защите информации, или специалисту по информационному обеспечению для непосредственного исполнения работ по внесению изменений в программное обеспечение и конфигурацию аппаратных средств информационной системы.

После проведения модификации программного обеспечения на рабочей станции специалист по информационному обеспечению производит контроль на наличие вирусов. Если рабочая станция или сервер относятся к защищаемым оборудованиям, то установка (снятие), внесение необходимых изменений настройки средств защиты от несанкционированного доступа и средств контроля целостности файлов осуществляется совместно со специалистом, ответственным по защите информации.

Установка и обновление общего программного обеспечения (системного, тестового и т.п.) на рабочие станции и серверы производится с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, а прикладного программного обеспечения - с эталонных копий программных средств.

После установки (обновления) программного обеспечения специалист по информационному обеспечению производит настройку средств управления доступом к компонентам данной задачи в соответствии с ее формуляром и совместно со специалистом структурного подразделения Министерства проверяет работоспособность программного обеспечения и правильность настройки средств защиты.

После завершения работ по внесению изменений в конфигурацию аппаратных средств защищенной рабочей станции ее системный блок опечатывается специалист по информационному обеспечению. Специалист по информационному обеспечению вместе со специалистом, ответственным по защите информации, делают отметку о выполненных работах на обратной стороне заявки и оставляют на хранение вместе с Карточкой рабочего места (приложение № 2 к настоящей инструкции).

Заявки, на основании которых производились изменения в составе технических или программных средств, хранятся у специалист по информационному обеспечению вместе с Карточкой рабочего места.

Они могут использоваться:

- для восстановления конфигурации рабочей станции после возникновения нештатных ситуаций;
- для контроля правомерности установки на рабочей станции программных и технических средств;
- для проверки правильности установки и настройки средств защиты рабочей станции.

Приложение № 1
к инструкции по установке,
модификации и техническому
обслуживанию программного
обеспечения и аппаратных
средств информационной
системы

ЗАЯВКА
на внесение изменений в конфигурацию программного обеспечения и аппаратных средств информационной системы

Прошу произвести следующие изменения в конфигурацию программного обеспечения и аппаратных средств информационной системы

_____
(наименование подразделения)

- установка нового оборудования (рабочей станции, сервера, средства связи, телекоммуникаций);
- замена оборудования;
- изъятие оборудования;
- добавление устройства (узла, блока) в состав оборудования;
- замена устройства (узла, блока) в составе оборудования;
- изъятие устройства (узла, блока) из состава оборудования;
- установка программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи);
- обновление (замена) программных средств, необходимых для решения определенной задачи;
- удаление программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи),

_____
(отметить нужное)

необходимые для решения следующих задач:

_____

_____

_____

_____

_____

Руководитель структурного
подразделения Министерства _____ _____
(подпись) (фамилия и инициалы)

«___» _____ 20___ г.

(оборотная сторона заявки)

Отметка о выполнении
(внесении изменений в конфигурацию программного обеспечения и аппаратных средств информационной системы)

В соответствии с Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и технических средств информационной системы специалистом, ответственным по защите информации, или специалистом по информационному обеспечению:

_____
(ФИО)

указанные в заявке изменения внесены (не внесены по следующей причине)

_____
(краткое пояснение причины)

_____

_____

Специалист по информационному обеспечению: _____ (подпись) _____ (фамилия и инициалы)

Специалист, ответственный по защите информации: _____ (подпись) _____ (фамилия и инициалы)

«_____» _____ 20___ г.

Приложение № 2
к инструкции по установке,
модификации и техническому
обслуживанию программного
обеспечения и аппаратных
средств информационной
системы

Карточка рабочего места

Дата _____

Структурное подразделение _____

Ф.И.О. пользователя _____

		Наименование	Серийный номер	
Монитор				
Системный блок				
	Материнская плата			
	Процессор			
	Винчестер			
	Винчестер			
	Винчестер			
	Память			
	Память			
	Память			
	Звуковая карта			
	Сетевая карта			
	Дисковод 3,5			
	Дисковод 3,5			
	CD-ROM			
	Видеокарта			
	Средство ЗИ			
Клавиатура				
Манипулятор мышь				
Принтер				
Звуковые колонки				
И.Б.П.				

Специалист по информационному обеспечению _____ _____

(подпись) (ФИО)

(обратная сторона карточки рабочего места)

Установленное программное обеспечение

№	Наименование	Путь установки	Дата
1	MS Windows 10 Pro		
2	MS Office 2010		
3	Win Rar		
4			

Пользователь _____ _____
(подпись) (ФИО)

Специалист по информационному обеспечению: _____ _____
(подпись) (ФИО)

Специалист, ответственный по защите информации _____ _____
(подпись) (ФИО)

Приложение № 4
к Положению по обеспечению
защиты информации в
Министерстве здравоохранения
и социального развития
Чувашской Республики

Инструкция
о порядке обращения со съемными накопителями информации

1. Организация учета и хранения съемных накопителей информации

1.1. Все вновь приобретенные съемные накопители информации учитываются специалистом, ответственным по защите информации, путем регистрации в журнале учета съемных накопителей информации (приложение № 1 к настоящей инструкции) и присвоения унифицированного учетного номера.

1.2. Ответственность за организацию работ по учету и хранению съемных накопителей информации возлагается на специалиста, ответственного по защите информации.

1.3. В целях обеспечения учета и хранения съемных накопителей информации специалист ответственный по защите информации обеспечивает выполнение следующих основных функций:

- принимает, учитывает, выдает и хранит съемные накопители информации;
- подготавливает съемные накопители информации на уничтожение в случае обнаружения дефекта.

2. Учет и выдача съемных накопителей информации

2.1. Выдачу съемных накопителей информации сотрудникам структурных подразделений Министерства осуществляет специалист, ответственный по защите информации.

2.2. Передача съемных накопителей информации с конфиденциальной информацией сторонним организациям производится с разрешения министра, заместителя министра, ответственного за защиту информации, руководителя структурного подразделения министерства.

3. Обращение со съемными накопителями информации

3.1. При хранении съемных накопителей информации и в процессе их эксплуатации необходимо обеспечить защиту от физических повреждений.

3.2. Ответственность за организацию в структурных подразделениях Министерства работ по использованию съемных накопителей информации возлагается на руководителя структурного подразделения министерства.

3.3. Руководитель структурного подразделения Министерства осуществляет контроль за информацией, передаваемой на съемных накопителях информации.

3.4. Запрещается использовать неучтенные съемные накопители информации и записывать посторонние программы. Перед использованием съемных накопителей информации необходимо проверить их на наличие вирусов.

3.5. При выявлении пользователем действий, направленных на несанкционированное использование или хищение съемных накопителей информации, он обязан немедленно сообщить об этом своему непосредственному руководителю структурного подразделения Министерства.

4. Уничтожение съемных накопителей информации

4.1. Съемные накопители информации подлежат физическому уничтожению в случае невосстанавливаемого физического повреждения.

4.2. Отбор съемных накопителей информации для уничтожения производится специалистом, ответственным по защите информации.

4.3. Уничтожение съемных накопителей информации производится специалистом, ответственным по защите информации, с оформлением акта (приложение № 2 к настоящей инструкции). В учетных формах делается ссылка на соответствующий акт.

Приложение № 1
к инструкции о порядке обращения со съемными накопителями информации

Типовая форма
журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов
(для обладателя конфиденциальной информации)

N п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение № 2
к инструкции о порядке
обращения со съемными накопи-
телями информации

УТВЕРЖДАЮ
Председатель технической комис-
сии по вопросам защиты информа-
ции Министерства здравоохранения
Чувашской Республики

_____ _____
(подпись) (Ф.И.О)
«_____» _____ 20___ г.

АКТ № _____
от «_____»_____ 20 г.

Техническая комиссия по вопросам защиты информации Министерства здравоохранения Чувашской Республики, созданная приказом Министерства здравоохранения Чувашской Республики от «__» _____ 20__ г. № _____, в составе:

председателя - _____
членов комиссии - _____
_____
_____
_____

составила настоящий акт о том, что были уничтожены следующие съемные накопители информации - _____
_____
_____

Председатель комиссии _____ / _____ /
Члены комиссии _____ / _____ /
_____ / _____ /
_____ / _____ /

Приложение № 5
к Положению по обеспечению
защиты информации в
Министерстве здравоохранения
Чувашской Республики

ИНСТРУКЦИЯ
по организации антивирусной защиты

1. Общие положения

1.1. Настоящая Инструкция является обязательной для исполнения всеми сотрудниками министерства, эксплуатирующими средства вычислительной техники.

1.2. Антивирусная защита - комплекс правовых, организационных, технических и технологических мер, применяемых для обеспечения защиты средств вычислительной техники и информационных систем от воздействия компьютерных вирусов.

Компьютерные вирусы - это специально разработанные программы, программные модули, блоки, группы команд, умышленно включаемые в программное обеспечение с целью дезорганизации вычислительного процесса (существенного замедления обработки информации), осуществления модификации (изменения, стирания) хранящихся на магнитных носителях программ и данных.

Антивирусное средство - программное средство, предназначенное для выявления фактов вирусного воздействия на средства вычислительной техники и обладающее средствами восстановления их исходного состояния.

1.3. Целями антивирусной защиты является противодействие угрозам нарушения целостности обрабатываемой информации, сохранение работоспособности информационной системы и её восстановление с минимальными финансовыми издержками и временными затратами.

1.4. Основными принципами антивирусной защиты являются:

- использование в работе только лицензионного программного обеспечения;
- периодическое создание архивных копий файлов, с которыми ведётся работа;
- проверка всех съемных носителей информации и файлов, полученных по электронной почте, из Интернета или от организаций, на наличие вирусов перед их использованием;
- периодическая проверка средств вычислительной техники на наличие вирусов, с использованием последней версии антивирусной программы.

1.5. Инструкция регламентирует действия сотрудников подразделений министерства при организации антивирусной защиты электронных технологий министерства.

2. Организация антивирусной защиты

2.1. Реализация мероприятий антивирусной защиты возложена на специалиста, ответственного по защите информации, и специалиста по информационному обеспечению.

2.2. На специалиста, ответственного по защите информации, возлагается:

- разработка и согласование проектов нормативных документов по организации антивирусной защиты;
- определение потребностей в антивирусных средствах;

- анализ состояния антивирусной защиты, разработка мероприятий по ее совершенствованию;

- внесение предложений по ежегодной закупке антивирусного программного обеспечения, продлению договоров на его техническую поддержку и сопровождение.

2.3. На специалиста по информационному обеспечению возлагается:

- регулярное получение новых версий антивирусного программного обеспечения, систематическое обновление антивирусных баз;

- доведение программного обеспечения до всех сотрудников структурных подразделений министерства, эксплуатирующих средства вычислительной техники;

- контроль за осуществлением антивирусной защиты;

- проведение расследований случаев заражения средств вычислительной техники вирусами, принятие мер к локализации и уничтожению вирусов.

3. Установка и обновление антивирусных средств

3.1. К применению в министерстве допускаются лицензионные антивирусные средства AVP Касперского.

3.2. Установка и регулярное обновление антивирусных средств осуществляется специалистом по информационному обеспечению.

3.3. Антивирусные средства устанавливаются на соответствующих серверах министерства и рабочих станциях в структурных подразделениях Министерства.

3.4. Обновление антивирусного программного обеспечения производится по мере получения новых версий. Антивирусные базы обновляются автоматически 1 раз в день.

4. Контроль за осуществлением антивирусной защиты

4.1. Установка (изменение) системного и прикладного программного обеспечения компьютера и локально-вычислительной сети должна осуществляться только специалистом по информационному обеспечению или специалистом, ответственным по защите информации.

4.2. Устанавливаемое (изменяемое) системное и прикладное программное обеспечение должно быть проверено на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) системного и прикладного программного обеспечения, компьютер и локально-вычислительную сеть необходимо проверить на наличие компьютерных вирусов.

4.3. Настройка антивирусных средств должна обеспечивать автоматический контроль на наличие компьютерных вирусов при каждой перезагрузке компьютера (для серверов локально - вычислительной сети - при перезапуске).

4.4. Обязательной проверке на отсутствие компьютерных вирусов подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация со съёмных носителей (магнитные диски, CD-ROM, флешки и т.п.), получаемых от сторонних лиц и организаций.

4.5. Контроль информации на съёмных носителях производится перед её использованием непосредственно в структурных подразделениях Министерства.

4.6. Особое внимание следует обратить на использование съёмных носителей, принадлежащих лицам, временно допущенным к работе на компьютере в министерстве (студенты-практиканты, сотрудники подведомственных организаций и т.п.). Работа этих лиц должна проводиться под непосредственным контролем руко-

водителя структурного подразделения министерства, особенно если работа происходит с использованием ресурсов локально-вычислительной сети.

5. Действия при обнаружении компьютерного вируса

5.1. При возникновении подозрения на наличие компьютерного вируса сотрудник структурного подразделения министерства должен провести внеочередную проверку на наличие или отсутствие компьютерного вируса.

5.2. При обнаружении компьютерного вируса необходимо:

- приостановить работу, поставить в известность о факте обнаружения заражённых вирусом файлов руководителя структурного подразделения министерства, специалиста по информационному обеспечению, владельца этих файлов, а также структурные подразделения министерства, использующие эти файлы в работе;
- совместно с владельцем заражённых вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение заражённых вирусом файлов антивирусными средствами, при невозможности или неэффективности лечения уничтожить заражённые вирусом файлы способом, исключающим их восстановление.

6. Ответственность при организации антивирусной защиты

6.1. Руководители структурных подразделений министерства несут персональную ответственность за антивирусную защиту в своих структурных подразделениях министерства, осуществляя постоянный контроль за выполнением сотрудниками структурного подразделения министерства правил антивирусной защиты информации.

6.2. Ответственность за выполнение положений настоящей Инструкции возлагается на руководителей структурных подразделений министерства.

6.3. Периодический контроль за соблюдением положений настоящей Инструкции возлагается на специалиста, ответственного по защите информации.

Приложение № 6
к Положению по обеспечению
защиты информации в
Министерстве здравоохранения
Чувашской Республики

ИНСТРУКЦИЯ
по организации парольной защиты информации

1. Общие положения

1.1. Настоящая Инструкция устанавливает требования о необходимости разграничения доступа должностных лиц к информационным ресурсам, хранящимся в персональных компьютерах, вычислительных сетях и базах данных информационных систем министерства.

1.2. Настоящая Инструкция определяет правила выработки, назначения, изменения и ввода имен пользователей и паролей разграничения доступа к указанным информационным ресурсам, порядок работы с парольной документацией.

1.3. Настоящая Инструкция является составной частью комплексной системы защиты от несанкционированного доступа к информационным ресурсам и обязательна к исполнению всеми сотрудниками министерства.

1.4. Имя пользователя представляет собой последовательность символов установленного формата, позволяющую однозначно аутентифицировать пользователя при входе в систему и проведении им каких-либо действий над информационными ресурсами.

1.5. Пароль, как средство идентификации доступа пользователей в компьютерной сети, используется для защиты от несанкционированного доступа к средствам вычислительной техники, сетям, базам данных информационных систем и представляет собой буквенную, цифровую или буквенно-цифровую группу символов определенной длины.

1.6. В системе пользователю присваиваться персональные имя и пароль для доступа к определенным информационным ресурсам. При этом устанавливаются следующие уровни защиты:

- пароль на включение персонального компьютера;
- имя и пароль для аутентификации-идентификации пользователей на доступ к работе в сети;
- имя и пароль для аутентификации-идентификации пользователей при обращении к базам данных (по каждой базе данных отдельно).

2. Правила формирования личного пароля

2.1. Личные пароли должны выбираться сотрудниками министерства самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее восьми символов;
- в числе символов пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы, такие, как ~ ! @ # $ % ^ & * ( ) - + _ = \ | / ;
- пароль должен легко запоминаться;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.п.), а также общепринятые сокращения (ЭВМ, ЛВС, User и т.п.).

2.2. При выборе пароля надо учитывать ограничения конкретных систем и программ, которые не могут соответствовать таким требованиям (например, не все программы позволяют вводить пробелы в пароле или длина пароля может быть ограничена до какого-либо числа символов).

2.3. Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

2.4. Ввод пароля должен осуществляться с учётом регистра (верхний - нижний), в котором пароль был задан и с учётом текущей раскладки клавиатуры (RU-EN).

2.5. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или отражённом свете) или техническими средствами (видеокамеры, фотоаппараты, телефоны и др.).

2.6. Личный пароль сотрудники министерства не имеют права сообщать никому.

3. Организация парольной защиты разграничения доступа к информации

3.1. Одним из условий нормального функционирования системы защиты информации от несанкционированного доступа является проведение следующих мероприятий:

- внесение изменений в Перечень сведений конфиденциального характера, имеющихся в Министерстве;
- внесение изменений в Список должностей, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных в Министерстве;
- внесение изменений в Список лиц, допущенных к обработке персональных данных в Министерстве;
- разграничение прав доступа к конфиденциальной информации.

Указанные мероприятия должны проводиться периодически, но не реже одного раза год.

3.2. Предоставление пользователям необходимых прав доступа к информационным ресурсам осуществляют руководители структурных подразделений Министерства. Список сотрудников министерства, имеющих доступ к конфиденциальной информации (приложение № 1 к настоящей Инструкции) к защищаемым информационным ресурсам, согласно их функциональным обязанностям, представляются специалисту ответственному по защите информации.

3.3. Специалистом ответственным по защите информации на основании Списка сотрудников министерства, имеющих доступ к конфиденциальной информации, представленных руководителями структурных подразделений министерства, формируется общий список, который утверждается министром.

3.4. Настройка системных средств разграничения правил доступа осуществляется специалистом по информационному обеспечению средствами сетевого программного обеспечения на серверах, а при необходимости, в условиях распределенной сети и на рабочих станциях в соответствии со Списком сотрудников министерства, имеющих доступ к конфиденциальной информации.

4. Порядок смены паролей сотрудников министерства

4.1. Полная плановая смена паролей сотрудников министерства должна проводиться регулярно, не реже одного раза в месяц.

4.2. Внеплановая смена личного пароля сотрудника министерства в случае прекращения его полномочий (увольнение, перевод на другую работу и т.п.) должна производиться специалистом по информационному обеспечению немедленно после окончания последнего сеанса работы данного сотрудника министерства с системой.

4.3. Внеплановая полная смена паролей всех сотрудников министерства должна производиться в случае прекращения полномочий (увольнение, перевод на другую работу и другие обстоятельства) системного администратора и специалиста, ответственного по защите информации, которым по роду работы были предоставлены полномочия по управлению парольной защитой информации.

4.4. Смена личного пароля производится самостоятельно каждым сотрудником министерства в соответствии с планом, или же ввиду каких-либо особых случаев.

4.5. При смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.

4.6. Специалист по информационному обеспечению оказывает необходимую помощь сотрудникам министерства в процессе смены пароля.

5. Хранение пароля

5.1. Всем сотрудникам министерства запрещается:

- проводить работы, связанные с решением задач конфиденциального характера, без выполнения мероприятий по защите информации;
- допускать к решению задач конфиденциального характера лиц, не имеющих к ним отношения и не включенных в список сотрудников министерства, имеющих доступ к конфиденциальной информации;
- записывать пароли на бумаге, в файле, электронной записной книжке, также на других окружающих предметах (на клавиатуре, мониторе, и т.п.);
- сообщать другим сотрудникам министерства личный пароль и регистрировать их в системе под своим паролем.

5.2. При увольнении сотрудника министерства, руководитель структурного подразделения министерства обязан в срок не более 1 (одного) рабочего дня сообщить об этом специалисту ответственному по защите информации или специалисту по информационному обеспечению. Специалист по информационному обеспечению удаляет имя и пароль, соответствующие этому сотруднику министерства, из средств электронно-вычислительной техники.

6. Действия в случае утери и компрометации пароля

6.1. Под компрометацией пароля понимается: утрата, хищение, несанкционированное копирование содержания парольной документации (Список сотрудников министерства, имеющих доступ к конфиденциальной информации), разглашение паролей лицам, которые не должны иметь доступ к информационным ресурсам системы или другая ситуация, которая может сложиться с паролем, когда информация о паролях становится известной.

6.2. При компрометации паролей сотрудник министерства обязан немедленно сообщить о случившемся специалисту по информационному обеспечению, своему непосредственному руководителю и сменить пароль в соответствии с выше-

указанными требованиями.

7. Ответственность при организации парольной защиты

7.1. Ответственность за организацию парольной защиты возлагается на специалиста, ответственного по защите информации, специалиста по информационному обеспечению и руководителя подразделения.

7.2. Периодический контроль за соблюдением требований данной Инструкции возлагается на специалиста, ответственного по защите информации.

7.3. Сотрудники министерства должны быть ознакомлены с данной инструкцией и предупреждены об ответственности за использование паролей не соответствующих требованиям, а также за разглашение парольной информации.