



Алтайский государственный технический университет им И.И. Ползунова
Факультет информационных технологий
Кафедра информатики, вычислительной техники и информационной безопасности
Информационная безопасность

Проектирование защищенного комплекса средств автоматизации приема вызовов скорой медицинской помощи

Выполнил: студент группы ИБ-62 Липатов Владимир Алексеевич

Руководитель: заместитель руководителя отдела системной
интеграции

ООО «ЦИБ» Циклаков Антон Владимирович

Цель и задачи работы

Цель работы:

- Спроектировать защищенный комплекс средств автоматизации приема вызовов скорой медицинской помощи

Задачи работы:

- Провести анализ функционального процесса системы
- Определить информацию подлежащую защите
- Составить модель угроз и возможных нарушителей.
- Выбрать целесообразные технические средства и организационные мероприятия для защиты.
- Провести оценку эффективности подсистемы защиты информации

Актуальность

- Научная новизна работы заключается в обоснованном и оптимальном выборе современных средств защиты, а также в выработке организационных мер для обеспечения информационной безопасности комплекса средств автоматизации приема вызовов скорой медицинской помощи, соответствующих нормативной базе ФСТЭК России.
- Объектом выполненной работы является центр обработки вызовов скорой помощи в с. Майма Республики Алтай.
- Предметом выпускной квалификационной работы является обеспечение информационной безопасности средств автоматизации приема вызовов скорой медицинской помощи.

Анализ функционального процесса

- Система вызова службы скорой помощи функционирует в форме электронного взаимодействия согласовывая деятельность дежурного персонала службы скорой помощи действующей на территории Республики Алтай и обеспечивающей безопасность жизнедеятельности населения.
- Приём вызовов, являющихся сообщениями о происшествии, осуществляется операторами ЦОВ, которые вводят в базу данных информацию о происшествии, которая регистрируется, анализируется и уходит в обработку.
- Решение об организации реагирования на вызов (сообщение о происшествии) диспетчер должен принимать на основании оценки достоверности полученных данных с учётом возможной «необоснованности» вызова, типа происшествия, требований руководящих документов и инструкций, условий обстановки, а также наличия сил и средств (ресурсов) реагирования.

Анализ архитектуры автоматизированной системы

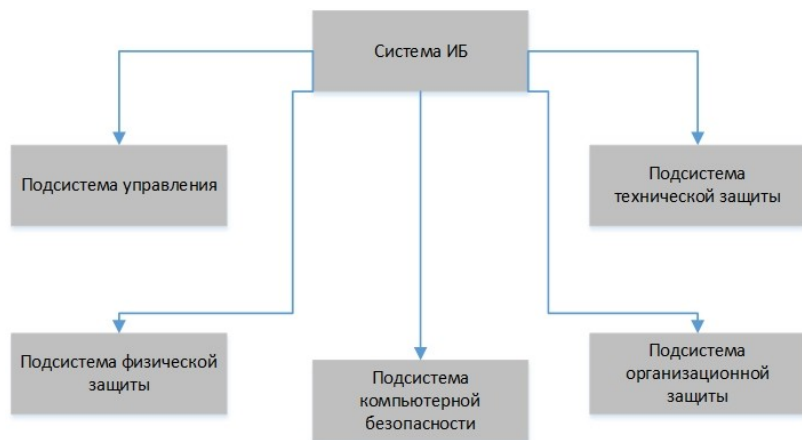
Прием и обработка вызовов (сообщений о происшествиях) службой скорой медицинской помощи осуществляется в установленном порядке.

В составе операторского персонала основного и резервного центров обработки вызовов кроме дежурных специалистов могут быть предусмотрены также:

- Старший смены;
- Специалист - переводчик-лингвист;
- Специалист психолог;
- Ведущий инженер электроник.

Состав и оценка эффективности проектируемой системы ИБ

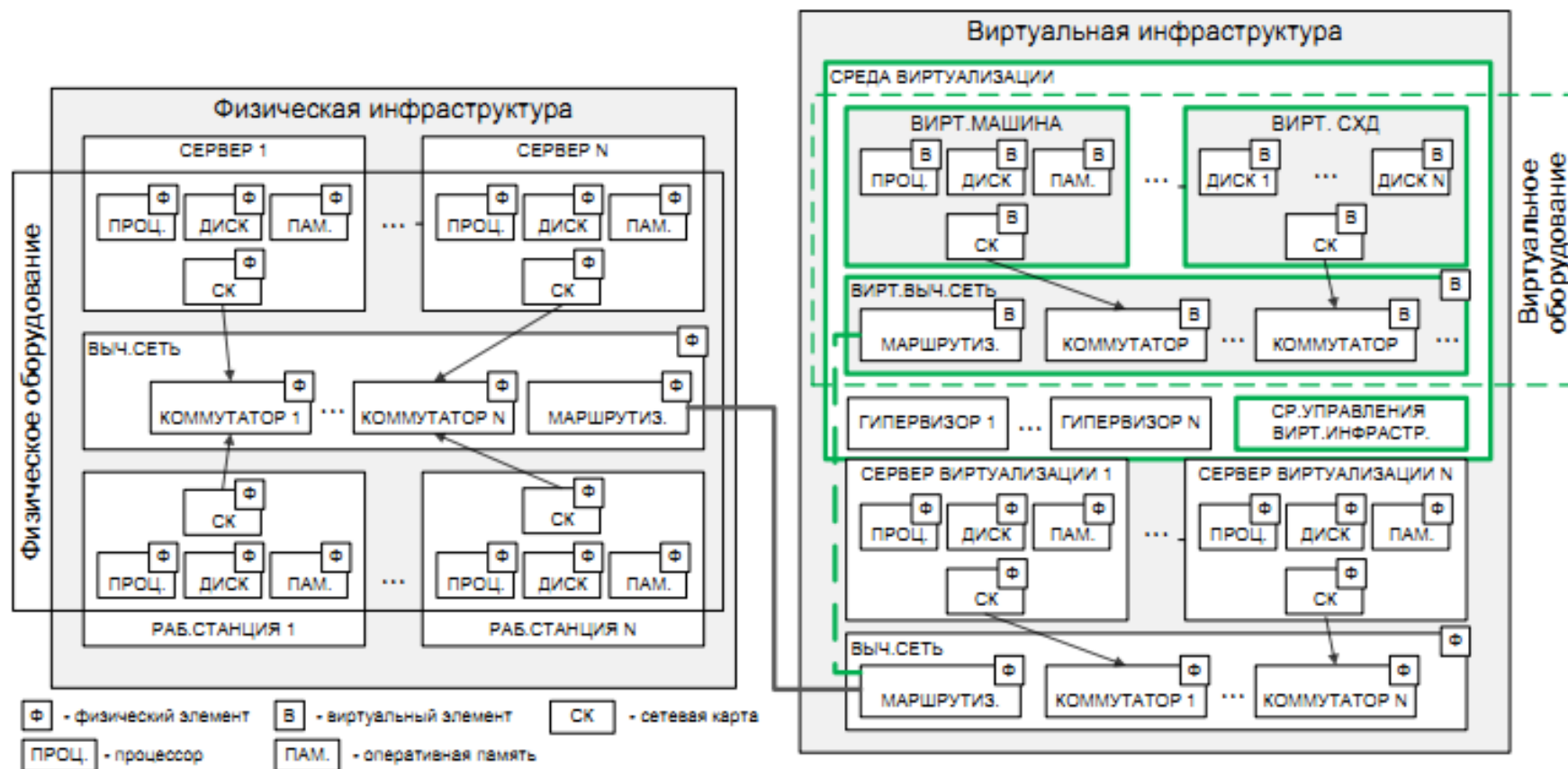
6



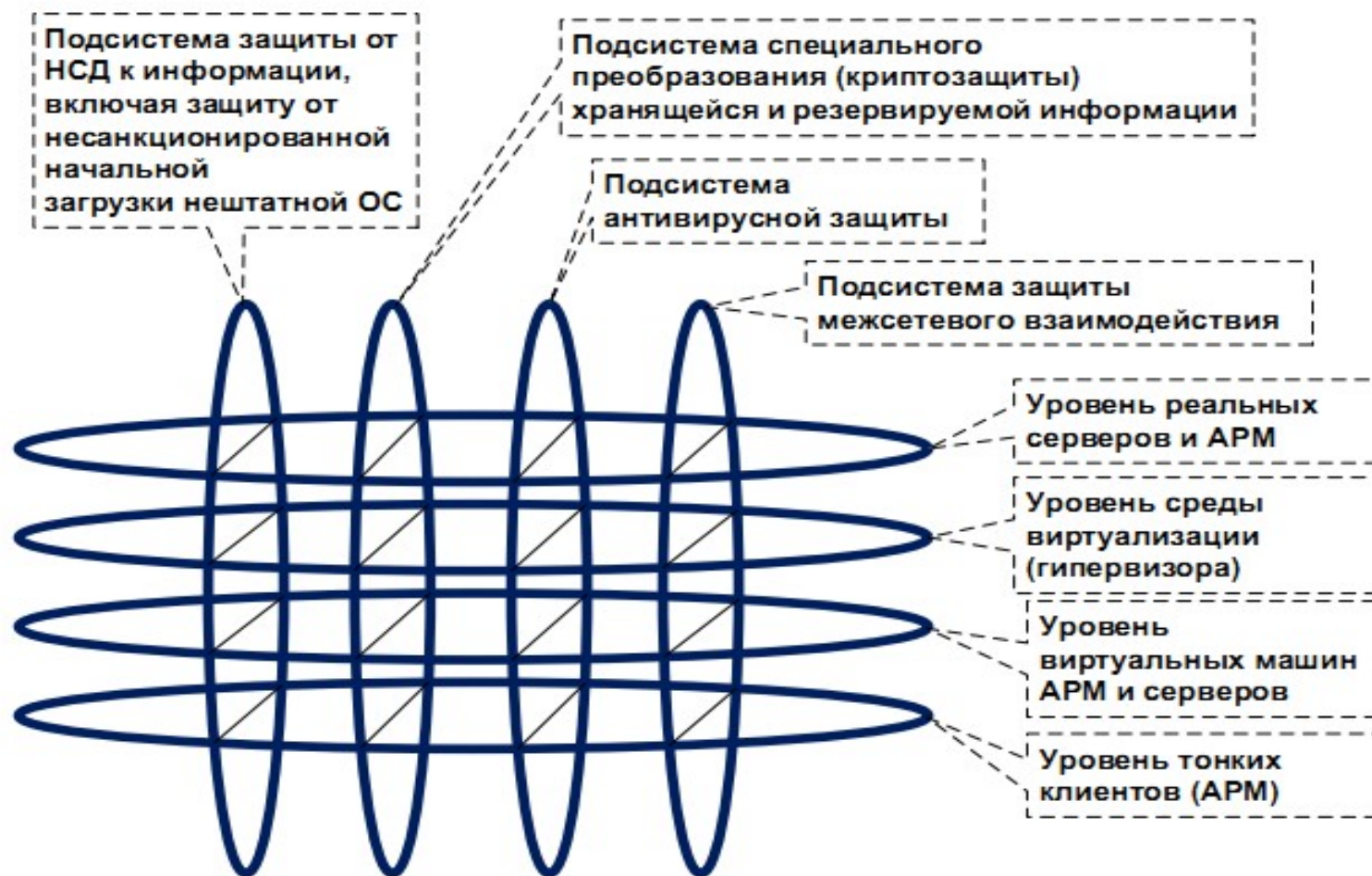
Так как руководством организации была принята наступательная стратегия обеспечения информационной безопасности, вероятность защиты информации должна быть не ниже 0,87.

Показатели	Подсистемы ИБ Управления					Q _{сзи}
	1	2	3	4	5	
	Коэффициенты важности по направлениям					
	0,2	0,2	0,2	0,2	0,2	
Количественный	0,89	0,88	0,88	0,87	0,84	0,86

Физическая и виртуальная инфраструктура компьютерной сети



Уровни и подсистемы защиты



Программно-аппаратные средства ЦОВ и ЦОД

Наименование программно-технического средства	Место установки	Основные функции
1. Общесистемное программное обеспечение:		
Astra Linux «Смоленск» (в комплекте с ПК СВ «Брест»)	ЦОД	Серверная операционная система
Astra Linux «Орёл»	ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ	Операционная система рабочих станций
1. Прикладное программное обеспечение:		
LibreOffice 6.4.2	ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ	Набор офисных программ для создания, редактирования документов, таблиц, баз данных, презентаций
Браузер Yandex Browser	ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ	Просмотр интернет-сайтов
1. Применяемые средства защиты информации:		
Kaspersky Endpoint Security Linux 10.1.1.6421	ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ, ЦОД	Комплексная антивирусная защита на всех каналах поступления и передачи информации
VipNet Client 4 for Linux	ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ	Программный комплекс, предназначенный для построения и обеспечения безопасной передачи данных между защищенными сегментами виртуальной сети VipNet, а также фильтрации IP-трафика, с использованием транспортной среды произвольной телекоммуникационной инфраструктуры IP-сетей, включая сети связи общего доступа.
VipNet CSP	ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ	Крипто-провайдер установки и использования электронно-цифровой подписи
ПАК «Соболь 4.2» АМДЗ	ДДС ЦОВ, ведущий инженер электроник, специалист психолог, старший смены ЦОВ	Аппаратный модуль доверенной загрузки, предотвращение НСД к АРМ
VIPNet IDS 1000	ЦОД	Программно-аппаратный комплекс для обнаружения вторжений в информационные системы,

Функциональная оценка эффективности

1. Определение объектов ИС. Подлежащих защите	0,9	
2. Выявление потенциальных угроз	0,89	
3. Проведение оценки угроз и рисков		0,88
4. Определение требований к СЗИ	0,88	
5. Осуществление выбора средств защиты информации	0,88	
6. Внедрение средств ЗИ	0,87	
7. Осуществление управления	0,91	

Оценка защищенности подсистемы технической защиты информации показывает, что эффективность этапа № 5 составляет 0,88 при требуемом показателе вероятности защиты информации от 0,87 до 0,95.

Показатели	Подсистемы ИБ Управления					Q _{сзи}
	1	2	3	4	5	
	Коэффициенты важности по направлениям					
	0,2	0,2	0,2	0,2	0,2	
Количественный	0,89	0,88	0,88	0,87	0,88	0,88

Результаты расчета затрат на реализацию проекта

№	Наименование статей	Обозначение	Сумма, руб.
1	Оборудование	$C_{\text{мат}}$	433 750
2	Программное обеспечение	$C_{\text{пр}}$	431 103
Итого		$C_{\text{модерн}}$	864 853

Результаты работы

Для повышения эффективности подсистемы технической защиты был предложен ряд технических средств защиты для оборудования защищаемого помещения.

В результате оценки эффективности предложенных мер определено, что мероприятия по совершенствованию вывели на требуемый уровень как подсистему технической защиты информации, так и всю систему информационной безопасности центра обработки вызовов в целом.

Также была разработана Политика безопасности защищаемого помещения.

Таким образом, был предложен комплекс организационных мер и технических средств защиты для подсистемы технической защиты информации в системе информационной безопасности организации. Цели работы достигнуты, проект экономически выгоден.

**БЛАГОДАРЮ ЗА
ВНИМАНИЕ!**