



Содержание

projectIT

projectIT

projectIT

Введение..... 4

1 Исследование исходных данных по объекту защиты 12

1.1 Общие сведения об ИС, эксплуатируемых Учреждением 12

1.1.1 ИСПДн «Бухгалтерия и кадры» 12

projectIT

1.1.2 ИСПДн «Медицинская информационная система»..... 14

projectIT

projectIT

1.1.3 МИС «Республиканская медицинская информационная система» 17

1.2 Установление уровней защищённости ПДн в ИС Учреждения 20



1.2.1 Установление уровня защищённости ПДн в ИСПДн «БиК» 21



1.2.2 Установление уровня защищённости ПДн в ИСПДн «МедИС»..... 21

1.2.3 Установление уровня защищённости ПДн в МИС «РМедИС» 21

projectIT

projectIT

projectIT

1.3 Установление классов защищённости МИС в Учреждении 22

1.3.1 Установление класса защищённости МИС «РМедИС»..... 23

1.4 Актуальные угрозы безопасности информации в ИС Учреждения 23

projectIT

1.4.1 Актуальные угрозы в ИСПДн «БиК» 23

projectIT

projectIT

1.4.2. Актуальные угрозы в ИСПДн «МедИС»..... 31

1.4.3 Актуальные угрозы в МИС «РМедИС»..... 37

1.5 Требования к ИС Учреждения..... 43



1.5.1 Требования к ИСПДн «БиК» 43



1.5.2 Требования к ИСПДн «МИС» 44

1.5.3 Требования к МИС «РМедИС» 44

2 Разработка методов и способов защиты конфиденциальной информации 45

projectIT

projectIT

projectIT

2.1 Технические меры защиты информации 45

2.1.1 СрЗИ НСД. Dallas Lock 8.0-К..... 45

2.1.2 ABC. Dr.Web Enterprise Security Suite 6.0 47

2.1.3 САЗ. XSpider 7.8..... 48

projectIT

projectIT

projectIT

projectIT

projectIT

2.1.4 МЭ и СОВ. ViPNetCustom 3.2 50

2.2 Организационные меры защиты информации 50

2.2.1 Общие требования 50

2.2.2 Организационные меры по размещению ТС 51

2.2.3 Организационные меры по работе со съёмными носителями информации 52

2.2.4 Организация работ по защите информации от НСД 52

2.2.5 Организация работы администратора безопасности 53

2.3 Меры защиты информации в целях нейтрализации актуальных угроз 55

2.4 Схемы построения СЗИ в ИС Учреждения 58

3 Экономика. Оценка затрат на разработку и внедрение СЗИ 61

3.1 Смета затрат на разработку и внедрение СЗИ в ИС «БиК» 61

3.2 Смета затрат на разработку и внедрение СЗИ в ИС «МедИС» 64

3.3 Смета затрат на разработку и внедрение СЗИ в МИС «РМедИС» .. 65

4 Безопасность жизнедеятельности. Расчёт искусственного освещения 68

Заключение 75

Список использованных источников 76

Список сокращений 79



Введение

projectIT

projectIT

projectIT

Проблема защиты информации в Учреждениях здравоохранения рассматривается в Доктрине информационной безопасности Российской Федерации [1], утверждённой Приказом Президента РФ №1895 от 9 сентября 2000 г. Согласно данной Доктрине Россия отстает от ведущих стран мира по уровню информатизации органов здравоохранения, и данное отставание относится к внутренним источникам угроз информационной безопасности Российской Федерации.



В Учреждениях здравоохранения обрабатываются значительные объемы информации с ограниченным доступом, включающей в себя врачебную тайну (сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении [2]). Данная информация нередко подвергается угрозам информационной безопасности.

projectIT

projectIT

projectIT

Необходимость анализа этих угроз, разработка путей их преодоления и важность создания конкретной системы защиты информации (СЗИ) для отдельного учреждения здравоохранения, несомненно, доказывает актуальность данной ВКР.



Объектом исследования является обеспечение информационной безопасности Учреждений здравоохранения в РФ.

projectIT

projectIT

projectIT

Информатизация Учреждений здравоохранения осуществляется в соответствии с Концепцией создания единой государственной информационной системы в сфере здравоохранения [3], утверждённой Приказом Министерства здравоохранения и социального развития РФ от 28 апреля 2011 г. № 364 “Об утверждении концепции создания единой государственной информационной системы в сфере здравоохранения”.

projectIT

projectIT

projectIT

projectIT

projectIT



Согласно этой концепции, единая государственная информационная система в сфере здравоохранения (ЕГИСЗ) представляет собой совокупность информационно-технологических и технических средств, обеспечивающих информационную поддержку методического и организационного обеспечения деятельности участников системы здравоохранения. Одним из принципов создания данной системы является обеспечение информационной безопасности и защиты персональных данных в соответствии с законодательством Российской Федерации.

Предмет исследования данной ВКР – разработка СЗИ в информационных системах (ИС) Государственного бюджетного Учреждения здравоохранения «Станция скорой медицинской помощи г. Улан-Удэ» (Учреждение) в контексте концепции создания ЕГИСЗ.

Цель работы заключается в разработке СЗИ, удовлетворяющей требованиям действующих нормативно-правовых актов в области защиты информации.

Задачи:

- изучение документации в области защиты информации;
- исследование исходных данных по Учреждению, существующих средств защиты информации (СрЗИ) в Учреждении;
- разработка эффективной СЗИ для Учреждения, удовлетворяющей требованиям законодательства РФ, а также нормативно-методическим документам ФСТЭК и ФСБ.

В первом разделе исследуются исходные данные по объекту защиты: ИС, эксплуатируемые на объекте, наличие СрЗИ и т.п. Раздел разделён на пять подразделов:

- исследование общих сведений об ИС, эксплуатируемых Учреждением;
- установление уровня защищённости ИСПДн;
- установление класса защищённости муниципальной ИС;



- актуальные угрозы информационной безопасности ИС Учреждения;
- требования к ИС Учреждения.

Во втором разделе осуществляется разработка методов и способов защиты конфиденциальной информации в соответствии с законодательством РФ. Раздел разделён на четыре подраздела:

- технические меры защиты информации;
- организационные меры защиты информации;
- меры защиты информации в целях нейтрализации актуальных угроз;
- схемы построения СЗИ в ИС Учреждения.

В третьем разделе (раздел «Экономика») выполняется оценка затрат на создание и внедрение СЗИ в ИС Учреждения.

В четвёртом разделе (раздел «Безопасности жизнедеятельности») производится расчёт искусственного освещения для некоторых помещений Учреждения.

В списке использованных источников приводятся используемые документы, литература, Интернет-сайты, и другие источники информации, используемой в данной ВКР.

Согласно информации, предоставленной на официальном сайте Учреждения [4], в настоящее время оно осуществляет работу по оказанию скорой медицинской помощи населению г. Улан-Удэ.

Учреждение осуществляет медицинскую деятельность на основании лицензии Министерства здравоохранения Республики Бурятия №ЛО-03-01-001085 от 28 февраля 2013 г.

Медицинская помощь оказывается детскому и взрослому населению при угрожающих жизни состояниях, несчастных случаях, острых и обострениях хронических заболеваний, как на месте происшествия, так и в пути следования в стационар, в том числе при чрезвычайных ситуациях и

массовых катастрофах. Медицинская помощь оказывается и при непосредственном обращении на подстанцию больных и пострадавших.

Свою работу Учреждение осуществляет под непосредственным руководством Министерства здравоохранения Республики Бурятия и в тесной связи и взаимодействии с лечебно-профилактическими Учреждениями города.

Учреждение работает в режиме постоянной мобильной готовности оказывать скорую помощь при чрезвычайных ситуациях, различных происшествиях и заболеваниях.

Имеются службы оказания психиатрической помощи, педиатрической помощи, а также оказание врачебной консультативной помощи по телефону обратившимся гражданам.

Бригадами Учреждения проводится медицинское обеспечение массовых мероприятий и дежурств в порядке, установленном Министерством здравоохранения РБ.

В настоящее время в Учреждении работает более 500 сотрудников. Ежедневно выполняется от 350 до 450 выездов бригад скорой помощи.

В Учреждении эксплуатируются три ИС:

- ИС «Бухгалтерия и Кадры» (локальная ИС);
- ИС «Медицинская информационная система» (локальная ИС);
- ИС «Республиканская медицинская информационная система» (региональная ИС).

Более подробное описание ИС приведено в подразделе 1.1.

Согласно ФЗ [5], информационные системы включают в себя государственные, муниципальные и иные информационные системы. Муниципальные информационные системы создаются на основании решения органа местного самоуправления.

ИС «Республиканская медицинская информационная система» является муниципальной информационной системой (МИС), поскольку

она внедрена Приказом Министерства здравоохранения Республики Бурятия №247-ОД от 05.03.2012 г «Об организации мероприятий по внедрению республиканской медицинской информационной системы в здравоохранение Республики Бурятия» [6].

В соответствии с Требованиями [7], данные требования распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством РФ.

При обработке в государственной (муниципальной) информационной системе информации, содержащей персональные данные, настоящие Требования применяются наряду с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных [10], утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

Состав требований к мерам защиты информации и их базовые наборы для соответствующего класса ИС приведён в Приложении №2 к Требованиям [7]. Следовательно, требования к базовому набору мер защиты информации для муниципальной ИС «РМедИС» уже разработаны, однако необходимо адаптировать, уточнить и дополнить данный набор мер в соответствии с п.21 Требованиям [7].

Для детализации мер используется Методический документ [8], утверждённый ФСТЭК России 11 февраля 2014 г. Данный Методический документ детализирует организационные и технические меры защиты информации, принимаемые в государственных информационных системах в соответствии с Требованиями [7] о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, а также определяет содержание мер защиты информации и правила их реализации.

Согласно Федеральному закону РФ «О персональных данных» от 27 июля 2006 г. N 152-ФЗ [9]:

- персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Все вышеперечисленные ИС обрабатывают ПДн, и, следовательно, являются (за исключением МИС «РМедИС») ИСПДн.

Требования [10] к защите персональных данных при их обработке в информационных системах персональных данных, утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119.

Согласно данным Требованиям существует четыре уровня защищённости ПДн (1, 2, 3, 4). На основании исходных данных [раздел 1] по ИС, эксплуатируемым Учреждением, с помощью разработанной программы были составлены документы, устанавливающие уровень защищённости ПДн, обрабатываемых в ИС Учреждения.

Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для каждого из уровней защищённости персональных данных приведены в Составе и содержании организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [11], утвержденных приказом ФСТЭК России от 18 февраля 2013 г. № 21.

Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

техническим заданием) на создание системы защиты информации информационной системы с учетом ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания», ГОСТ Р 51583 и ГОСТ Р 51624 и в том числе включает [7]:

- проектирование системы защиты информации информационной системы;
- разработку эксплуатационной документации на систему защиты информации информационной системы;
- макетирование и тестирование системы защиты информации информационной системы (при необходимости).



8 (952) 106-88-60



vk.com/a.projectit



a.projectit



8 (952) 106-88-60



vk.com/a.projectit



a.projectit



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

Заклучение

projectIT

projectIT

projectIT

Защита информации очень важна в XXI веке — веке информационных технологий.

Во время выполнения данной ВКР:

projectIT

- была изучена документация в области защиты информации;

projectIT

projectIT

- в разделе 1 были исследованы исходные данные по объекту защиты, определены актуальные угрозы безопасности информации в ИС Учреждения, определены требования к информации и ИС;



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

- в разделе 2 были выбраны организационные и технические меры защиты информации, схемы установки технических средств защиты информации в ИС Учреждения;

projectIT

projectIT

projectIT

- в разделе 3 (экономика) был выполнена оценка затрат на разработку и внедрение СЗИ;

projectIT

projectIT

projectIT

- в разделе 4 (безопасность жизнедеятельности) был выполнен расчёт параметров искусственного освещения некоторых помещений Учреждения.

Таким образом, была разработана СЗИ Государственного бюджетного учреждения здравоохранения «Станция скорой медицинской помощи г.



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

Улан-Удэ», отвечающая требованиям законодательства и федеральных органов исполнительной власти.

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

Список использованных источников

projectIT

projectIT

projectIT

1. Доктрина информационной безопасности РФ; Утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895

projectIT

2. Об основах охраны здоровья граждан в Российской Федерации: Федеральный закон Российской Федерации от 21 ноября 2011 г. №323-ФЗ.

projectIT

projectIT

3. Концепция создания единой государственной информационной системы в сфере здравоохранения: Утв. Приказом Министерства здравоохранения и социального развития РФ от 28 апреля 2011 г. № 364 “Об утверждении концепции создания единой государственной информационной системы в сфере здравоохранения”.



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

projectIT

4. <http://ssmp.uuzdrav.ru/> — официальный сайт Государственного бюджетного учреждения здравоохранения «Станция скорой медицинской помощи г. Улан-Удэ»

projectIT

projectIT

projectIT

5. «Об информации, информационных технологиях и о защите информации»: Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ 1.

projectIT

projectIT

projectIT



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

projectIT

6. Приказ Министерства Здравоохранения Республики Бурятия от 05.03.2012 № 247-ОД 19 апреля 2012 г. «Об организации мероприятий по внедрению республиканской медицинской информационной системы в здравоохранение Республики Бурятия”.

projectIT

projectIT

projectIT

projectIT

7. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Утв. Приказом ФСТЭК России от 11 февраля 2013 г. N 17.

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

projectIT

8. Методический документ. Меры защиты информации в государственных информационных системах: Утв. ФСТЭК России 11 февраля 2014.

9. «О персональных данных»: Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ.

10. Требования к защите персональных данных при их обработке в информационных системах персональных данных: Утв. постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Утв. Приказом ФСТЭК России от 18 февраля 2013 г. N 21.

12. Информационное сообщение ФСТЭК России (по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных») от 15 июля 2013 г. № 240/22/2637

13. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах: Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.

14. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах: Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.

15. ГОСТ 34.602-89 Техническое задание на создание автоматизированной системы.

16. ГОСТ 34.201-89 Виды, комплектность и обозначения документов при создании автоматизированных систем.

17. РД 50-34.698-90. Автоматизированные системы. Требования к содержанию документов.

18. <http://www.drweb.com/> – официальный сайт ABC Dr. Web.

19. <http://www.dallaslock.ru/> – официальный сайт СpЗИ DallasLock.

20. <http://www.infotecs.ru/> – официальный сайт компании-производителя программного комплекса ViPNetCustom.

21. Козловская, В. Б. Электрическое освещение: справочник / В. Б. Козловская, В. Н. Радкевич, В. Н. Сацукевич. – Минск: Техноперспектива, 2008.

22. Андреев, А. И. Безопасность жизнедеятельности в дипломном проектировании : метод. указания для студентов, изучающих курс «Безопасность жизнедеятельности» / А. И. Андреев. – Хабаровск: Изд-во ДВГУПС, 2009. – 38 с.: ил.

23. Безопасность жизнедеятельности. Примеры решения задач: Учебное пособие. – В 2-х частях. – Ч. 2 / Под ред. Б. А. Мамота. – Хабаровск: Изд-во ДВГУПС, 2002. – 84 с.: ил.

24. Тесленко, И. М. Производственное освещение: учеб. пособие / И. М. Тесленко. – Хабаровск: Изд-во ДВГУПС, 2014. – 103 с.: ил.