Департамент образования
города Москвы
ГБПОУ КДПИ им. Карла Фаберже

Дипломная работа

на тему: «Организация защиты персональных данных в корпорации RHANA»

Специальность «Организация и технология защиты информации»

Работу выполнил:
Студент группы ТЗИ – 4
Попов Соломон Юрьевич
Руководитель: Корнеев Юрий Иванович

Цель дипломной работы

Целью данной дипломной работы является: проведение анализа угроз безопасности персональных данных и предложение рекомендаций по защите персональных данных.

Задачи

Задачи дипломного проекта:

- ✔ Провести анализ угроз персональных данных в организации;
- ✔ Внести предложения по защите персональных данных;
- ✔ Рассчитать затраты по защите персональных данных;
- ✔ Рассмотреть организацию рабочего места и технику безопасности при работе с ПЭВМ.

Предмет и объект исследования

Объектом исследования данного дипломного проекта является клиника пластической хирургии и косметологии ООО «RHANA».

Предмет исследования: организация защиты персональных данных информационной системы организации.

Глава 1. Основной состав информационной системы персональных данных организации и характеристика угроз безопасности

В системе данной организации обрабатываются следующие персональные данные, подлежащие защите:

- Фамилия, имя, отчество сотрудников и клиентов, серии и номера документов;
- Любые иные сведения о клиентах, собранных с целью дальнейшего использования клиникой.

Классификация угроз безопасности персональных данных

Возможные угрозы безопасности ПДН в клинике RHANA классифицируются на:

1. Угрозы утечки информации по техническим каналам (акустической (речевой) информации, видовой, по каналам побочных электромагнитных излучений и наводок);
2. Угрозы несанкционированного доступа к информации в информационной системе персональных данных;
3. Угрозы безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия
4. Угрозы программно-математических воздействий.

Характеристика угроз безопасности

Источниками угроз несанкционированного доступа могут являться:

- Нарушитель (внутренний и внешний);
- Носитель вредоносной программы или непосредственно сама вредоносная программа;
- Аппаратная закладка.

Глава 2. Организация защиты персональных данных

2.1. Для определения мер по защите информационной системы персональных данных необходимо:

Определить уровень исходной защищенности

№ п/п	Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
		Высокий	Средний	Низкий
1.	ИСПДн, имеющие одноточечный выход в сеть общего пользования		+	
2.	Запись, удаление, сортировка данных ИСПДн		+	

Для примера возьмем несколько пунктов из таблицы определения уровня исходной защищенности.

Степень исходной защищенности

Числовой коэффициент (Y_2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя: маловероятно ($Y_2 = 0$); низкая ($Y_2 = 2$); средняя ($Y_2 = 5$); высокая ($Y_2 = 10$).

В нашем случае, 70% характеристик ИСПДн соответствует уровню не ниже «средний», следовательно, $Y_1=5$.

№ п/п	Угроза безопасности ПДн	Вероятность реализации угрозы нарушителем категории Kn
1.	Угроза модификации BIOS	K1, K4-K8 (0)
2.	Угроза анализа сетевого трафика	K2, K4-K6 (5)

В данной таблице мы определяем вероятность реализации угроз в ИСПДн.

Определение вероятности реализации угроз в ИСПДн (

По итогам оценки уровня исходной защищенности (Y1) и вероятность реализации угрозы (Y2) рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы рассчитывается по формуле: Y=(Y1+Y2)/20.

№ п/п	Угроза безопасности угроз ИСПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы
1.	Угроза модификации BIOS	0,25	Маловероятная
2.	Угроза анализа сетевого трафика	0,5	Средняя
3.	Угроза перехвата управления	0,35	Низкая

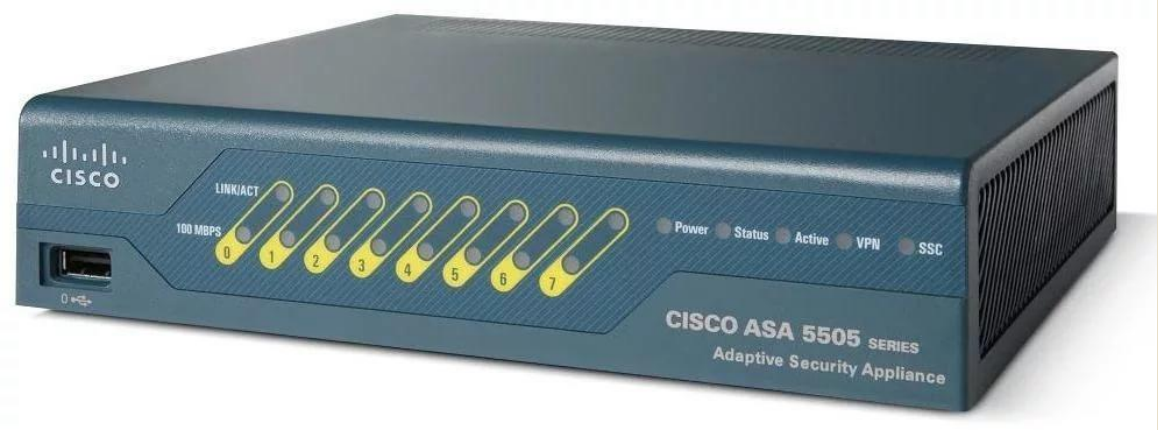
2.2. Меры защита информационной системы персональных данных

Исходя из актуальных угроз безопасности, необходимо предусмотреть следующие меры защиты:

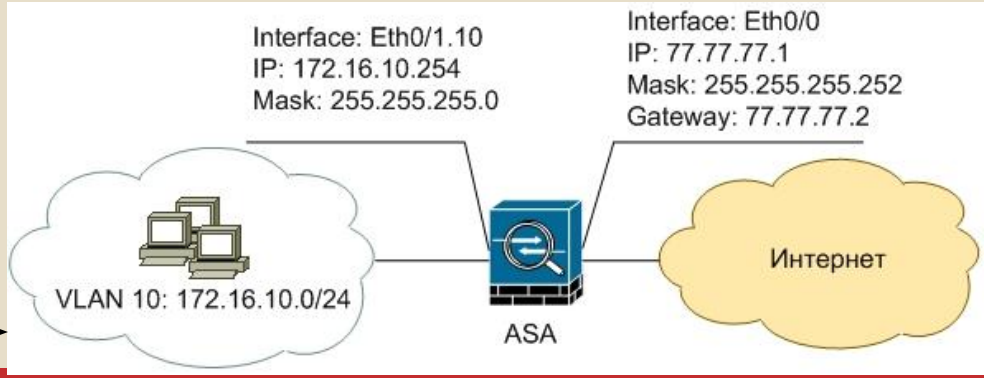
ПО сетевого сканера безопасности *GFI LanGuard* - обнаружение, определение и исправление уязвимостей в сети.

2.2. Меры защита информационной системы персональных данных

Межсетевой экран **Cisco ASA** – современные функциональные устройства для защиты локальных сетей.

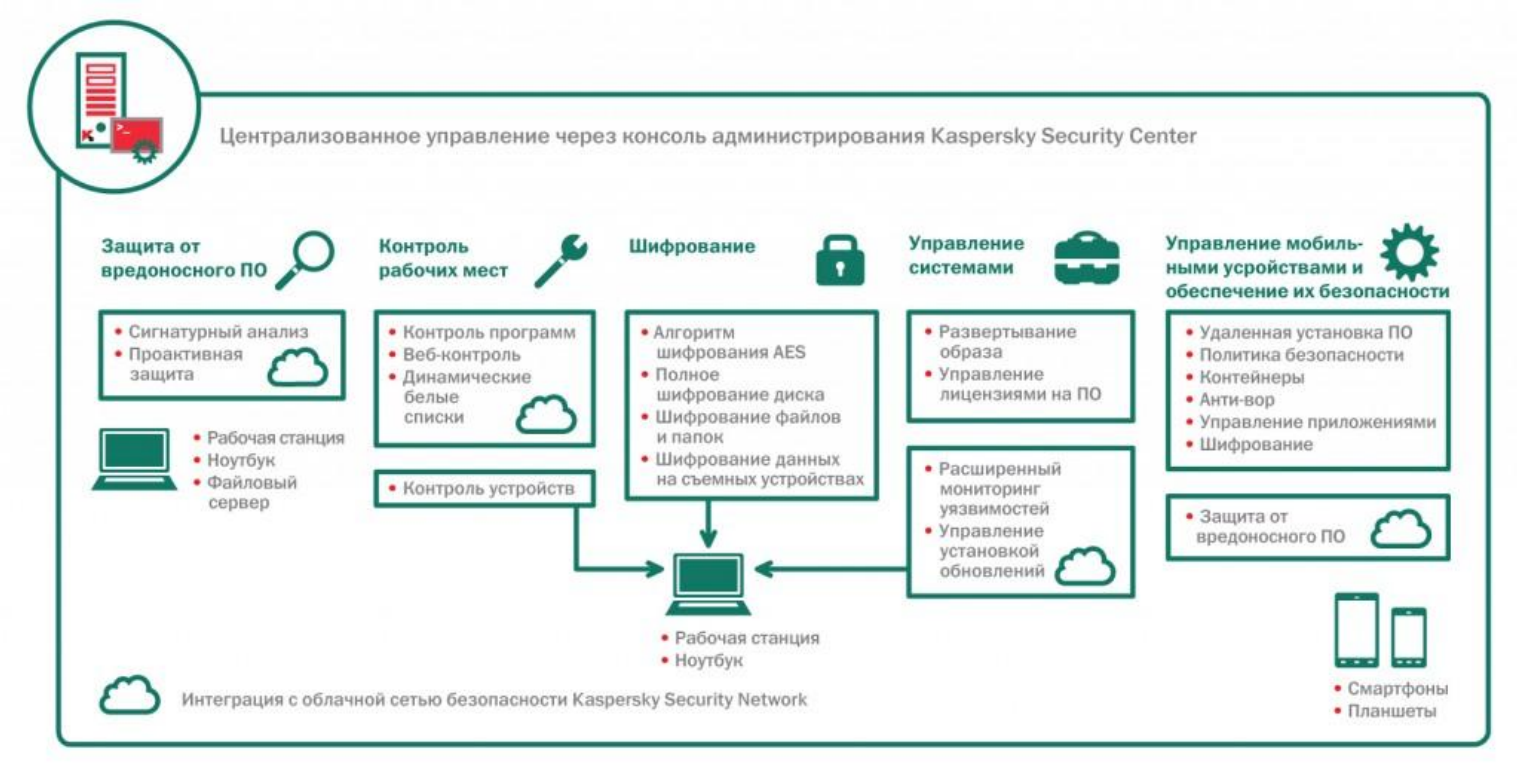


Принцип работы данного межсетевого экрана



2.2. Меры защита информационной системы персональных данных

Универсальное программное антивирусное обеспечение Kaspersky Endpoint Security для бизнеса расширенный - предоставляет высокоэффективные технологии и инструменты обеспечения IT-безопасности для построения системы многоуровневой защиты.



Глава 3. Технико-экономическое обоснование.

Определим стоимость оборудования для защиты персональных данных.

Наименование	Количество лицензий на 1 год	Стоимость (с учетом НДС), руб.
Сканер безопасности GFI LanGuard	25	45500
Межсетевой экран Cisco	4 шт.	28159 (1 шт.)
Антивирусное обеспечение Kaspersky Endpoint Security	25	59050
	Итого	217186

В организации понадобится установить 4 проводных межсетевых экрана, общая стоимость которых составит 28159*4=112636 руб.

Анализ прибыли и себестоимости

Показатель	Годы		Отклонение	
	2015	2016		
	тыс. руб.	тыс. руб.	Абсолютное руб.	Относительное %
1	2	3	4	5
Выручка	8138150	7765500	-372650	-4,58
Себестоимость	1403500	1105000	-298500	-21,27
Прибыль от продаж (без учета оборудования)	5934650	5660500	-274150	-4,62
Прибыль от продаж (с учетом оборудования)	6934650	7217269	+282619	+4,07

Анализ прибыли за 2015-2016 год.

Глава 3. Анализ прибыли и себестоимости.

Как видно из таблицы, после введения нового оборудования прибыль предприятия увеличилась на 282619 руб., что составляет 4,07%.

Вывод: исходя из проведённого анализа можно сказать, что после введения оборудования для защиты персональных данных на предприятии ООО «RHANA», прибыль предприятия с учетом оборудования увеличилась на 282619 рублей, что составляет 4,07%.

Глава 3. Анализ прибыли и себестоимости.

На основании проведенного экономического расчета можно дать рекомендации по повышению эффективности защиты информации:

- увеличить численность персонала по защите информации;
- провести установку межсетевых экранов и программного обеспечения по защите информации.

Заключение

В дипломном проекте был произведен анализ актуальных угроз, которым наиболее подвержена клиника «RHANA».

С учетом данных угроз был произведен подбор аппаратного и программного обеспечения для защиты персональных данных, был произведен расчет затрат на аппаратное и программное обеспечение, произведен анализ динамики прибыли предприятия ООО «RHANA», даны рекомендации по улучшению деятельности организации в области защиты персональных данных.

Цели и задачи дипломного проекта были достигнуты.