МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ

ПРИКАЗ

От 19.02.2018 № 267
г. Симферополь

О утверждении концепции информационной безопасности.

Согласно Положению о Министерстве здравоохранения Республики Крым (далее – Министерство), утвержденному постановлением Совета министров Республики Крым от 27.06.2014 № 149, с целью подготовки к закупке услуги уполномоченной фармацевтической организации,

ПРИКАЗЫВАЮ:

1. Утвердить концепцию информационной безопасности государственной информационной системы «Единая медицинская информационная система здравоохранения Республики Крым», согласно приложению № 1 к настоящему приказу.
2. Контроль за исполнением настоящего приказа возложить на заместителя министра здравоохранения Н.Н. Деркача.

МИНИСТР **А. ГОЛЕНКО**

Приложение № 1
к приказу Министерства здравоохранения
Республики Крым от
«19.02.2018» № 267

Концепция информационной безопасности государственной информационной системы «Единая медицинская информационная система здравоохранения Республики Крым»

Перечень сокращений и определений

3. Единая государственная информационная система в сфере здравоохранения (далее - **ЕГИСЗ**) – совокупность информационно-технологических и технических средств, обеспечивающих информационную поддержку методического и организационного обеспечения деятельности участников системы здравоохранения.
4. Единая медицинская информационная система здравоохранения Республики Крым (**далее - ЕМИСЗ РК**) – государственная информационная система Республики Крым, состоящая из комплекса программных и технических средств, баз данных, обеспечивающих информационно-технологическую поддержку функционирования системы здравоохранения Республики Крым, и предназначенную для выполнения функций регионального фрагмента ЕГИСЗ.
5. Министерство здравоохранения Республики Крым (**далее – МЗ РК**) – исполнительный орган государственной власти Республики Крым, проводящий государственную политику и осуществляющий функции по нормативно-правовому регулированию в сфере охраны здоровья граждан на территории Республики Крым, контроль в сфере охраны здоровья, отраслевое или межотраслевое управление в наиболее важных отраслях и установленных сферах деятельности, оказание государственных услуг в сфере охраны здоровья и управление государственным имуществом, а также координирующий в установленных случаях деятельность в этой сфере иных исполнительных органов государственной власти Республики Крым.
6. Медицинская организация (**далее – МО**) – организация, осуществляющая деятельность в области здравоохранения или оказания медицинских услуг, поддерживающая развитие медицины как науки, занимающаяся мероприятиями по поддержанию здоровья и оказания медицинской помощи людям посредством изучения, диагностики, лечения и возможной профилактики болезней и травм.
7. Оператор информационной системы (**далее – оператор**) – физическое или юридическое лицо, осуществляющее деятельность по эксплуатации информационной систем, в том числе по обработке информации, содержащейся в ее базе данных.
8. Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
9. Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
10. Информационная безопасность – непрерывный во времени процесс обеспечения конфиденциальности (кроме общедоступной информации), целостности и доступности защищаемой информации.
11. Средства обеспечения информационной безопасности ЕМИСЗ РК – технические и организационные меры, используемые для обеспечения информационной безопасности ЕМИСЗ РК.
12. Информация – сведения (сообщения, данные) независимо от формы их представления.
13. Государственные информационные системы (**далее – ГИС**) – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.
14. Персональные данные (**далее – ПДн**) – 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.
15. Пользователи ЕМИСЗ РК – сотрудники МО, сотрудники органа управления здравоохранением, пациенты МО, иные участники информационного взаимодействия в сфере здравоохранения (на основании заключенных договоров), участвующие в

ЕМИСЗ РК имеет клиент-серверную архитектуру, включает серверную часть, состоящую из сервера баз данных, сервера приложений, веб-сервера, и клиентскую часть – «тонкого клиента» (веб-браузера) и реализуется для работы по модели «облачных вычислений». В состав объектов защиты ЕМИСЗ РК входят автоматизированные рабочие места, серверы, структурированная кабельная система, средства защиты информации.

Основные цели и задачи обеспечения информационной безопасности

3.1. Цели обеспечения информационной безопасности

Основными целями обеспечения информационной безопасности являются:

– предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию;

– повышение качества оказания населению государственных и муниципальных услуг в электронном виде в сфере здравоохранения;

– повышение эффективности использования современных информационных технологий;

– соответствие применяемых мер защиты информации действующему законодательству Российской Федерации, нормативным и методическим документам уполномоченных органов.

3.2. Задачи обеспечения информационной безопасности

Задачами деятельности по обеспечению информационной безопасности являются:

– формирование и проведение единой политики в области обеспечения защиты информации в ЕМИСЗ РК;

– формирование единых требований к АРМ пользователей ЕМИСЗ РК;

– координация деятельности МО при разработке организационно-распорядительной документации по защите информации, содержащейся в ЕМИСЗ РК.

– поддержание системы информационной безопасности в состоянии, устойчивом к существующим и вновь выявляемым угрозам в информационной сфере;

– разработка и внедрение в информационную инфраструктуру МО современных методов и средств обеспечения информационной безопасности;

– организация контроля состояния и оценки эффективности системы информационной безопасности и реализация мер по ее совершенствованию.

Правовые основы деятельности по обеспечению безопасности персональных данных

Деятельность по обеспечению информационной безопасности, должна осуществляться в рамках действующего законодательства, руководящих документов уполномоченных государственных органов исполнительной власти, рекомендаций Министерства здравоохранения РФ, ведомственных документов МЗ РК и настоящей Концепции.

В части организации обработки и защиты персональных данных следует руководствоваться следующими документами:

– Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».

– Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

– Федеральный закон от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

– Постановление Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

– Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление Правительства РФ №1119).

– реализация единой технической политики в части информационной безопасности при организации работ;

– мониторинг внутренних и внешних условий функционирования объектов защиты, анализ эффективности управления защитой информации и подготовка решений по корректировке состава и содержания структурных элементов системы обеспечения информационной безопасности.

Состав Рабочей группы и Положение о Рабочей группе утверждается приказом МЗ РК.

В рамках обеспечения информационной безопасности ЕМИСЗ РК технический оператор обеспечивает:

– организацию процесса разработки методических документов в сфере информационной безопасности МО;

– информирование МО РК о необходимых мероприятиях по обеспечению информационной безопасности;

– контроль выполнения мероприятий по обеспечению информационной безопасности в МО.

Руководители МО:

– организуют работу по обеспечению информационной безопасности в учреждениях здравоохранения Республики Крым;

– создают подразделение (назначают сотрудника), отвечающее за обеспечение информационной безопасности;

– назначают лицо, ответственное за организацию обработки ПДн (им может быть в том числе руководитель МО);

– согласуют изменения в программном и аппаратном обеспечении АРМ ЕМИСЗ РК с Рабочей группой.

Работники МО, ответственные за организацию обработки персональных данных:

– организуют взаимодействие с субъектами персональных данных в соответствии с требованиями законодательства РФ;

– доводят до сведения работников МО положения законодательства Российской Федерации, локальных актов МЗ РК по вопросам обработки персональных данных, требований к защите персональных данных;

– осуществляют внутренний контроль соблюдения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных и доводят результаты контроля до МЗ РК.

Средства обеспечения информационной безопасности ЕМИСЗ РК

6.1. Общие положения.

Средства обеспечения информационной безопасности ЕМИСЗ РК – технические и организационные меры, используемые для обеспечения информационной безопасности ЕМИСЗ РК.

Защита информации, содержащейся в информационных системах, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания и в ходе эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы защиты информации информационной системы (далее – подсистема защиты информации).

6.2. Порядок создания системы защиты информации в информационных системах.

В общем случае порядок создания систем защиты информации приведен в ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Создание системы защиты информации должно выполняться в следующем порядке:

– формирование требований к защите информации, содержащейся в информационной системе;

6.3. Мероприятия по обеспечению информационной безопасности

Мероприятия по обеспечению информационной безопасности ЕМИСЗ РК должны носить упреждающий характер и быть направленными на предотвращение инцидентов, связанных с угрозами безопасности информации.

При выборе мер защиты информации, обрабатываемой с применением средств автоматизации необходимо определить актуальные угрозы для данной ИС, тип обрабатываемых данных, тип самой ИС, ее класс защищенности и иные параметры, определяемые действующим законодательством в качестве основополагающих при выборе правил и мер защиты информации.

В целях нейтрализации угроз безопасности информации применяются организационные и технические меры защиты информации.

Организационные меры обеспечения информационной безопасности предусматривают:

– назначение ответственных за организацию обработки ПДн, за обеспечение безопасности информационной системы, за техническое обслуживание информационной системы, за проведение мероприятий по обезличиванию обрабатываемых ПДн, за хранение материальных носителей информации;

– ознакомление сотрудников с законодательством и внутренними документами МЗ РК в области информационной безопасности;

– обучение сотрудников, непосредственно осуществляющих обработку ПДн, правилам безопасной работы с персональными данными;

– повышение квалификации специалистов по защите информации и лиц, ответственных за организацию защиты информации;

– назначение ответственности сотрудников и руководителей всех уровней за выполнение установленных требований по защите информации;

– проведение контроля соблюдения сотрудниками требований по обеспечению информационной безопасности;

– обезличивание ПДн в случаях, когда не требуется определение субъекта персональных данных;

– прием и обработку обращений и запросов субъектов ПДн или их представителей;

– установление уровней защищенности ПДн в ИСПДн;

– установление класса защищенности ГИС;

– оценку вреда, который может быть причинен субъектам ПДн в случае нарушения требований Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей по защите ПДн;

– уведомление уполномоченного органа по защите прав субъектов ПДн (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) о начале обработки ПДн в соответствии со ст.22 Федерального закона № 152-ФЗ;

– выявление угроз безопасности и разработку моделей угроз и нарушителя;

– управление доступом сотрудников к информационной системе;

– назначение минимально необходимых прав и привилегий пользователям;

– регистрацию всех действий пользователей;

– обучение пользователей и персонала, обслуживающего системы защиты информации, правилам и способам работы с подсистемой информационной безопасности;

– учет машинных носителей информации;

– применение средств защиты информации, прошедших обязательный контроль соответствия требованиям нормативных документов по защите информации;

– мероприятия по обеспечению физической безопасности средств вычислительной техники и материальных носителей информации;

– оценку эффективности реализованных мер по обеспечению безопасности ПДн (аттестация ЕМИСЗ РК и ее сегментов по требованиям безопасности информации);

– унификацию и стандартизацию средств защиты информации;

– должно быть зарегистрировано в реестре отечественного ПО.

Технический оператор должен осуществлять контроль процесса выполнения разработки ОРД по защите ПДн, обрабатываемых в ЕМИСЗ РК. Для координации деятельности МО РК по разработке ОРД, МЗ РК совместно с техническим оператором организует единое мероприятие по обучению сотрудников МО РК по работе с Региональным ПО.

7.2.2. Реализация технических мер защиты информации.

Перечень технических мер защиты информационных систем формируется в соответствие с требованиями приказов ФСТЭК России № 17 и № 21.

Перечень технических мер защиты информационных систем включает в себя следующие группы:

- Идентификация и аутентификация субъектов доступа и объектов доступа.
- Управление доступом субъектов доступа к объектам доступа.
- Ограничение программной среды.
- Защита машинных носителей информации.
- Регистрация событий безопасности.
- Антивирусная защита.
- Обнаружение вторжений.
- Контроль (анализ) защищенности информации.
- Обеспечение целостности информационной системы и информации.
- Обеспечение доступности информации.
- Защита среды виртуализации.
- Защита технических средств.
- Защита информационной системы, ее средств, систем связи и передачи данных.

Перечень защитных мер должен быть адаптирован применительно к структурно-функциональным характеристикам выбранной информационной системы и особенностям ее функционирования. Допускается исключение из перечня мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе.

При невозможности реализации в информационной системе, в рамках ее системы защиты информации, отдельных выбранных мер защиты информации, могут разрабатываться компенсирующие меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации. Достаточность и адекватность компенсирующих мер подтверждается в ходе аттестационных испытаний информационной системы.

7.3. Средства защиты информации.

В составе подсистемы информационной безопасности информационных систем допускается использовать только средства защиты информации, сертифицированные на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также требуемого класса защищенности. В случае, если с помощью сертифицированных средств защиты невозможно реализовать отдельные защитные меры, должны разрабатываться компенсирующие меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

7.4. Использование существующих средств защиты информации.

Для защиты информации, обрабатываемой в ЕМИСЗ РК, МЗ РК совместно с организацией-лицензиатом ФСТЭК и ФБС России, был выполнен комплекс технических мер, направленных на реализацию требований законодательства в области защиты информации.

Для обеспечения защиты канала связи между операторами ЕМИСЗ РК развернута и функционирует защищенная сеть передачи данных, построенная с использованием технологии ViPNet (сеть ViPNet № 4960).

7.8. Аттестация ЕМИСЗ РК по требованиям защиты информации

Аттестация ЕМИСЗ РК по требованиям защиты информации организуется МЗ РК и включает проведение комплекса организационных и технических мероприятий, в результате которых устанавливается степень соответствия ЕМИСЗ РК безопасности информации.

Аттестация ЕМИСЗ РК проводится МЗ РК с привлечением организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

По результатам аттестационных мероприятий оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям защиты информации и аттестат соответствия в случае положительных результатов аттестационных испытаний.

При выполнении МО РК требований настоящей Концепции, регламента подключения и технического задания допускается аттестация рабочих мест МО ЕМИСЗ РК, реализующих полную технологию обработки информации на основе результатов аттестационных испытаний типового рабочего места ЕМИСЗ РК.

В качестве исходных данных, необходимых для оценки эффективности реализованных мер по обеспечению информационной безопасности, должны использоваться:

– модель угроз информационной безопасности;

– акт установления уровня защищенности или акт классификации ИС;

– техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание подсистемы информационной безопасности;

– проектная и эксплуатационная документация на подсистему информационной безопасности ЕМИСЗ РК;

– организационно-распорядительные документы по защите информации, результаты анализа уязвимостей информационных систем, материалы предварительных и приемочных испытаний системы информационной безопасности информационной системы, а также иные документы, разрабатываемые в соответствии с требованиями уполномоченных органов.

Повторная аттестация информационной системы осуществляется в случае окончания срока действия аттестата соответствия или повышения класса защищенности информационной системы. При увеличении состава угроз безопасности информации или изменения проектных решений, реализованных при создании системы защиты информации информационной системы, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

При необходимости привлечения сторонних организаций к проведению работ по проектированию системы информационной безопасности, внедрению средств защиты информации и аттестации информационных систем, должны привлекаться организации имеющие лицензии ФСТЭК России и ФСБ России на оказание услуг в области защиты конфиденциальной информации.

Общая структура ЕМИСЗ РК

Общая структура ЕМИСЗ РК представлена:

–уровень ядра ЕМИСЗ РК;

–уровень МО РК.

1.1. Уровень ядра ЕМИСЗ РК

Уровень ядра ЕМИСЗ РК располагается у технического оператора и представлен центром обработки данных (далее - ЦОД), в котором располагаются сервера ЕМИСЗ РК, а также необходимое сетевое телекоммуникационное оборудование и каналы связи с МО РК и федеральным сегментом единой государственной информационной системы в сфере здравоохранения. Меры по защите ЦОД и рекомендованный состав средств защиты информации для обеспечения информационной безопасности представлен в разделе 3 настоящего Приложения.

1.2. Уровень МО РК

Уровень МО РК представляет из себя защищенный сегмент локально-вычислительной сети (далее-ЛВС) МО РК, предназначенный для работы с ЕМИСЗ РК, и АРМ в защищенном исполнении.

Защищенный сегмент ЛВС МО РК, предназначенный для работы с ЕМИСЗ, функционирует на основе персональных компьютеров, располагающихся в выделенном сегменте ЛВС МО РК и подключающихся к ЦОД технического оператора посредством организации защищенного взаимодействия по каналам связи. Меры по защите сегмента ЛВС МО РК, предназначенного для работы с ЕМИСЗ РК, и состав средств защиты информации для обеспечения информационной безопасности представлен в разделе 3 настоящего Приложения.

Организация защищенного межсетевого взаимодействия

Для организации защищенного межсетевого взаимодействия по каналам связи общего доступа между всеми участниками ЕМИСЗ РК должна применяться защищенная частная виртуальная сеть ViPNet № 4960.

На уровне технического оператора располагается ядро защищенной сети – ПО ViPNet Administrator, которое обеспечивает централизованное управление элементами сети ViPNet и централизованную рассылку ключей шифрования.

ПАК ViPNet Coordinator HW 2000, установленный у технического оператора в режиме горячего резервирования, обеспечивает безотказное защищенное взаимодействие с учреждениями здравоохранения, а также используется для защиты и разграничения доступа к серверам ЦОД.

На уровне МО РК должна производится установка ПАК ViPNet Coordinator HW1000, обеспечивающих защиту ЛВС МО РК от различных видов сетевых атак, а также реализующих защищенное взаимодействие с другими МО РК и ЦОД технического оператора. При территориальной удаленности зданий МО РК (т.е. в случае, если каждое здание имеет собственную локальную сеть и точку выхода в сети международного обмена), для организации безопасного межсетевого взаимодействия должна быть произведена установка ПАК в каждом территориально удаленном здании. Для отдельных, локально удаленных АРМ производится установка ViPNet Клиент для защищенного взаимодействия с сетью 4960.

Для организации работы персонала с ЕМИСЗ РК в ЛВС МО РК организуется выделенный сегмент. Межсетевое экранирование и защита каналов связи данного сегмента осуществляется ПАК ViPNet Coordinator. В случае необходимости использования дополнительных АРМ (персональных компьютеров) в качестве тонких клиентов, необходимо подключить данные АРМ к выделенному сегменту ЛВС и выполнить мероприятия по их защите. Меры по защите АРМ, используемых в качестве тонких клиентов для работы с ЕМИСЗ РК, и состав средств защиты информации для обеспечения информационной безопасности представлен в разделах 3.3-3.7.

3.5. Средства антивирусной защитыю.

В соответствии с приказом ФСТЭК России № 17, должны быть реализованы меры по антивирусной защите (АВЗ).

Антивирусное программное обеспечение должно иметь сертификат ФСТЭК России на соответствие требованиям документов «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа А четвертого класса защиты. ИТ.САВЗ.А4.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ» (ФСТЭК России, 2012) и «Профиль защиты средств антивирусной защиты типа В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Г четвертого класса защиты. ИТ.САВЗ.Г4.ПЗ».

Для антивирусной защиты серверов и АРМ пользователей ЕМИСЗ РК используется ссертифицированное ФСТЭК России АВПО Kaspersky Anti-Virus.

3.6. Средства анализа защищенности.

В соответствии с приказом ФСТЭК России № 17, для установленного класса ЕМИСЗ РК должны быть реализованы меры по выявлению и анализу уязвимостей информационной системы, контроль правильности настройки программного обеспечения и средств защиты информации (АНЗ).

Требования по анализу защищенности должны реализовываться сертифицированным ФСТЭК России средством защиты информации с функциями по сканированию защищенности компонентов ГИС и обнаружению уязвимостей, содержащихся в компонентах информационной системы.

Средство защиты информации с функциями сканирования защищенности компонентов ГИС и обнаружения уязвимостей должно иметь сертификат ФСТЭК России на соответствие 4-му уровню контроля отсутствия НДВ.

3.7. Средства обнаружения вторжений.

В соответствии с приказом ФСТЭК России № 17, для установленного класса ЕМИСЗ РК должны быть реализованы меры по обнаружению вторжений в сетевом трафике (СОВ.1), автоматическое обновление базы сигнатур атак (СОВ.2).

Требования по обнаружению вторжений должны быть реализованы с использованием сертифицированного ФСТЭК и ФСБ России средства защиты информации с функцией обнаружения вторжений. Средство обнаружения вторжений устанавливается на границе подключения ЕМИСЗ РК к сети связи общего пользования.

Средство защиты информации с функцией обнаружения вторжений должно иметь сертификат ФСТЭК России на соответствие 4 классу защиты для СОВ и сертификат ФСБ России на соответствие классу В для систем обнаружения компьютерных атак.

В качестве средства обнаружения вторжений в ЦОД ЕМИСЗ РК установлен ПАК ViPNet IDS 2(версия 2.4), который полностью выполняет требования приказа ФСТЭК России № 17 и обладает необходимыми сертификатами ФСТЭК России и ФСБ России.

4. Изменение состава средств защиты информации ЕМИСЗ РК

Состав средств защиты информации, используемых в целях защиты информации, подлежит изменению только при:

– изменении законодательства Российской Федерации в области обработки и защиты персональных данных;

– изменении актуальных угроз безопасности персональных данных;

– значительных изменений технологического процесса обработки персональных данных;

– изменении технологии построения защищенной сети;

– окончании срока действия сертификатов соответствия ФСТЭК России и ФСБ России на используемые средства защиты.