Уфимский государственный авиационный технический университет

Кафедра Вычислительной техники и Защиты информации

**Разработка КСЗИ**

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовому проекту по

КСЗИ на предприятии

Группа ЗИ-509

Студент

Королёв Е.М.

Консультант

Никитин А.А.

Принял

Никитин А.А.

Уфа 2003 г.

Уфимский государственный авиационный технический университет

Кафедра ВТиЗИ

факультет ИРТ

## **Задание**

# на курсовое проектирование по Комплексной системе защиты информации на предприятии

на тему

Разработка КСЗИ

выдано 25 сентября2004 г.

студенту пятого курса

ЗИ-509 группы

Королёву Евгению Михайловичу

Срок выполнения 26 ноября 2004 г.

**Руководитель проекта** Никитин А.А.

**1. Технические условия**

1) План предприятия; 2) Сводная таблица стоимости информации

на предприятии;3) Сводная таблицы времени, необходимое для преодоления барьера, для задерживающих средств защиты;

**2. Содержание проекта**

1 Оценка вероятности несанкционированного доступа на охраняемый объект

2 Оценка и оптимизация коэффициента готовности средств сигнализации

3 Расчет показателя информационной безопасности и размера потенциального ущерба (риска)

**3. Оформление проекта**

1. Пояснительная записка – с рисунками и расчетными работами.
2. Чертежи.

Пояснительная записка содержит 21 листа, 11 рисунков, 7 таблиц

**4. Литература**

1. Организация и управление комплексной защитой информации на предприятии.

Методические указания к курсовой работе.

2. Попов Л.И., Зубарев А.В. Основные принципы повышения эффективности реализации мероприятий по комплексной защите информации. http://security.list.ru

3. Смирнов Н.В., Дунин-Барковский Н.В. Курс теории вероятности и математической статистики (для технических приложений). – М.: Наука, 1969. – 230 с

**Зав. кафедрой** Васильев В.И.

**Руководитель проекта** Никитин А.А.

**Реферат**

Пояснительная записка содержит 21 листа, 11 рисунков, 7 таблиц. Во время выполнения курсовой работы использовано 3 источника.

В данной курсовой работе составлена модель поведения злоумышленника при совершении проникновения на рассматриваемый объект, проведены расчеты надежности системы сигнализации и риска. Произведен анализ наиболее, уязвимых мест предприятия с точки зрения безопасности на основе выполненных расчетов.

**Содержание**

Введение

1 Оценка вероятности несанкционированного доступа на охраняемый объект

1.1 План помещения

1.2 Топологическая модель помещения

1.3 Модель поведения злоумышленника при совершении проникновения в помещение

1.4 Расчет вероятностей доступа к отдельным топологическим элементам

2 Оценка и оптимизация коэффициента готовности средств сигнализации

2.1 Расчет надежности системы сигнализации для каждого топологического элемента

2.2 Расчет коэффициентов готовности и коэффициентов простоя

2.3 Оптимизация периода профилактических работ

3 Расчет показателя информационной безопасности и размера потенциального ущерба (риска)

Заключение

Источники информации

**Введение**

Информационную безопасность предприятия определяет используемая им информационная технология, представляющая собой информационный процесс, реализуемый на распределенных по территории предприятия технических средств; а также наличие мест доступа или утечки информации, создающих потенциальную возможность реализации угроз; и наличие эффективных средств защиты.

В связи с тем, что различные охраняемые объекты расположены в различных помещениях, возможные пути несанкционированного доступа к ним также различны. Они определяются, в первую очередь, путями доступа в рассматриваемое помещение, основными из которых являются дверные и оконные проемы.

Наиболее эффективными мероприятиями, проведение которых целесообразно в первую очередь, представляются создание средств защиты от хищения носителей информации и обеспечение их надежности в эксплуатации. Средства защиты (защитные барьеры) предназначены для того, чтобы ликвидировать или уменьшить до приемлемого уровня последствия от вредных воздействий на информационный процесс.

Определение мероприятий по обеспечению требуемого уровня защищенности предполагает определение структуры, состава и размещения средств защиты информации, при которых обеспечивается требуемый уровень защищенности предприятия от реального спектра угроз безопасности. Задача синтеза системы защиты информации на предприятии должна проводиться на основе количественных показателей, полно и достоверно отражающих уровень информационной безопасности предприятия.

**1 Оценка вероятности несанкционированного доступа на охраняемый объект**

**1.1 План помещения**

На предприятии все информационные процессы могут быть обобщены в единый процессы могут быть обобщены в единый процесс, все нарушения которого связаны с реализацией угрозы хищения материальных ценностей, в том числе бумажных и электронных носителей информации в виде программ и электронных документов, компьютеров и периферийного оборудования и сервисного оборудования (копировальных аппаратов и т. п.).

Схема помещений рассматриваемого предприятия с пронумерованными кабинетами представлена на Рисунке 1.



Рисунок 1 – План помещений

**1.2 Топологическая модель помещения**

Элементы охраняемого пространства и связи между ними, определяющие возможность перехода из одного элемента в другой или проникновения извне (окон, дверей, переходов и т.д.), выявляются по плану его пространственного размещения. Они могут быть представлены в виде графа и соответствующей ему матрицы смежности, где - множество помещений (топологических элементов, выявленных ранее); – множество связей между ними. Связь между внутренними помещениями предприятия и внешней средой соответствует наличию входных дверей и оконных проемов, через которые потенциально возможно осуществить проникновение (Рисунок 2).



Рисунок 2 – Граф путей доступа в помещение



Таким образом, топологическая модель пространственного размещения предприятия представляет собой неориентированный граф G, вершины которого соответствуют топологическим элементам предприятия (помещениям, различным охраняемым и неохраняемым зонам), а дуги – связям между этими элементами, определяющими возможность перехода злоумышленника из одного топологического элемента в другой.

Каждому элементу охраняемого пространства сопоставляется состояние злоумышленника в процессе совершения злоумышленных действий. Каждому состоянию злоумышленника сопоставим нахождение его в элементах охраняемого пространства, на котором находится предприятие. Начальное состояние злоумышленника при этом соответствует его нахождению в неохраняемом пространстве, который будем интерпретировать как элемент пространства .



**1.3 Модель поведения злоумышленника при совершении проникновения в помещение**

Проникновение на предприятие возможно по двум основным путям – через главный вход в предприятие и наружные окна. Двери предприятия оснащены замками и тревожной сигнализацией, срабатывающей при открытии или взломе двери. Окна оснащены металлическими решетками и тревожной сигнализацией. Срабатывание сигнализации отражается на пульте охраны, которая осуществляет функцию обнаружения места проникновения и удаления злоумышленника из помещений предприятия. Пронумеровав все имеющиеся помещения, составляем топологическую модель предприятия в виде графа , который показан на Рисунке 3.



Рисунок 3 – Топологическая модель помещения в виде графа



Путь, выбираемый злоумышленником, зависит от многих условий, таких как цели проникновения, осведомленность злоумышленника о структуре предприятия и имеющихся средствах защиты, техническая оснащенность злоумышленника и т. п. В условиях неопределенности относительно выбора злоумышленника начала пути проникновения примем вероятности выбора того или иного направления действий равными.

**1.4 Расчет вероятностей доступа к отдельным топологическим элементам**

Для выполнения курсового проекта были предоставлены следующие значения параметров системы защиты информации:

1 Надежность имеющейся на предприятии СЗИ:

- интенсивность отказов элементов комплекса: 1 раз в 365 суток;

- период профилактических работ: 182 суток;

- длительность профилактических работ: 8 часов;

- длительность восстановления системы сигнализации в случае поломки: 36 часов.

2 Стоимость информации хранимой на предприятии (Таблица 1).

Таблица 1 – Стоимость информации хранимой на предприятии

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Номер комнаты | 1 | 2 | 3 | 4 | 5 | 6 | Итого |
| Стоимость (руб.) | 5000 | 15000 | 25000 | 40000 | 35000 | 20000 | 140000 |

3 Время, необходимое для преодоления барьера, для задерживающих средств защиты (Таблица 2).

Таблица 2 - Время, необходимое для преодоления барьера, для задерживающих средств защиты (мин.)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Номер помещения | Наименование барьера | | | | | | |
| окна (решетки) | | двери (замки) | | | | входная дверь |
| 1 | 2 | 1 | 2 | 3 | 4 |
| 1 | - | - | 16 | 19 | 20 | 19 | 28 |
| 2 | 20 | - | 16 | 13 | - | - | - |
| 3 | 21 | - | 13 | - | - | - | - |
| 4 | 20 | 20 | 19 | - | - | - | - |
| 5 | - | - | 20 | - | - | - | - |
| 6 | 23 | - | 19 | - | - | - | - |

4 Время реакции для удаляющих средств защиты (Таблица 3)

Таблица 3 - Время реакции для удаляющих средств защиты

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Номер помещения | 1 | 2 | 3 | 4 | 5 | 6 |
| Время (мин.) | 3 | 4 | 6 | 6 | 5 | 4 |

Заменим значения элементов матрицы смежности вершин графа на значения переходных вероятностей:



* – вероятность удаления злоумышленника из i-го охраняемого помещения в неохраняемое пространство;



* – вероятность преодоления барьера злоумышленником при переходе из i-го помещения в j-е (при условии, что преступник не был до сих пор схвачен);



Для расчета переходных вероятностей используются следующие параметры систем защиты: – интенсивность событий удаления злоумышленника из охраняемых помещений; – интенсивность событий преодоления злоумышленником защитного барьера.



Период времени, в течение которого злоумышленником может быть совершено не более одного перехода из одного помещения в другое определяется исходя из выражения

, (1)



где - сумма интенсивностей всех событий в системе.



В Таблице 4 приведены значения интенсивности событий преодоления злоумышленником защитного барьера и вероятность преодоления барьера злоумышленником.

Таблица 4 – Вероятности проникновения злоумышленника в помещение

|  |  |  |  |
| --- | --- | --- | --- |
| i-е помещение | j-е помещение |  | Вероятность |
| 0 | 1 | 0,0357 | 0,0438 |
| 0 | 2 | 0,0500 | 0,0613 |
| 0 | 3 | 0,0476 | 0,0583 |
| 0 | 4 | 0,0500 | 0,0613 |
| 0 | 6 | 0,0435 | 0,0533 |
| 1 | 2 | 0,0625 | 0,0766 |
| 1 | 4 | 0,0526 | 0,0645 |
| 1 | 5 | 0,0500 | 0,0613 |
| 1 | 6 | 0,0526 | 0,0645 |
| 2 | 1 | 0,0625 | 0.0766 |
| 2 | 3 | 0,0769 | 0,0942 |
| 3 | 2 | 0,0769 | 0,0942 |
| 4 | 1 | 0,0526 | 0,0645 |
| 5 | 1 | 0.0500 | 0.0613 |
| 6 | 1 | 0,0526 | 0,0645 |

Исходя из полученных интенсивностей , находим и вычисляем .



В Таблице 5 приведены значения интенсивность событий удаления злоумышленника из охраняемых помещений и вероятность удаления злоумышленника.

Таблица 5 – Вероятность удаления злоумышленника из i-го помещения

|  |  |  |
| --- | --- | --- |
| Номер помещения |  | Вероятность |
| 1 | 0,0333 | 0,4085 |
| 2 | 0,2500 | 0,3064 |
| 3 | 0,1667 | 0,2042 |
| 4 | 0,1667 | 0,2042 |
| 5 | 0,2000 | 0,2451 |
| 6 | 0,2500 | 0,3064 |

Составим матрицу смежности (Таблица 6).

Таблица 6 – Матрица смежности

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | А0 | А1 | А2 | А3 | А4 | А5 | А6 |
| А0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| А1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| А2 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| А3 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| А4 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| А5 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| А6 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |

Матрица переходных вероятностей будет иметь вид:



Итак получаем следующую матрицу переходных вероятностей:



Решая систему уравнений Колмогорова-Чепмена для дискретного времени, определяются финальные вероятности нахождения преступника в различных состояниях, то есть в различных комнатах помещения:

, (2)



где – вектор-строка начального состояния системы; – квадратная матрица переходных вероятностей; – вектор-столбец анализируемого состояния, который имеет все нулевые элементы и одну единицу, которая стоит в позиции, соответствующей порядковому номеру анализируемого состояния.



Получим финальные вероятности нахождения злоумышленника в различных комнатах помещения.



Таким образом, вероятность неуспешной реализации угрозы доступа равна P0=0.728, где P0 – вероятность нахождения злоумышленника за пределами помещения в конкретный момент времени (в общем случае комнаты, где нет ценностей).



Графики зависимости вероятностей доступа в отдельные помещения объекта от времени, начиная от момента начала атаки, приведены на Рисунке 4. График изменения защищенности объекта в зависимости от времени, прошедшего от момента начала атаки приведен на Рисунке 5.

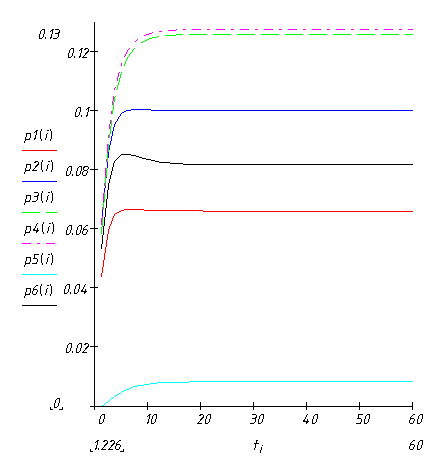


Рисунок 4 – График изменения вероятностей доступа в отдельные помещения кафедры в зависимости от времени

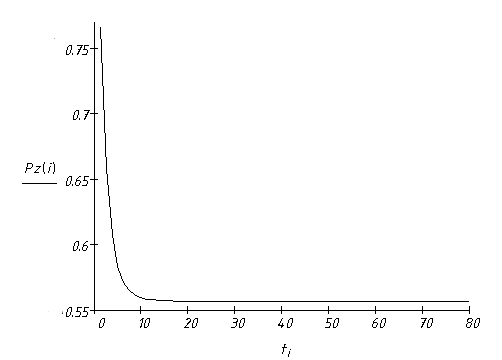


Рисунок 5 – График изменения защищенности объекта в зависимости от времени, прошедшего от момента начала атаки

**2 Оценка и оптимизация коэффициента готовности средств сигнализации**

**2.1 Расчет надежности системы сигнализации для каждого топологического элемента**

Структурная схема для расчета надежности отдельной ветви системы сигнализации приведена на Рисунке 6. Произведем ее декомпозицию на четыре блока:

Блок 1 – датчики:

а) датчики открытия двери;

б) датчики движения;

Блок 2 – линии связи, по которым передается сигнал от датчиков на центральный пульт охраны;

Блок 3 – пульт охранной сигнализации;

Блок 4 – блок питания.



Рисунок 6 – Структурная схема для расчета надежности сигнализации

Из опыта известно, что показатели безотказности элементов каждого блока равны:



Для расчета надежности по схеме (Рисунок 6) определим вероятность безотказной работы каждого блока:

* Блок 1: , поскольку отказ любого комплекта датчиков не приведет к отказу системы;



* Блок 2: ;



* Блок 3: ;



* Блок 4: .



Тогда вероятность безотказной работы системы сигнализации буде вычисляться по формуле (3).

(3)



На Рисунке 7 приведены графики изменения вероятностей безотказной работы в зависимости от времени.

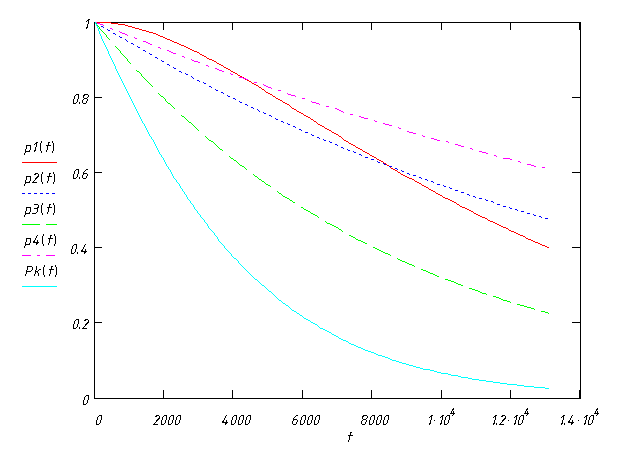


Рисунок 7 - Вероятности безотказной работы отдельных блоков и системы сигнализации в целом

Интенсивность отказов блоков определяется по формулам (4):

(4)



Построим графики зависимости интенсивностей от времени (Рис. 8).

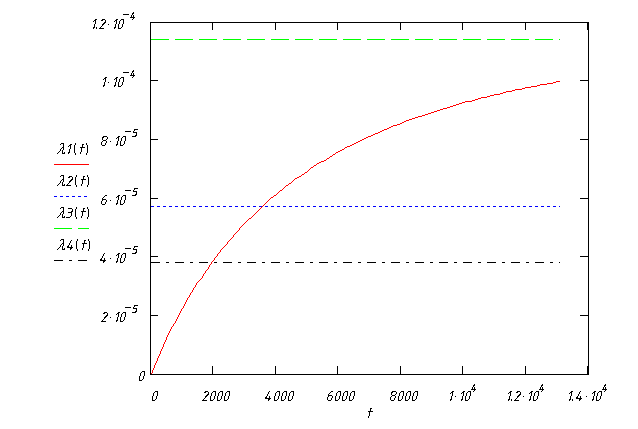


Рисунок 8 – Графики изменения интенсивностей в зависимости от времени

**2.2 Расчет коэффициентов готовности и коэффициентов простоя**

Оценим коэффициент готовности системы охранной сигнализации и рассмотрим возможность его повышения за счет выбора оптимального периода проведения профилактических работ.

Глубина контроля блока датчиков равна нулю (), поскольку датчики не контролируются, а любой отказ линий связи, пульта охранной сигнализации и блока питания обнаруживается автоматически, поэтому значения их глубины контроля могут быть приняты равными единице, т.е. .



Интенсивность отказов комплекса определяется по формуле (5), а глубина контроля всей системы по формуле (6).

(5)



(6)

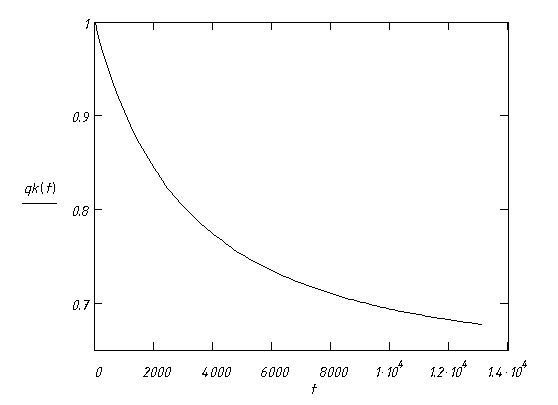


Рисунок 9 - График зависимости глубины контроля всей системы от времени

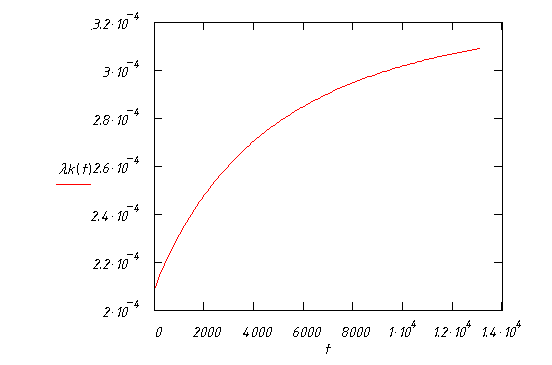


Рисунок 10 – Зависимость интенсивности отказов комплекса от времени



Профилактические работы в помещении проводятся 2 раза в год, то есть интенсивность профилактических работ равна:

(7)



Определяем значения показателей системы к моменту начала профилактических работ. Время наработки к началу профилактических работ составляет:

(8)



Вычислим значения интенсивностей профилактических работ для каждой комнаты:



Устанавливаем параметры системы технического обслуживания. Профилактические работы проводятся в течение 8 часов, т. е. интенсивность обслуживания: (9)



В случае наличия неисправностей в системе сигнализации ремонтные работы проводятся в течение 1,5 суток, т. е. интенсивность восстановления составляет

(10)



Определим состав анализируемых состояний комплекса:

- - работоспособное состояние;



- - состояние контролируемого отказа;



- - состояние неконтролируемого отказа;



- - состояние проведения профилактических работ.



Составим диаграмму графа, моделирующего поведение системы с учетом процессов технического обслуживания (Рисунок 7).



Рисунок 11 - Диаграмма графа, моделирующего поведение системы с учетом процессов технического обслуживания

По полученному графу составим систему уравнений Колмогорова-Чепмена:

(11)



Решая систему, получим значение коэффициента готовности:

(12)



Коэффициент простоя равен:

(13)



Итак, коэффициент готовности равен , а коэффициент простоя .



**2.3 Оптимизация периода профилактических работ**

Для определения минимального значения коэффициента простоя находим его производную по интенсивности профилактических работ и приравниваем ее к нулю.

Оптимальные интенсивность и период профилактических работ при заданных параметрах обслуживания и ожидания равны:

(14)



(15)



(16)



Получаем значение оптимального периода профилактических работ, который равен 353 часа или 15 дней. При этом оптимальный коэффициент простоя равен , а коэффициент готовности .



**3 Расчет показателя информационной безопасности и размера потенциального ущерба (риска)**

Размер потенциального ущерба (риска) в случае реализации угрозы определяется по формуле:

(17)



где – стоимость ценностей, хранимых в i-ой комнате



(18)



где – коэффициент готовности,



– финальная вероятность нахождения злоумышленника в i-ой комнате.



Риск потенциального ущерба после оптимизации:

(19)



Рассчитанные значения рисков до оптимизации и после оптимизации приведены в Таблице 9:

Таблица 7 - Оптимизация периода профилактических работ

|  |  |  |
| --- | --- | --- |
| Номер комнаты | Риск до оптимизации Ri | Риск после оптимизации Ri |
| 1 | 1390 | 573 |
| 2 | 4565 | 2202 |
| 3 | 8110 | 4286 |
| 4 | 13038 | 6934 |
| 5 | 8167 | 2092 |
| 6 | 5808 | 2595 |
| Все помещение | 41078 | 18682 |

Коэффициент выгоды системы защиты:



То есть оптимальная организация профилактических работ позволила бы снизить риск в 2,2 раза.

При использовании установленной системы защиты до оптимизации возможный суммарный ущерб при реализации угрозы составил бы до 29% от стоимости хранимых в помещении ценностей.

После оптимизации возможный суммарный ущерб уменьшился на 16% и составляет до 13%.

**Заключение**

В результате анализа наиболее, уязвимых мест рассматриваемого объекта выяснилось, что комнаты 2, 3 и 4 являются самыми уязвимыми. Возможный риск от реализации одной угрозы составил бы 41078 рублей.

После оптимизации периода профилактических работ, когда коэффициент готовности средств сигнализации равен 0,948, возможный риск составил бы 18682 рублей, т. е. оптимальная организация профилактических работ позволила бы снизить риск в 2,2 раза.

Таким образом, на рассматриваемом предприятии необходимо:

* повысить безопасность во второй, третьей и четвертой комнатах;
* использовать оптимальный период профилактических работ.

**Источники информации**

1 Организация и управление комплексной защитой информации на предприятии. Методические указания к курсовой работе.

2 Попов Л.И., Зубарев А.В. Основные принципы повышения эффективности реализации мероприятий по комплексной защите информации. http://security.list.ru

3 Смирнов Н.В., Дунин-Барковский Н.В. Курс теории вероятности и математической статистики (для технических приложений). – М.: Наука, 1969. – 230 с.