УТВЕРЖДАЮ:

Руководитель управления информационных технологий министерства здравоохранения Самарской области

_____ Бондаренко В.В.

«_____» _____ 2015 г.

УТВЕРЖДАЮ:

Генеральный директор
ООО «ИК «ХОСТ»

_____ Суслов К.Ю.

«_____» _____ 2015 г.

Самарская область
Государственная информационная система

Программное обеспечение

наименование программы

«Регистр медицинских справок»

Руководство администратора

наименование документа

Обеспечение информационной безопасности

75746556.425730.002.И3.09.3

листов: 17

объем документа

СОГЛАСОВАНО:

Директор ГБУЗ «Самарский областной медицинский информационно-аналитический центр»

_____ Сорокин С.Г.

«_____» _____ 2015 г.

СОГЛАСОВАНО:

Менеджер проекта
ООО «ИК «ХОСТ»

_____ Колташева А.С.

«_____» _____ 2015 г.

Аннотация

Настоящий документ представляет собой руководство администратора по обеспечению информационной безопасности программного обеспечения государственной информационной системы Самарской области «Регистр медицинских справок» (далее – *ПО*, *система, ПО «Регистр медицинских справок»*).

Документ является частью рабочей документации на ПО «Регистр медицинских справок». Настоящий документ непосредственно предназначен для Администратора безопасности информации – должностного лица, обладающего знаниями и полномочиями достаточными для того, чтобы контролировать безопасность информации в системе.

В документе приведены рекомендации по организации защиты информации с использованием средств СКЗИ «КриптоПро JSP». Применение СКЗИ «КриптоПро JSP» должно дополняться общими мерами предосторожности и физической безопасности ПЭВМ.

Система является областным электронным регистром медицинских справок и предназначена для электронного подтверждения подлинности документа, удостоверяющего факт прохождения медицинского освидетельствования гражданином Российской Федерации, иностранным гражданином или лицом без гражданства, для проведения проверки достоверности представленных в нем сведений, контроля использования бланков строгой отчетности в МО, осуществления межведомственного электронного взаимодействия между МЗ СО и Управлением ГИБДД, между МЗ СО и УФМС.

Система является элементом комплексной информационной системы здравоохранения Самарской области как регионального фрагмента единой государственной информационной системы в сфере здравоохранения Российской Федерации.

Заказчик: Министерство здравоохранения Самарской области, г. Самара.

Исполнитель: Группа Компаний ХОСТ, ООО «ИК «ХОСТ», г. Екатеринбург.

Содержание

1 Введение

1.1 Список терминов и сокращений

Необходимые термины, сокращения и их определения отражены в таблице 1.

Таблица 1 – Список терминов и сокращений

Термин / Сокращение	Определение
Администратор	Специалист по обслуживанию компьютерной техники, сети и программного обеспечения (баз данных и информационных систем)
Аутентификация	Процедура проверки подлинности
ГИБДД	Управление Государственной инспекции безопасности дорожного движения Главного управления министерства внутренних дел Российской Федерации по Самарской области
ГОСТ	Государственный стандарт
МЗ СО	Министерство здравоохранения Самарской области
ОС	Операционная система
ПО	Программное обеспечение государственной информационной системы Самарской области «Регистр медицинских справок»
Система	Программно-аппаратный комплекс, предназначенный для автоматизации целенаправленной деятельности конечных пользователей, обеспечивающий (в соответствии с заложенной в него логикой обработки) возможность получения, модификации и хранения информации
СКЗИ	Средство криптографической защиты информации
СУБД	Система управления базами данных
Токен (Token)	USB-ключ, являющийся персональным средством аутентификации
УФМС	Управление Федеральной миграционной службы по Самарской области
ФАПСИ	Федеральное агентство правительственной связи и информации РФ
ФСБ	Федеральная служба безопасности РФ
ФСО	Федеральная служба охраны РФ
ФСТЭК	Федеральная служба по техническому и экспортному контролю РФ
ЭВМ	Электронно-вычислительная машина
ЭЦП	Электронно-цифровая подпись

1.2 Сведения о системе

ПО «Регистр медицинских справок» государственной информационной системы Самарской области предназначено для автоматизации процессов прохождения медицинского освидетельствования гражданами Российской Федерации, иностранными гражданами или лицами без гражданства в медицинских организациях Самарской области.

ПО «Регистр медицинских справок» предназначено для достижения следующих целей:

1) электронное подтверждение подлинности документа, удостоверяющего факт прохождения медицинского освидетельствования гражданином Российской Федерации, иностранным гражданином или лицом без гражданства и проведения проверки достоверности представленных в нем сведений;

2) контроль использования бланков строгой отчетности в медицинских организациях;
3) организация межведомственного электронного взаимодействия между министерством здравоохранения Самарской области и Управлением ГИБДД Главного управления Министерства внутренних дел РФ по Самарской области, между министерством и УФМС РФ по Самарской области.

1.3 Перечень эксплуатационной документации

Для общего понимания и соблюдения процедур информационной безопасности при работе с системой администратору достаточно ознакомиться со следующими документами перед началом работы:

- настоящий документ;
- документ «Руководство пользователя по обеспечению информационной безопасности»;

Перед началом непосредственной эксплуатации СКЗИ «КриптоПро JSP» рекомендуется внимательно ознакомиться с содержанием полного комплекта эксплуатационной документации, а также нормативными и методическими документами, регулирующими обеспечение информационной безопасности, включая политику безопасности информации организации, эксплуатирующей СКЗИ «КриптоПро JSP».

1.4 Состав и содержание дистрибутивного носителя данных

Основная функциональность ПО «Регистр медицинских справок» представлена в виде web-интерфейса и не требует установки на локальный компьютер пользователя какого-либо программного обеспечения.

Для корректной работы ПО «Регистр медицинских справок» (в части подписывания заключений председателя врачебной комиссии и отправки подписанных сообщений через Web-сервисы) на сервере приложений должно быть установлено и настроено СКЗИ «КриптоПро JSP» (см. п. 4). В конфигурационном файле `/certificates-smev-service/src/META-INF/JCP.properties` требуется указать следующие данные:

- `keystore.type` – тип ключевого хранилища;
- `privatekey.alias` – алиас открытого ключа;
- `privatekey.password` – пароль закрытого ключа;
- `certificate.alias` – алиас сертификата;

Для полнофункциональной работы ПО «Регистр медицинских справок» на персональном компьютере пользователя должно быть установлено и настроено специальное программное обеспечение – шифровальные (криптографические) средства, используемые для авторизации в системе и для создания ЭЦП сообщений (см. п. 4).

Пользователь должен иметь USB-ключ (токен), являющийся персональным средством аутентификации, а также актуальный сертификат квалифицированной ЭЦП. Данный сертификат выдается авторизованным удостоверяющим центром и подтверждает принадлежность ЭЦП к конкретному пользователю, уполномоченному для работы в системе.

1.5 Порядок загрузки данных и программ, проверка работоспособности системы

Загрузка системы, выполненной по технологии «клиент-сервер», осуществляется автоматически через Интернет-браузер. Для начала информационного диалога достаточно указать адрес сайта системы (тестовый либо рабочий стенд) в строке адреса браузера, после чего ввести имя пользователя и соответствующий пароль. В случае работоспособности ПО на данном шаге будет открыта страница авторизации системы.

http://141.0.177.154:8080/ - Тестовый стенд (используется для обучения и проверки работоспособности версий).
http://141.0.177.154:6363/ — Рабочий стенд (В сети ТМС – **http://10.2.22.33:6363/**).

1.6 Порядок подключения к системе

Руководитель организации:

1) Обращается в:
   а) **МЗ СО** (Управление лицензирования и контроля качества) с заявлением о наличии у медицинской организации лицензий на проведение медицинского освидетельствования заявителей и о подключении к ГИС РМС;
   б) **МИАЦ** для организации обмена информацией между пользователями организации и МИАЦ. Обмен должен производиться в круглосуточном режиме с использованием ТМС или защищенных каналов связи с использованием криптографической защиты информации VipNet.
2) Проверяет актуальность сведений об организации в «Справочнике организаций сферы здравоохранения (LPU)». Если сведения об организации неактуальны или отсутствуют, заполняет анкету (форма анкеты приведена также на сайте МИАЦ по адресу: http://medlan.samara.ru/node/6141) и обращается в МИАЦ с заявлением об актуализации данных об организации.
3) Обращается в МИАЦ с заявлением о предоставлении доступа пользователей организации к ГИС РМС. К заявлению прилагаются:
   а) сведения о должностном лице, ответственном в организации за использование системы (ФИО, контактные данные).
   б) сведения о пользователях ПО «Регистр медицинских справок». Форма предоставления сведений приведена в разделе «Пользователи ГИС РМС».

МИАЦ, по предоставленным сведениям о пользователях при наличии положительных решений по п. 1-3, осуществляет регистрацию организации и индивидуальную настройку ГИС РМС. По завершению работ информирует организацию о возможности использовать систему.

2 Общие положения

Настоящий документ определяет функциональные обязанности, права и ответственность администратора по обеспечению безопасности информации.

Администратор по обеспечению безопасности информации должен знать:

- **законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой информации ограниченного доступа, нормативные и методические документы по вопросам обеспечения технической защиты информации:**
  - *Основные нормативно-правовые акты и методические документы в области защиты информации:*
    - Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
    - Стратегия развития информационного общества в Российской Федерации, утверждённая Президентом Российской Федерации 07.02.2008 № Пр-212.
    - Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная Указом Президента Российской Федерации от 12 мая 2009 г. № 537.
    - Основы организации защиты информации в Приволжском федеральном округе (Одобрены Решением Координационного Совета по защите информации при полномочном представителе Президента Российской Федерации в Приволжском федеральном округе от 12 ноября 2009 года).
    - Концепция защиты информации ограниченного доступа в Самарской области, утвержденная Губернатором Самарской области 14 декабря 2010 г.
  - *Основные общие нормативные правовые акты:*
    - Конституция Российской Федерации.
    - Федеральный закон Российской Федерации от 28 декабря 2010 г № 380 – ФЗ "О безопасности".
    - Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации».
    - Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
    - «Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утверждено постановлением Совета Министров – Правительства Российской Федерации от 15.09.1993 г. № 912-51.
  - *По вопросам защиты информации ограниченного доступа, не содержащей сведения государственной тайны (конфиденциальность информации, доступ к которой ограничен федеральными законами):*
    - Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».
    - Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служеб-

ной информацией ограниченного распространения в федеральных органах исполнительной власти».

- Специальные требования и рекомендации по технической защите конфиденциальной информации. Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
- Указ Президента Российской Федерации от 17.03.2008 № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена".
- Приказ Федеральной службы охраны Российской Федерации от 07.08.2009 г. № 487 "Об утверждении положения о сегменте информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.
- Приказ ФСТЭК России от 12 июля 2012 г. № 83 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации».
- Приказ ФСТЭК России от 20 июля 2012 г. № 89 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации».

- *По вопросам безопасности информационных систем персональных данных:*
  - Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
  - Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
  - Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".
  - Постановление Правительства РФ от 6 июля 2008 г. № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных".
  - Постановление Правительства РФ от 21.03.2012 г. № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".
  - Постановление Правительства РФ от 18.09.2012 г. № 940 «Об утверждении Правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных

данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю».

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных". Утверждена Зам. директора ФСТЭК России 14 февраля 2008 г.
- Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
- Приказ ФСТЭК России от 18.02.2013 г. № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (Зарегистрировано в Минюсте России 14.05.2013 г. № 18375)
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ»).
- «Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Роскомнадзором 13.12.2013 г.).
- Административный регламент исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных. Утвержден приказом Минкомсвязи от 14.11.2011 г. № 312.
- Приказ Минкомсвязи России от 21.12.2011 г. № 346 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги "Ведение реестра операторов, осуществляющих обработку персональных данных» (Зарегистрировано в Минюсте России 29.03.2012 г. № 23650).

- Приказ Роскомнадзора от 19 августа 2011 г. № 706 "Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных".
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 15 марта 2013 г. № 274 г. Москва «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

- *По вопросам безопасности информации в государственных информационных системах и информационных системах общего пользования:*
  - Постановление Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».
  - Приказ Министерства связи и массовых коммуникаций РФ от 25 августа 2009 г. № 104 "Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования"
  - Приказ ФСБ РФ и ФСТЭК РФ от 31.08.2010 г. № 416/489 "Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования"
  - Приказ Министерства экономического развития Российской Федерации от 16.11.2009 г. № 470 "О требованиях к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами федеральных органов исполнительной власти".
  - Постановление Правительства Самарской области от 13.08.2010 г. № 380 "Об обеспечении доступа к информации о деятельности Правительства Самарской области и органов исполнительной власти Самарской области, размещаемой в сети интернет.
  - Приказ Министерства связи и массовых коммуникаций РФ от 27.06.2013 г. № 149 «Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети "Интернет" в форме открытых данных, а также для обеспечения ее использования».
  - Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 г. № 28608).
  - Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11.02.2014 г.
  - Постановление Правительства РФ от 10.07.2013 г. № 582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети "Интернет" и обновления информации об образовательной организации».

- Постановление Правительства РФ от 24.11.2009 г. № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти».
- Приказ Минкомсвязи РФ от 27.12.2010 г. № 190 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия».
- Приказ ФСО РФ от 07.08.2009 г. № 487 «Об утверждении Положения о сегменте информационно-телекоммуникационной сети "Интернет" для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации»
- Приказ Минкомсвязи РФ от 02.09.2011 г. № 221 «Об утверждении Требований к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающих в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения».

- *По вопросам электронной подписи и криптографической защите информации:*
  - Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
  - Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
  - Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении Инструкции 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».
  - Приказ ФСБ РФ от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».
  - Приказ ФСБ РФ от 27 декабря 2011 г. №796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».
- *Специальные нормативные документы:*
  - Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Показатели защищенности от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.
  - Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 г.
  - Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. Руководство по регистрации профилей защиты. Руководство по формированию семейств профилей защиты. Руководство по разработке

профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 год.

- *Государственные стандарты:*
  - ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России.
  - ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России.
  - ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России.
  - ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России.
  - ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России.
  - ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.
  - ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования.
  - ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России.
  - ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России.
  - ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России.
  - ГОСТ РО 0043-001-2010 Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Термины и определения.
  - ГОСТ РО 0043-002-2012 Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Система документов. Общие положения Для служебного пользования.
  - ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения. Национальный стандарт Российской Федерации, ограниченного распространения.
  - ГОСТ РО 0043–004–2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний.

- **объекты информатизации, подлежащие защите;**
- **специализацию и направления деятельности МЗ СО и ее подразделений; применяемые информационные технологии и системы; структуру управления, связи, автоматизации;**

- **средства технической разведки и методы оценки их возможностей, угрозы безопасности информации и классификацию (категории) нарушений;**
- **оснащенность объектов информатизации основными и вспомогательными техническими средствами и системами, комплексами и средствами технической защиты информации, сервисами и механизмами безопасности автоматизированных систем управления;**
- **подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты от преднамеренного воздействия, контроля целостности информации, перспективы их развития и модернизации;**
- **методы оценки результатов состояния систем безопасности, выявления каналов утечки информации, контроля процесса резервирования и дублирования критичных вычислительных и информационных ресурсов;**
- **порядок работы с техническими, программными, программно-аппаратными средствами защиты информации и контроля, сервисами и механизмами безопасности автоматизированных систем управления и аудита их состояния.**

3 Функциональные обязанности

Администратор по обеспечению безопасности информации **ОБЯЗАН**:

- Устанавливать разграничение полномочий пользователей и порядок доступа к информационным ресурсам, порядок использования основных и вспомогательных технических средств и систем.

Описание операций по администрированию учетных записей пользователей в ПО «Регистр медицинских справок» приведено в документе «Руководство пользователя. Администратор».

- Проводить контроль выполнения пользователями ПО «Регистр медицинских справок» работ согласно перечню мероприятий по обеспечению безопасности информации; вести учет нештатных ситуаций; информировать руководство и уполномоченных работников службы безопасности об инцидентах и попытках несанкционированного доступа к информации по результатам функционирования и контроля систем технической защиты информации.
- Осуществлять администрирование сервисами, комплексами и средствами технической защиты информации и контроля; прекращать работы при несоблюдении установленной технологии обработки информации и невыполнении требований информационной безопасности; готовить предложения по совершенствованию технологических мер защиты информации.
- Контролировать работы по установке, модернизации и профилактике аппаратных и программных средств; созданию, учету, хранению и использованию резервных и архивных копий массивов данных и электронных документов.

Описание операций по администрированию СУБД Microsoft SQL Server 2008 R2 SP2 – 10.50.4000.0 (X64)) приведена на сайте компании Microsoft. Адрес в сети Интернет: http://msdn.microsoft.com/ru-ru/library/ms130214(v=sql.105).aspx

---

- Принимать участие в работах по внесению изменений в программно-аппаратную конфигурацию системы и контролировать ее соответствие требованиям обеспечения безопасности информации.
- Вести учет носителей информации, осуществлять их хранение, прием, выдачу ответственным исполнителям, контролировать правильность их использования.

Администратор по обеспечению безопасности информации **ИМЕЕТ ПРАВО**:

- Требовать от пользователей ПО «Регистр медицинских справок» соблюдения установленных технологий обработки информации и выполнения инструкций и других документов по обеспечению безопасности и защите информации;
- Обращаться к руководителю с требованием прекращения работы пользователей ПО «Регистр медицинских справок» при несоблюдении ими установленных технологий обработки информации или невыполнении требований по обеспечению информационной безопасности;
- Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи информации и технических средств;

- Давать руководителю предложения по совершенствованию мер информационной безопасности в подразделении;

4 СКЗИ «КриптоПро JSP»

4.1 Описание СКЗИ

Шифровальные (криптографические) средства, используемые для авторизации в системе и для создания ЭЦП сообщений, состоят из программных продуктов компании ООО «КРИПТО-ПРО». Официальный адрес сайта КриптоПро: https://www.cryptopro.ru.

КриптоПро JCP – средство криптографической защиты информации, реализующее российские криптографические стандарты, разработанное в соответствии со спецификацией JCA (Java Cryptography Architecture).

Интеграция КриптоПро JCP с архитектурой Java позволяет использовать стандартные процедуры, такие как создание и проверка ЭЦП (в том числе XMLdsig) , шифрование, генерацию ключей, вычисление кодов аутентификации (Message Authentication Code – MAC) в JavaTM Cryptography Extension (JCE) в соответствии со спецификациями JCE на различных операционных системах и аппаратных платформах.

Реализация СКЗИ КриптоПро JCP совместима с КриптоПро CSP.

Требования к СКЗИ КриптоПро JCP:

- *Версия:* 2.0;
- Исполнение СКЗИ КриптоПро JCP функционирует под управлением следующих Java-машин:
  - Java-машина производства Oracle «Java(TM) 2 Runtime Environment, Standard Edition версии 1.6 и выше на 32-битной и 64-битной платформе»;
  - Java-машина производства IBM «Java(TM) 2 Runtime Environment, Standard Edition версии 1.6 и выше на 32-битной и 64-битной платформе»

4.2 Назначение СКЗИ

СКЗИ «КриптоПро JCP» **предназначен** для:

- авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии с отечественными стандартами ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001;
- обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;
- обеспечения аутентичности, конфиденциальности и имитозащиты TLS-соединений;
- контроля целостности системного и прикладного программного обеспечения (для его защиты от несанкционированного изменения или от нарушения правильности функционирования);
- управления ключевыми элементами системы в соответствии с регламентом средств защиты.

4.3 Алгоритмы СКЗИ

В СКЗИ «КриптоПро JCP» реализуются следующие алгоритмы:

1) Алгоритм выработки значения хэш-функции реализован в соответствии с требованиями ГОСТ Р 34.11 94 «Информационная технология. Криптографическая защита информации. Функция хэширования».
2) Алгоритмы формирования и проверки ЭЦП реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
3) Алгоритм зашифрования / расшифрования данных и вычисление имитовставки реализованы в соответствии с требованиями ГОСТ 28147 89 «Системы обработки информации. Защита криптографическая».
4) При генерации закрытых и открытых ключей обеспечена возможность генерации с различными параметрами в соответствии с ГОСТ Р 34.10-2001.
5) При выработке значения хэш-функции и шифровании обеспечена возможность использования различных узлов замены в соответствии с ГОСТ Р 34.11-94 и ГОСТ 28147-89.

4.4 Документация

Ниже представлены ссылки на документы, предназначенные для администрирования СКЗИ «КриптоПро JSP»:

- Описание основной функциональности криптопровайдера КриптоПро JCP и примеры его использования (основной класс провайдера ru.CryptoPro.JCP.JCP) – **Руководство программиста. ЖТЯИ.00088-01 33 01** (документ `progguide.html` из дистрибутива КриптоПро JCP).
- Общее описание СКЗИ КриптоПро JCP 2.0, его состав, ключевая система, рекомендации по размещению технических средств, использующих СКЗИ, рекомендации по проверке целостности установленного ПО СКЗИ, по использованию СКЗИ в различных автоматизированных системах и средствах вычислительной техники – **Руководство администратора безопасности. ЖТЯИ.00088-01 90 01** (документ `admin.html` из дистрибутива КриптоПро JCP).
- Общее описание средства криптографической защиты информации КриптоПро и рекомендации по использованию СКЗИ в различных автоматизированных системах: https://www.cryptopro.ru/sites/default/files/docs/csp36r3/admin_guide_general_r3.pdf.
- Инструкции по установке, настройке и эксплуатации СКЗИ под управлением ОС Windows:
  - https://www.cryptopro.ru/sites/default/files/docs/csp36r3/instruction_csp_r3.pdf (основная инструкция);
  - https://www.cryptopro.ru/sites/default/files/docs/csp36r3/admin_guide_windows_r3.pdf (дополнительная инструкция).