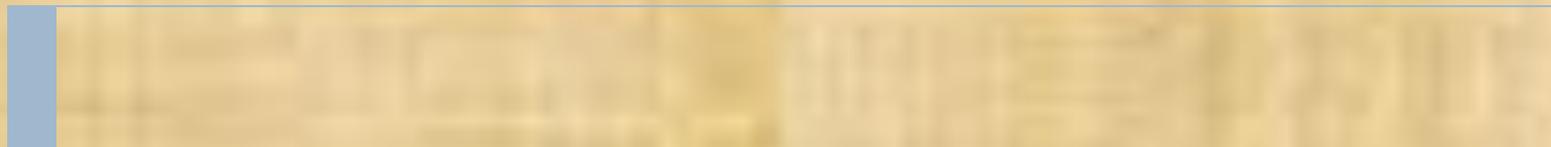


Владимирский государственный университет
кафедра Информатики и защиты информации
ассистент Полянский Д.А.
Антипов Р.Н. КЗИ-204

Комплексная система защиты информации на предприятии «ОВО при ОВД по Суздальскому району»



Цели и задачи

- Провести анализ ОИ – определить структуру угроз, множество уязвимостей и информационных ресурсов, выделить средства обработки информации и имеющихся в наличии средства защиты и мероприятия.
- В соответствии со спецификой предприятия предложить и обосновать диапазон удовлетворяющих значений общего показателя защищенности
- Рассчитать информационные риски при текущем уровне обеспечения ИБ
- Разработать комплекс средств и мероприятий направленных на совершенствование КСЗИ в рамках выделяемого предприятием финансирования.
- На основе расчетов новых значений информационных рисков (с учетом дополнительных мер) определить соответствие нового показателя защищенности установленному диапазону удовлетворительных значений.



Общие сведения



Название объекта:

«Отдел Вневедомственной охраны при ОВД по Суздальскому району.»

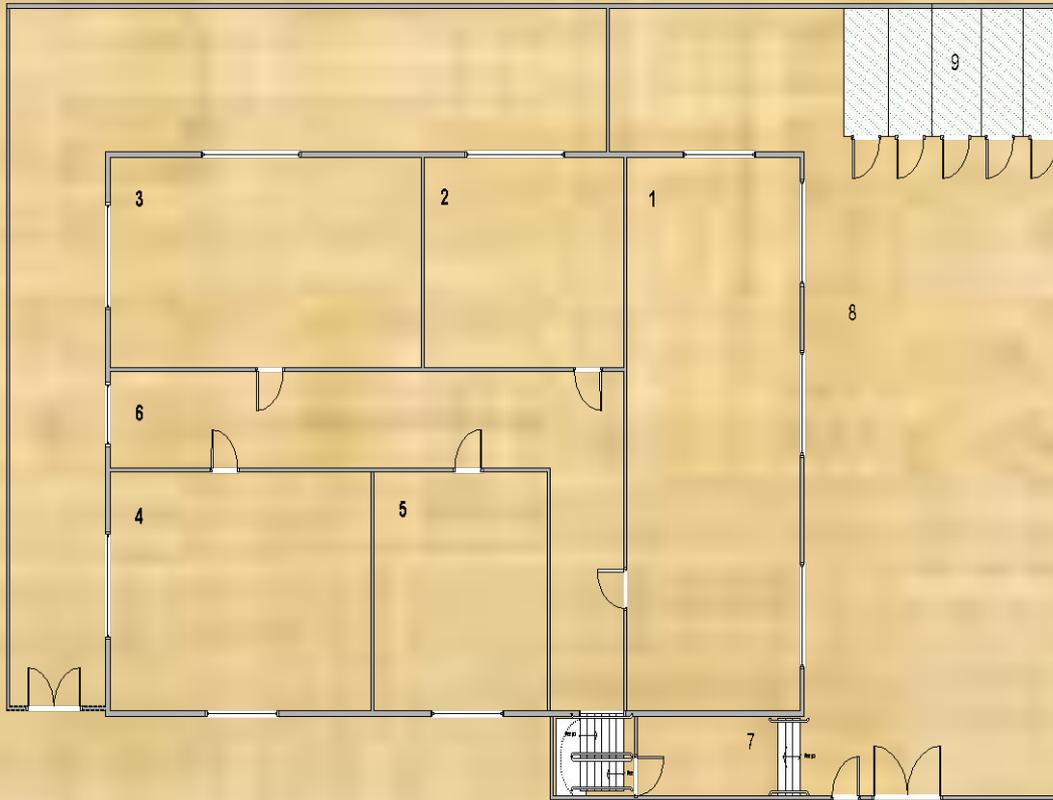
Адрес: Владимирская область, г.Суздаль, ул.Красная Площадь, д.8

Отдельно стоящее двухэтажное кирпичное здание, огороженное забором и имеющее стоянку для личных и служебных автомобилей. Отдел Вневедомственной Охраны занимает всю площадь 2 этажа. На первом этаже располагаются Судебные приставы. Организации имеют отдельные входы для персонала, а также свои выезды для авто транспорта. В ограждение защищаемой организации имеется калитка для персонала и распашные ворота для въезда и выезда автотранспорта



Описание объекта информатизации

Объект информатизации



- 1 – Кабинет начальника ОВО
- 2 - Бухгалтер и системный программист
- 3, 4 - комнаты отдыха групп быстрого реагирования
- 5 - Пульт централизованного наблюдения (ПЦН)
- 6 – Коридор
- 7 – Крыльцо
- 8 - Авто стоянка для служебного транспорта
- 9 – Авто боксы



Описание объекта информатизации

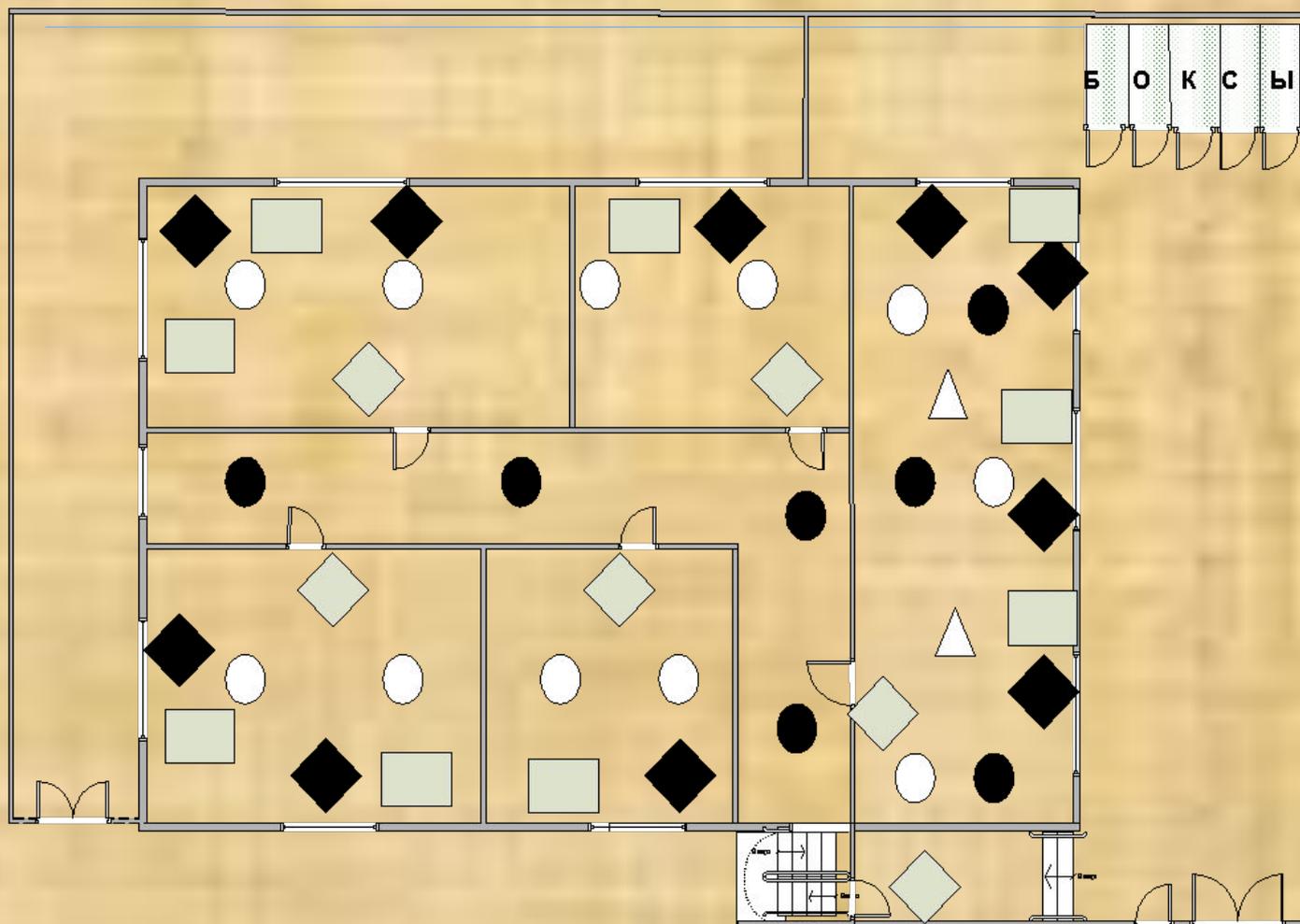
Перечень информационных ресурсов

- Информация о подготовке, принятии и исполнении отдельных решений руководства организацией по коммерческим, организационным, научно-техническим вопросам.
- Информация о существовании и о планах расширения организации, взятие под охрану новых объектов.
- Информация о кругообороте денежных средств в организации, бухгалтерская и налоговая отчётность.
- Информация о применяемой аппаратуре в охране собственного помещения и объектов клиентов, дубликаты ключей от объектов и коды доступа к ним.
- Данные о подготовке групп быстрого реагирования.
- Сведения о разработке и внедрения новых технических средств и программного обеспечения.
- Информация о графиках смен охраны и пропускном режиме организации.
- Информация, составляющая служебную или коммерческую тайну организаций, объектов клиентов и передаваемые ими в пользование на доверительной основе.



Анализ объекта исследования

Функционирующая система безопасности



Обозначение:

- Дымовой пожарный извещатель ●
- Тепловой пожарный извещатель ○
- Сплинклерный ороситель ▲
- Магнитноконтактный ◇
- Удароконтактный □
- Линейны(фольга) ◆

Анализ угроз и уязвимостей информационной системы Слайд 7

Множество уязвимостей информационной безопасности

- отсутствие контроля над территорией организации,
 - отсутствие сейфов для хранения резервных копий и бумажных носителей,
 - отсутствие физической защиты окон в выделенном помещении или неправильная установка решеток на окнах,
 - слабая техническая укрепленность дверей выделенного помещения,
 - отсутствие пропусков у сотрудников организации,
 - отсутствие или недостаточное количество источников бесперебойного питания,
 - не укомплектованность охраны, в т.ч. средствами активной обороны,
 - отсутствие сейфовой комнаты для хранения оружия,
 - отсутствие поста пропускного режима,
 - отсутствие или недостатки в системе видеонаблюдения.
-



Анализ угроз и уязвимостей информационной системы

Множество угроз информационной безопасности

- разглашение конфиденциальной информации персоналом
 - утечка информации по акустическим и виброакустическим каналам,
 - утечка информации по электрическим каналам,
 - утечка информации по каналам ПЭМИН,
 - ввод сотрудниками неверных данных или намеренное искажение информации,
 - потеря информации в результате отключения электропитания,
 - потеря или кража носителей информации на резервных носителях,
 - выход из строя линий связи.
-



Анализ информационных рисков с имеющейся системой безопасности

Слайд 9

Коэффициент защищенности информационной системы

$$K^{\text{защ}} = 1 - \frac{R^{\text{защ}}}{R^{\text{нз}}} = 0.5106$$

где $K^{\text{защ}}$ - коэффициент защищенности

$R^{\text{защ}}$ - риск для защищенной системы

$R^{\text{нз}}$ - риск для не защищенной системы

Анализ информационных рисков с имеющейся системой безопасности ^{Слайд 10}

Наиболее критичные угрозы

- разглашение конфиденциальной информации персоналом
- выход из строя линий связи.
- потеря информации в результате отключения электропитания,
- утечка информации по электрическим каналам,
- утечка информации по каналам ПЭМИН,



Реализация мер по повышению информационной безопасности

Меры по повышению ИБ

- Повышение функциональности охраны периметра и внутренних помещений.
- Организация выделенного помещения.

Повышение функциональности охраны организации

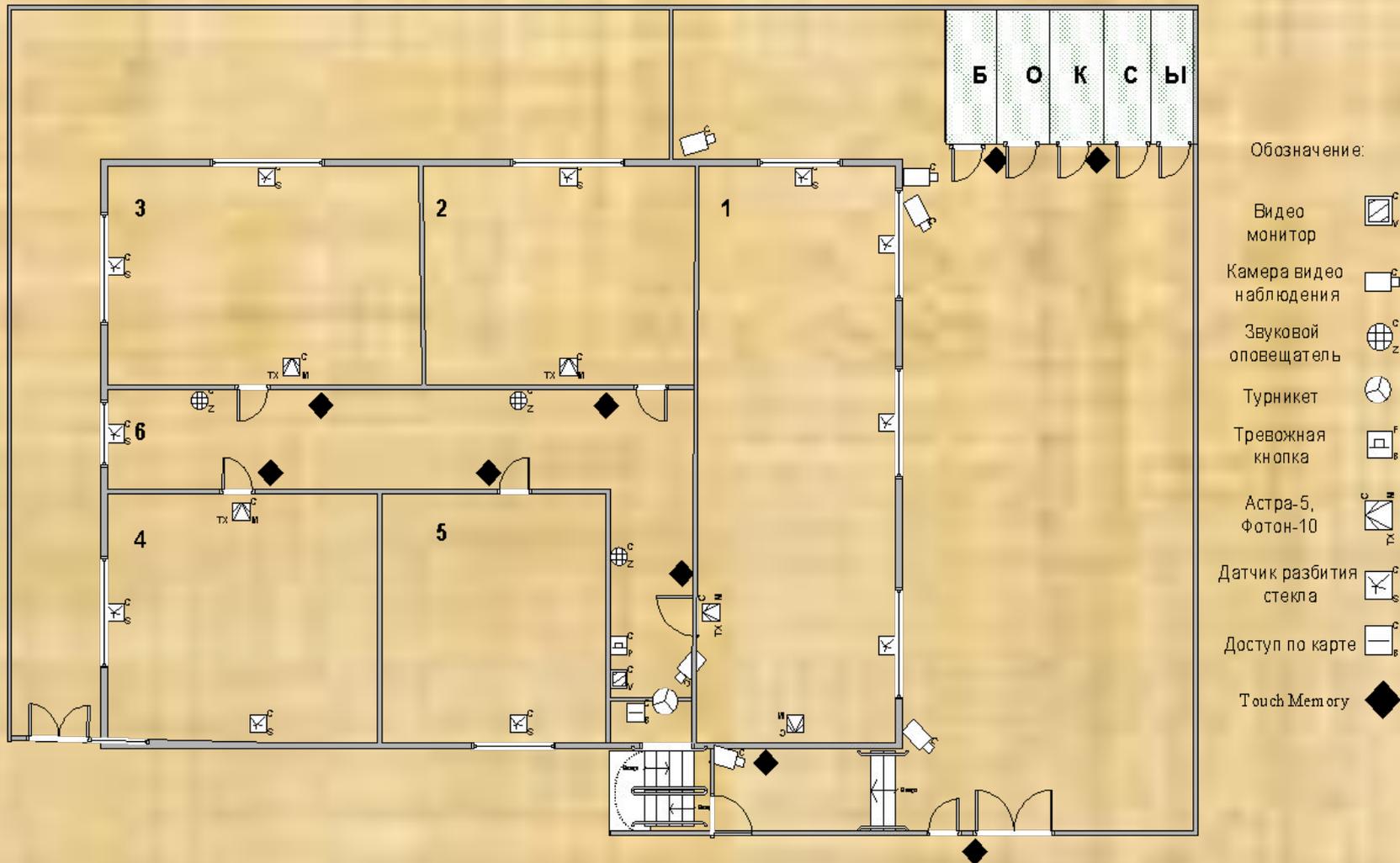
Оборудование организации средствами видеонаблюдения	80000рублей
Организация выделенного помещения	90000рублей
Установка охранно-тревожной сигнализации	110000рублей
Организация СКУД	25000рублей

Суммарные затраты 305000 рублей



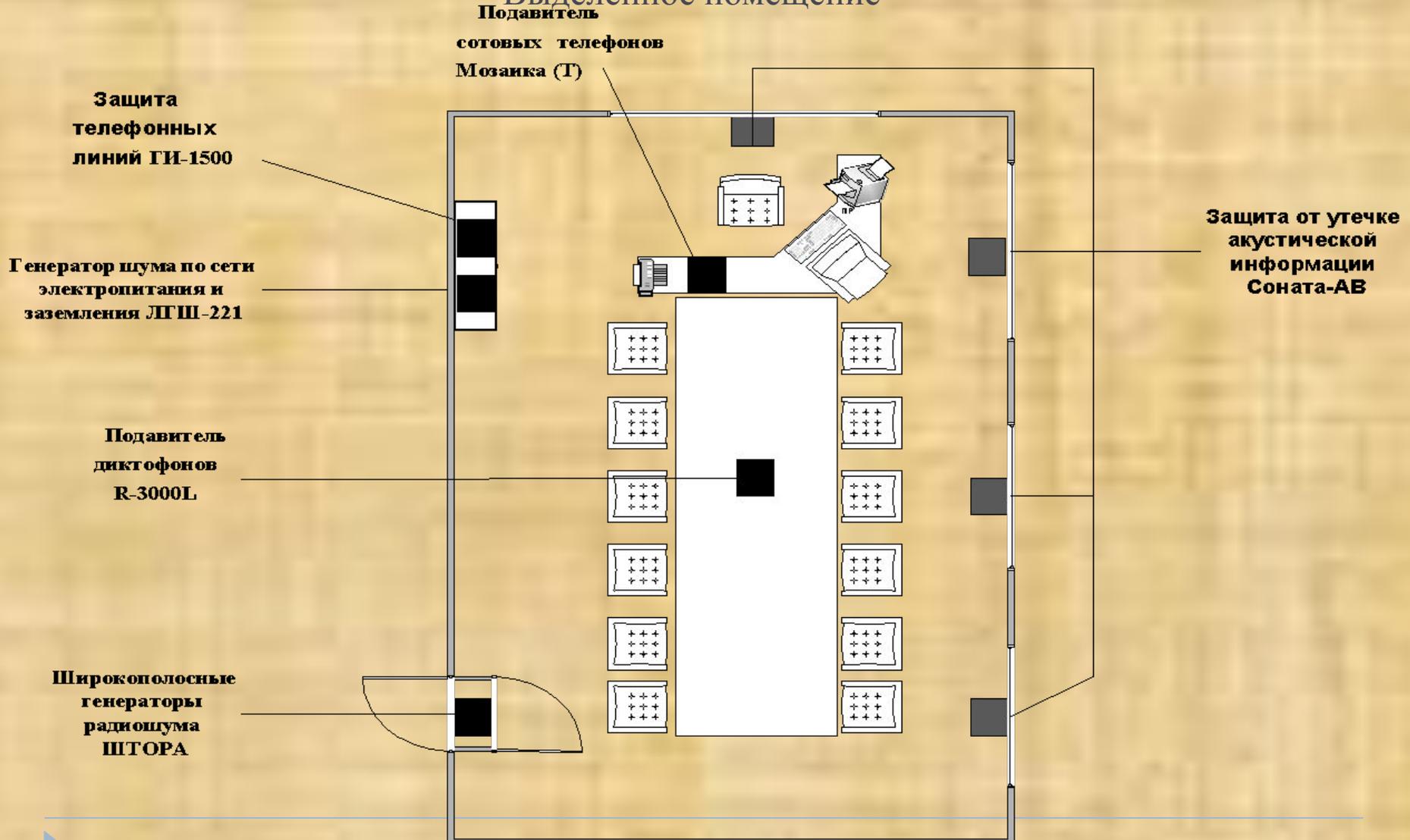
Реализация мер по повышению информационной безопасности

Схема модернизации системы охраны



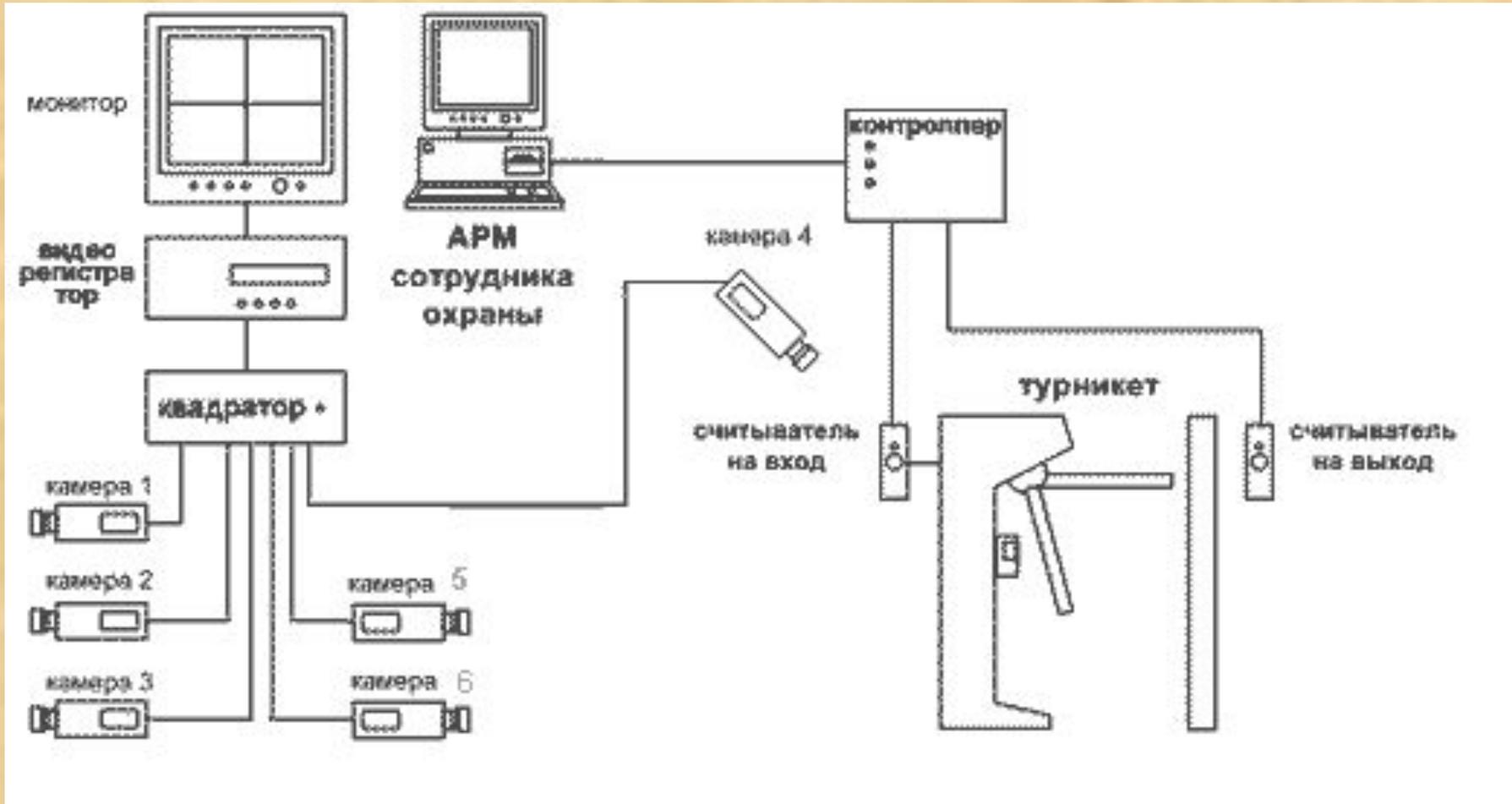
Реализация мер по повышению информационной безопасности

Выделенное помещение



Реализация мер по повышению информационной безопасности

Организация СКУД



Расчет экономических рисков в случае применения мер по повышению информационной безопасности

Коэффициент защищенности информационной системы

$$K^{\text{защ}} = 1 - \frac{R^{\text{защ}}}{R^{\text{нз}}} = 0,847$$

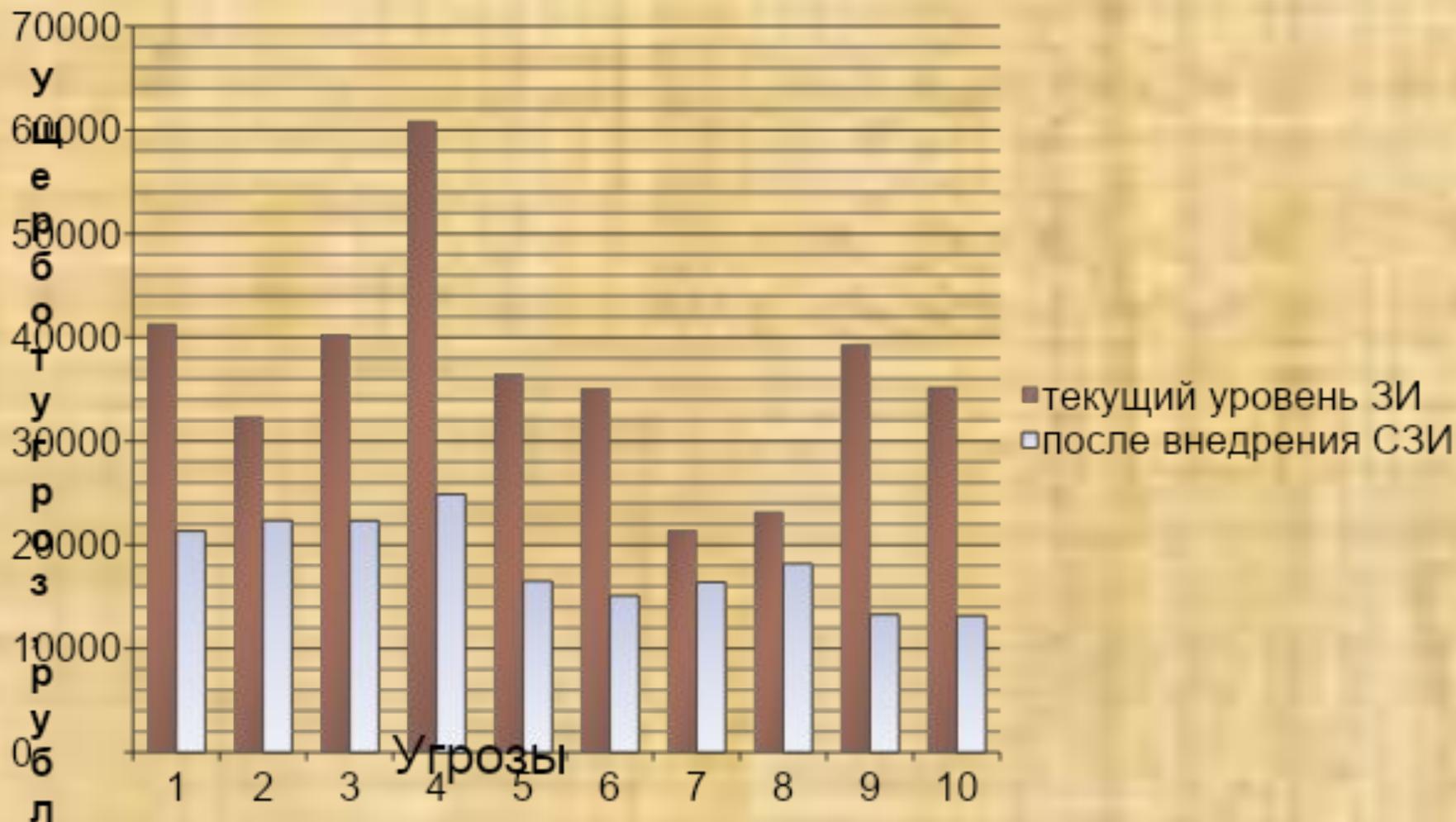
где $K^{\text{защ}}$ - коэффициент защищенности

$R^{\text{защ}}$ - риск для защищенной системы

$R^{\text{нз}}$ - риск для не защищенной системы

Расчет экономических рисков в случае применения мер по повышению информационной безопасности

Диаграмма ущерба от реализации угроз



Выводы

- Проведя анализ ОИ, была определена структура угроз, множество уязвимостей и информационных ресурсов. А так же были выделены имеющиеся в наличии средства обработки информации.
- И согласно РД МВД 78.36.003-2002 и постановлению Правительства Российской Федерации от 14 августа 1992 г. №585, был задан диапазон удовлетворительных значений общего показателя защищенности, коэффициентом 0,9.
- Но вследствие расчетов информационных рисков при текущем уровне обеспечения ИБ, было получено значение равное 0,5, что является недостаточным для данного рода организации. Поэтому было принято решение о разработке комплекса средств и мероприятий, направленных на совершенствование КСЗИ в рамках выделяемого организацией финансирования.
- По завершению внедрения дополнительных мер по ЗИ, был произведен перерасчет информационных рисков и был получен коэффициент защищенности равный 0,8. Что в целом говорит об эффективности внедряемых мер по защите информации.

▶ На основе полученных данных можно рекомендовать внедрение в организации предложенных мер.