

Министерство образования Республики Беларусь  
Учреждение образования  
«Белорусский государственный университет  
информатики и радиоэлектроники»

Кафедра проектирования информационно-компьютерных систем

**ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОЕКТИРОВАНИЯ  
ЭЛЕКТРОННЫХ СИСТЕМ БЕЗОПАСНОСТИ.  
ЛАБОРАТОРНЫЙ ПРАКТИКУМ**

Под редакцией С. М. Боровикова

*Рекомендовано УМО по образованию в области  
информатики и радиоэлектроники для специальности  
1-39 03 01 «Электронные системы безопасности» в качестве пособия*

Минск БГУИР 2014

УДК 621.396.6-027.31:654.9(076.5)  
ББК 32.844-02я73  
Т33

**Авторы:**

С. М. Боровиков, Е. Н. Шнейдеров, Р. П. Гришель,  
А. И. Бересневич, А. И. Бурак

**Рецензенты:**

кафедра информационных технологий в управлении  
Белорусского национального технического университета  
(протокол №9 от 30.05.2013);

профессор кафедры радиоэлектроники учреждения образования  
«Минский государственный высший радиотехнический колледж»,  
доктор технических наук, профессор Ф. Д. Троян

**Теоретические основы проектирования электронных систем без-**  
Т33 **опасности. Лабораторный практикум : пособие / С. М. Боровиков [и др.] ;**  
**под ред. С. М. Боровикова. – Минск : БГУИР, 2014. – 70 с. : ил.**  
**ISBN 978-985-543-019-4.**

Состоит из описания пяти лабораторных работ по учебной дисциплине «Теоретические основы проектирования электронных систем безопасности» для студентов специальности «Электронные системы безопасности» всех форм обучения.

Может быть использовано для проведения практических занятий по указанной дисциплине и выполнения лабораторных работ по учебной дисциплине «Теоретические основы проектирования и надёжности радиоэлектронных средств» специальности «Моделирование и компьютерное проектирование радиоэлектронных средств».

**УДК 621.396.6-027.31:654.9(076.5)**  
**ББК 32.844-02я73**

**ISBN 978-985-543-019-4**

© УО «Белорусский государственный  
университет информатики  
и радиоэлектроники», 2014

## СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ .....	5
<b>ЛАБОРАТОРНАЯ РАБОТА №1. АНАЛИЗ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЭЛЕКТРОННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ, ОБЕСПЕЧИВАЮЩЕЙ МОНИТОРИНГ СИТУАЦИИ НА ПЕРЕКРЁСТКЕ.....</b>	<b>6</b>
1.1. Цель работы.....	6
1.2. Краткие теоретические сведения .....	6
1.3. Исследуемая ЭСБ и особенность учебной программы для ЭВМ.....	8
1.4. Показатель эффективности функционирования ЭСБ .....	9
1.5. Задания на экспериментальную часть лабораторной работы .....	13
1.6. Содержание отчёта .....	14
1.7. Контрольные вопросы .....	15
Литература .....	15
<b>ЛАБОРАТОРНАЯ РАБОТА №2. ОЦЕНКА УЯЗВИМОСТИ ЭСБ МЕТОДОМ АНАЛИЗА ПУТЕЙ ПРОНИКНОВЕНИЯ К ОХРАНЯЕМЫМ РЕСУРСАМ .....</b>	<b>16</b>
2.1. Цель работы.....	16
2.2. Теоретические сведения .....	16
2.3. Описание и анализ исследуемой ЭСБ.....	19
2.4. Особенности учебной программы для ЭВМ.....	19
2.5. Задания на экспериментальную часть лабораторной работы .....	20
2.6. Содержание отчёта .....	21
2.7. Контрольные вопросы .....	22
Литература .....	22
<b>ЛАБОРАТОРНАЯ РАБОТА №3. ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЭСБ С УЧЁТОМ ЛОЖНЫХ ТРЕВОГ .....</b>	<b>23</b>
3.1. Цель работы.....	23
3.2. Теоретические сведения .....	23
3.3. Описание и анализ исследуемой ЭСБ.....	25
3.4. Особенности учебной программы для ЭВМ.....	27
3.5. Задания на экспериментальную часть лабораторной работы .....	27
3.6. Содержание отчёта .....	28
3.7. Контрольные вопросы .....	29
Литература .....	29

ЛАБОРАТОРНАЯ РАБОТА №4. ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЭСБ МЕТОДОМ ДЕКОМПОЗИЦИИ .....	30
4.1. Цель работы .....	30
4.2. Описание исследуемой ЭСБ.....	30
4.3. Методические указания по исследованию эффективности функционирования ЭСБ .....	33
4.4. Задания на экспериментальную часть лабораторной работы.....	49
4.5. Содержание отчёта .....	52
4.6. Контрольные вопросы.....	53
Литература .....	54

ЛАБОРАТОРНАЯ РАБОТА №5. ВЛИЯНИЕ ВИДА СРЕДСТВ ОБНАРУЖЕНИЯ И МОДЕЛЕЙ НАРУШИТЕЛЕЙ НА ЭФФЕКТИВНОСТЬ ФУНКЦИОНИРОВАНИЯ ЭСБ .....	55
5.1. Цель работы .....	55
5.2. Краткие теоретические сведения.....	55
5.3. Показатель эффективности функционирования ЭСБ.....	59
5.4. Описание программы для ЭВМ .....	60
5.5. Задания на экспериментальную часть лабораторной работы.....	61
5.6. Содержание отчёта .....	62
5.7. Контрольные вопросы.....	62
Литература .....	63

Приложение 1. Проверка значимости коэффициента корреляции .....	64
Приложение 2. Преобразование Фишера .....	67
Приложение 3. Справочная информация к лабораторной работе №4 .....	68

## ПРЕДИСЛОВИЕ

В соответствии с учебным планом специальности 1-39 03 01 «Электронные системы безопасности» дисциплина «Теоретические основы проектирования электронных систем безопасности» (ТОПЭСБ) предусматривает 16 часов лабораторных и 28 часов практических занятий.

Предлагаемый лабораторный практикум включает пять виртуальных лабораторных работ. Слово «виртуальные» подчёркивает то, что структура и состав электронной системы безопасности (ЭСБ), защищаемые объекты, процесс функционирования ЭСБ и их устройств моделируются в памяти ЭВМ. Практикум позволяет сформировать умения и развить навыки практической подготовки студентов по дисциплине ТОПЭСБ в соответствии с учебной программой дисциплины.

В процессе освоения дисциплины студент должен выполнить лабораторные работы. Конкретный перечень работ уточняется рабочей программой на текущий учебный год. Расчётно-аналитические методы, используемые в лабораторной работе №4 для оценки эффективности функционирования подсистем, на которые разбивается сложная ЭСБ, могут рассматриваться на практических занятиях с выдачей студентам индивидуальных заданий.

Виртуальные лабораторные работы разрабатывались кафедрой проектирования информационно-компьютерных систем (ПИКС) в рамках выполнения задания по молодёжному гранту на совершенствование учебного процесса по теме «Теоретические основы проектирования электронных систем безопасности: лабораторный практикум с использованием виртуальных объектов и систем».

В разработке и отладке прикладного программного обеспечения виртуальных лабораторных работ (программ для ЭВМ) приняли участие магистранты кафедры ПИКС А. А. Бруй, Ю. В. Янцевич, студенты Е. В. Ананич (группа 980223), Д. А. Сташевский (группа 912601) и Н. В. Сасковец (группа 902501).

Авторы будут признательны за высказанные рекомендации и предложения по усовершенствованию содержания и сценариев виртуальных лабораторных работ (e-mail: bsm@bsuir.by).

# **ЛАБОРАТОРНАЯ РАБОТА №1**

## **АНАЛИЗ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЭЛЕКТРОННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ, ОБЕСПЕЧИВАЮЩЕЙ МОНИТОРИНГ СИТУАЦИИ НА ПЕРЕКРЁСТКЕ**

### **1.1. Цель работы**

На примере системы видеонаблюдения как электронной системы безопасности (ЭСБ), обеспечивающей мониторинг движения транспорта на перекрёстке, ознакомиться с методами построения показателя, используемого для описания эффективности функционирования ЭСБ, и исследовать влияние на эффективность функционирования эксплуатационно-технических характеристик видеочамер и параметров их установки (крепления).

### **1.2. Краткие теоретические сведения**

Контроль движения транспорта и людей на перекрёстках улиц и дорог является весьма актуальной задачей для автоинспекции и правоохранительных органов. Постоянный контроль может быть обеспечен с помощью видеомониторинга, выполняемого системой видеонаблюдения.

Основная задача видеомониторинга состоит в идентификации объектов (автомобилей, людей и пр.), особенно в случаях, когда необходимо воспроизвести картину дорожно-транспортного происшествия и определить виновных лиц. Идентификация важна при анализе видеозаписей при расследовании дорожно-транспортных происшествий. Достоверность идентификации во многом зависит как от эксплуатационно-технических характеристик видеочамер, так и параметров их установки (монтажа на контролируемом объекте).

Промышленно выпускаемые видеочамеры имеют разные эксплуатационно-технические характеристики. Важнейшими из них являются:

- угол обзора;
- фокусное расстояние объектива;
- вероятность идентификации (распознавания);
- разрешающая способность;
- минимальная освещённость;
- стоимость.

Следует знать, что вероятность идентификации объектов зависит как от установки видеочамеры, так и от фокусного расстояния объектива. Вероятность идентификации также существенно зависит от времени суток и погодных условий (дождь, снег, туман). Ночью и при наличии осадков вероятность идентификации заметно падает. В солнечные дни вероятность идентификации возрастает, но всё равно во всех случаях она меньше единицы.

С уменьшением фокусного расстояния объектива заметно возрастает зона обзора видеочамеры, но уменьшается вероятность правильной идентификации объектов. Для повышения зоны обзора местности и повышения вероятности

идентификации объектов, как правило, одновременно используют несколько видеокамер. В тех зонах, контроль которых ведут две и более видеокамеры, вероятность идентификации заметно возрастает.

Для представления информации от видеокамер оператору необходимо использовать оборудование мультиплексирования видеосигналов от видеокамер с выводом информации на дисплей. В качестве устройства мультиплексирования видеосигналов, поступающих от видеокамер, используют видеорегистраторы с монитором. Общая схема сопряжения видеокамер с видеорегистратором и монитором приведена на рис. 1.1.

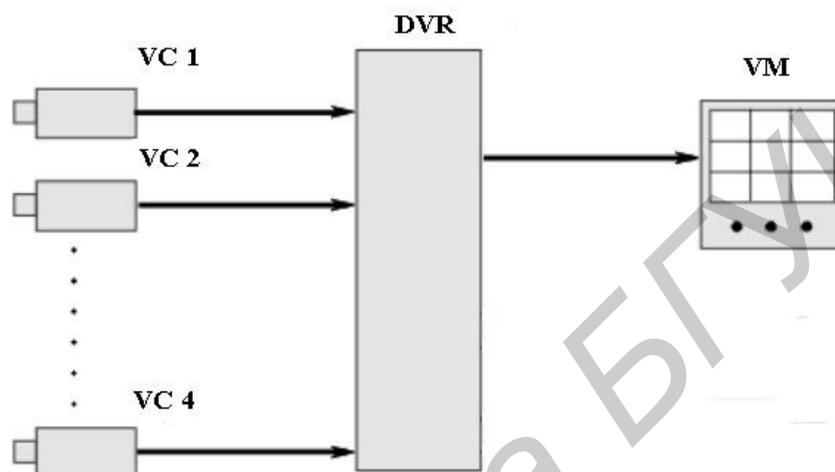


Рис. 1.1. Схема сопряжения видеорегистратора с монитором и видеокамерами:  
VC1...VC4 – видеокамеры; DVR – видеорегистратор; VM – видеомонитор

Удачность функционирования ЭСБ оценивают количественным критерием, называемым показателем эффективности функционирования. Он представляет собой количественную меру, с помощью которой судят о качестве и (или) объеме выполненной системой работы и т. д. Другими словами, эффективность функционирования ЭСБ – это мера выходного эффекта системы [1].

Показатель эффективности функционирования ЭСБ в течение времени  $t$  будем определять по формуле

$$E(t) = \sum_i h_i(t) \Phi_i, \quad (1.1)$$

где  $h_i(t)$  – вероятность того, что система в течение времени  $t$  будет находиться в  $i$ -м техническом состоянии;

$\Phi_i$  – коэффициент эффективности  $i$ -го технического состояния системы.

Переход ЭСБ из одного технического состояния (далее – просто состояния) в другое обусловлен потерей работоспособности той или иной составной части ЭСБ, например отказом и, следовательно, потерей работоспособности одной из видеокамер ЭСБ. В качестве коэффициентов эффективности  $\Phi_i$  логично рассматривать вероятность идентификации объекта в выделенной зоне контроля в случае нахождения ЭСБ в  $i$ -м состоянии.

### 1.3. Исследуемая ЭСБ и особенность учебной программы для ЭВМ

В качестве исследуемой ЭСБ рассматривается система видеоконтроля (мониторинга) ситуации на перекрёстке проспекта Независимости и улицы П. Бровки в городе Минске. В учебной программе для ЭВМ выделенная зона контроля включает перекрёсток дорог и пешеходный переход на ул. П. Бровки. Мониторинг на перекрёстке и пешеходном переходе должен выполняться в любое время суток и при любых погодных условиях (дождь, снег, туман). В качестве продолжительности при оценке эффективности функционирования ЭСБ взят один год.

ЭСБ, исследуемая в лабораторной работе, включает три видеокамеры, видеорегистратор, каналы передачи сигналов от видеокамер к видеорегистратору и монитор. Виртуальными в лабораторной работе являются перекрёсток, здания и территории, примыкающие к нему, а также сами видеокамеры ЭСБ. Предполагается, что видеорегистратор и монитор, используемый оператором, установлены в специально отведённом помещении. Каналы передачи сигналов – телекоммуникационные проводные.

Видеокамеры могут устанавливаться на зданиях учебного корпуса МГВРК, общежития БНТУ и служебного двухэтажного корпуса клинической больницы №1, а также на осветительных мачтах, расположенных на проспекте Независимости. Предельная высота установки видеокамер  $h$  на зданиях и осветительных мачтах указана на плане перекрёстка (см. главное окно программы для ЭВМ). Предусмотрены виртуальные устройства, позволяющие осуществлять поворот видеокамер в горизонтальной плоскости от  $-180$  до  $+180^\circ$  и изменение наклона по вертикали от  $0$  до  $90^\circ$ . На главном окне программы они обозначены соответственно как **Горизонтальный поворот** (радиус  $R$ ) и **Угол наклона** ( $A$ ).

Назначение кнопок на главном окне учебной программы для ЭВМ поясняется в табл. 1.1.

Таблица 1.1

Назначение кнопок программы

Название кнопки	Назначение, пояснение	Примечание
1. Уменьш	Уменьшение размера схемы перекрёстка	–
2. 100 %	Восстановление исходного (100-процентного) размера схемы перекрёстка	–
3. Увелич	Увеличение размера схемы перекрёстка	–
4. Спутник	Фотография перекрёстка со спутника	Режим фотоснимка из космоса
5. Тест	Выдача тестового задания студентам	Генерируется случайным образом
6. Задание	Задание на выполнение экспериментальной части лабораторной работы	–
7. Видео	Просмотр видеопрограммы по работе с программой	Приводятся отдельные этапы
8. Проекты	Показ/скрытие таблицы проектных решений системы видеонаблюдения (ЭСБ)	–
9. Удалить	Удаление установленной видеокамеры	–

## 1.4. Показатель эффективности функционирования ЭСБ

Обозначим через  $r_j(t)$  вероятность того, что  $j$ -я видеокамера будет иметь работоспособное состояние в произвольный момент времени, и с этого момента времени будет работать безотказно в течение заданного времени  $t$ , где  $j$  – номер видеокамеры,  $j = 1, 2, 3$ . В теории надёжности технических изделий этот показатель называют коэффициентом оперативной готовности за время  $t$  [1, 2]. Время  $t$  при определении эффективности функционирования ЭСБ выбрано равным одному году (8 760 часов).

Вероятности идентификации объектов в выделенной зоне перекрёстка  $j$ -й видеокамерой в определенных условиях обозначим как  $p_j^{(усл)}$ , где верхний индекс (усл) может обозначать д (день), н (ночь), о (осадки), т (туман).

Допущения, принятые в лабораторной работе:

1) видеорегистратор, каналы передачи сигналов и монитор имеют идеальную надёжность, т. е. вероятности их работоспособного состояния в течение времени  $t$  приняты равными единице;

2) видеорегистратор, каналы передачи сигналов и монитор с точки зрения восприятия, передачи и отображения картинок, получаемых от видеокамер, являются также идеальными, т. е. указанные технические части ЭСБ не изменяют вероятность правильной идентификации объектов.

С учётом сделанных допущений при построении показателя эффективности функционирования ЭСБ во внимание будут приняты только надёжность видеокамер и степень их способности идентифицировать объекты в то или иное время суток (день, ночь) и в тех или иных погодных условиях (осадки, туман).

Ниже в таблице приведены формулы, которые будут использоваться для определения технических состояний исследуемой ЭСБ, включающей три видеокамеры (табл. 1.2).

Таблица 1.2

Возможные технические состояния рассматриваемой ЭСБ

Номер технического состояния ЭСБ, $i$	Описание технического состояния ЭСБ: состояние работоспособности видеокамер ВК1...ВК3			Условное обозначение состояния	Формула определения вероятности технического состояния ЭСБ в целом $h_i(t)$
	ВК1	ВК2	ВК3		
1	1	1	1	1 1 1	$h_1(t) = r_1(t) r_2(t) r_3(t)$
2	1	1	0	1 1 0	$h_2(t) = r_1(t) r_2(t) [(1 - r_3(t))]$
3	1	0	1	1 0 1	$h_3(t) = r_1(t) [(1 - r_2(t)) r_3(t)]$
4	1	0	0	1 0 0	$h_4(t) = r_1(t) [(1 - r_2(t)) [(1 - r_3(t))]]$
5	0	1	1	0 1 1	$h_5(t) = [(1 - r_1(t)) r_2(t) r_3(t)]$
6	0	1	0	0 1 0	$h_6(t) = [(1 - r_1(t)) r_2(t) [(1 - r_3(t))]]$
7	0	0	1	0 0 1	$h_7(t) = [(1 - r_1(t)) [(1 - r_2(t)) r_3(t)]]$
8	0	0	0	0 0 0	$h_8(t) = [(1 - r_1(t)) [(1 - r_2(t)) [(1 - r_3(t))]]]$

*Примечание.* Принятые обозначения в столбцах ВК1...ВК3: 1 – работоспособное состояние видеокамеры; 0 – неработоспособное состояние видеокамеры.

Выражение вида  $[(1 - r_j(t))]$  в табл. 1.2 представляет собой вероятность неработоспособного состояния  $j$ -й видеокамеры за время  $t$  и показывает долю времени, в течение которой за время  $t$   $j$ -я видеокамера будет находиться в неработоспособном состоянии,  $j = 1, 2, 3$ .

В качестве коэффициентов эффективности ЭСБ, находящейся в  $i$ -м состоянии, будем рассматривать усреднённую вероятность идентификации объектов в выделенной зоне контроля. Перед тем как записать расчётные формулы, введём для коэффициентов эффективности состояний ЭСБ следующие обозначения:

- $\Phi_{123}$  – работоспособны все три видеокамеры;
- $\Phi_{12}$  – работоспособны первая и вторая видеокамеры;
- $\Phi_{13}$  – работоспособны первая и третья видеокамеры;
- $\Phi_{23}$  – работоспособны вторая и третья видеокамеры;
- $\Phi_1$  – работоспособна только первая видеокамера;
- $\Phi_2$  – работоспособна только вторая видеокамера;
- $\Phi_3$  – работоспособна только третья видеокамера.

С учётом принятых обозначений для определения коэффициентов эффективности, соответствующих условиям «день без осадков и тумана (д)», «ночь без осадков и тумана (н)», «осадки (о)», «туман (т)», могут быть предложены расчётные формулы.

Для условия «день без осадков и тумана (д)»:

$$\Phi_{123д} = \frac{S_{123}}{S} p_{123}^д + \frac{S_{12}}{S} p_{12}^д + \frac{S_{13}}{S} p_{13}^д + \frac{S_{23}}{S} p_{23}^д + \frac{S_1}{S} p_1^д + \frac{S_2}{S} p_2^д + \frac{S_3}{S} p_3^д, \quad (1.2)$$

где  $S_{123}$  – площадь зоны контроля (мониторинга), перекрываемая одновременно тремя видеокамерами;

$S_{12}, S_{13}, S_{23}$  – площади зоны контроля, перекрываемые одновременно первой и второй, первой и третьей, второй и третьей видеокамерами;

$S_1, S_2, S_3$  – площади зоны контроля, перекрываемые соответственно только первой, только второй и только третьей видеокамерами;

$S$  – общая площадь зоны контроля;

$p_{123}$  – вероятность идентификации объекта в зоне, перекрываемой сразу тремя видеокамерами;

$p_{12}, p_{13}, p_{23}$  – вероятности идентификации объекта в зоне, перекрываемой соответственно первой и второй, первой и третьей, второй и третьей видеокамерами;

$p_1, p_2, p_3$  – вероятности идентификации объекта в зоне, перекрываемой соответственно только первой, только второй и только третьей видеокамерами.

Применяя формулы теории вероятностей, для определения величины  $p_{123}$  может быть получено выражение

$$p_{123} = 1 - (1 - p_1) (1 - p_2) (1 - p_3), \quad (1.3)$$

а для определения вероятностей  $p_{12}, p_{13}$  и  $p_{23}$  – формулы

$$p_{12} = 1 - (1 - p_1) (1 - p_2),$$

$$p_{13} = 1 - (1 - p_1) (1 - p_3),$$

$$p_{23} = 1 - (1 - p_2) (1 - p_3).$$

Вероятности  $p_1$ ,  $p_2$  и  $p_3$  определяются техническими возможностями соответствующих видеокамер и в лабораторной работе рассматриваются как справочные данные.

Аналогично определению  $\Phi_{123д}$  могут быть определены коэффициенты эффективности, соответствующие другим условиям: «ночь без осадков и тумана (н)», «осадки (о)», «туман (т)»:

$$\Phi_{123н} = \frac{S_{123}}{S} p_{123}^н + \frac{S_{12}}{S} p_{12}^н + \frac{S_{13}}{S} p_{13}^н + \frac{S_{23}}{S} p_{23}^н + \frac{S_1}{S} p_1^н + \frac{S_2}{S} p_2^н + \frac{S_3}{S} p_3^н, \quad (1.4)$$

$$\Phi_{123о} = \frac{S_{123}}{S} p_{123}^о + \frac{S_{12}}{S} p_{12}^о + \frac{S_{13}}{S} p_{13}^о + \frac{S_{23}}{S} p_{23}^о + \frac{S_1}{S} p_1^о + \frac{S_2}{S} p_2^о + \frac{S_3}{S} p_3^о, \quad (1.5)$$

$$\Phi_{123т} = \frac{S_{123}}{S} p_{123}^т + \frac{S_{12}}{S} p_{12}^т + \frac{S_{13}}{S} p_{13}^т + \frac{S_{23}}{S} p_{23}^т + \frac{S_1}{S} p_1^т + \frac{S_2}{S} p_2^т + \frac{S_3}{S} p_3^т, \quad (1.6)$$

$$\Phi_{12д} = \frac{S_{12}}{S} p_{12}^д + \frac{S_1}{S} p_1^д + \frac{S_2}{S} p_2^д, \quad (1.7)$$

$$\Phi_{12н} = \frac{S_{12}}{S} p_{12}^н + \frac{S_1}{S} p_1^н + \frac{S_2}{S} p_2^н, \quad (1.8)$$

$$\Phi_{12о} = \frac{S_{12}}{S} p_{12}^о + \frac{S_1}{S} p_1^о + \frac{S_2}{S} p_2^о, \quad (1.9)$$

$$\Phi_{12т} = \frac{S_{12}}{S} p_{12}^т + \frac{S_1}{S} p_1^т + \frac{S_2}{S} p_2^т, \quad (1.10)$$

$$\Phi_{13д} = \frac{S_{13}}{S} p_{13}^д + \frac{S_1}{S} p_1^д + \frac{S_3}{S} p_3^д, \quad (1.11)$$

...

$$\Phi_{13т} = \frac{S_{13}}{S} p_{13}^т + \frac{S_1}{S} p_1^т + \frac{S_3}{S} p_3^т, \quad (1.12)$$

$$\Phi_{23д} = \frac{S_{23}}{S} p_{23}^д + \frac{S_2}{S} p_2^д + \frac{S_3}{S} p_3^д, \quad (1.13)$$

...

$$\Phi_{23\Gamma} = \frac{S_{23}}{S} p_{23}^{\Gamma} + \frac{S_2}{S} p_2^{\Gamma} + \frac{S_3}{S} p_3^{\Gamma}, \quad (1.14)$$

$$\Phi_{1д} = \frac{S_1}{S} p_1^д, \quad (1.15)$$

$$\Phi_{1н} = \frac{S_1}{S} p_1^н, \quad (1.16)$$

$$\Phi_{1о} = \frac{S_1}{S} p_1^о, \quad (1.17)$$

$$\Phi_{1\Gamma} = \frac{S_1}{S} p_1^{\Gamma}, \quad (1.18)$$

...

Поскольку ЭСБ должна осуществлять круглосуточное наблюдение (мониторинг) на перекрёстке, пешеходном переходе и вблизи его в любое время суток и при любых погодных условиях, то при формировании коэффициента эффективности необходимо усреднить его значение, приняв во внимание среднюю продолжительность функционирования ЭСБ в течение года в тех или иных погодных условиях (табл. 1.3).

Таблица 1.3

Средняя годовая продолжительность условий функционирования ЭСБ

Условия функционирования ЭСБ		Средняя годовая продолжительность, ч
1. Туман (т)		300
2. Осадки (о)		160
3. Без осадков и тумана	дневное время (д)	4200
	ночное время (н)	4100
Всего		8760

Тогда формула общего коэффициента эффективности, соответствующего состоянию 111 (см. табл. 1.2), запишется в виде

$$\Phi_{123\Sigma} = \frac{t_д}{t} \Phi_{123д} + \frac{t_н}{t} \Phi_{123н} + \frac{t_о}{t} \Phi_{123о} + \frac{t_{\Gamma}}{t} \Phi_{123\Gamma}, \quad (1.19)$$

состояния 110 – в виде

$$\Phi_{12\Sigma} = \frac{t_д}{t} \Phi_{12д} + \frac{t_н}{t} \Phi_{12н} + \frac{t_о}{t} \Phi_{12о} + \frac{t_{\Gamma}}{t} \Phi_{12\Gamma}. \quad (1.20)$$

Аналогично могут быть записаны формулы расчёта общего коэффициента эффективности, соответствующие остальным состоянием ЭСБ, указанным в табл. 1.2.

## 1.5. Задания на экспериментальную часть лабораторной работы

1. Ознакомиться с исследуемой ЭСБ и особенностью учебной программы для ЭВМ.

2. Запустить программу для ЭВМ (имя запускаемого файла **Cross.exe**), разобраться с кнопками на главном окне программы, виртуальными перекрёстком, видеокамерами и элементами управления ими.

3. Выбрать фокусные расстояния ( $F$ ) видеокамер и последовательно установить в отмеченных для этого местах три видеокамеры. При этом видеокамеры могут иметь разные фокусные расстояния. Используя виртуальные устройства поворота видеокамер в горизонтальной плоскости от  $-180$  до  $+180^\circ$  и изменение наклона по вертикали от  $0$  до  $90^\circ$ , следует попытаться обеспечить максимальное перекрытие выделенной (контролируемой) зоны перекрёстка тремя видеокамерами. При этом необходимо учитывать, что с уменьшением фокусного расстояния  $F$  уменьшается цена камеры и увеличивается площадь контроля, однако при этом способность идентификации падает.

4. После первой установки трёх камер нажать кнопку «Тест» и выполнить тестовое задание. Значение искомой вероятности определяется не менее чем до четырёх знаков после запятой. При правильном выполнении теста будет обеспечен доступ студента в проектный режим.

5. Получить первое проектное решение ЭСБ. Под проектным решением понимается совокупность трёх видеокамер с выбранными фокусными расстояниями, определёнными местами их установки, высотами установки, углами поворота в горизонтальной плоскости и углом наклона по вертикали. Заслуживают рассмотрению такие проектные решения, которые обеспечивают (с точки зрения студента) максимальную эффективность функционирования ЭСБ и, следовательно, высокую идентификацию объектов в выделенной зоне перекрёстка.

Рекомендуется в качестве первого проектного решения использовать то, для которого выполнялось тестовое задание. Нажатие кнопки «Добавить проект» отображает в таблице информацию о проекте. Указываются фокусные расстояния объектива видеокамер и параметры их установки. Приводится (в процентах) также перекрытие контролируемой зоны одновременно тремя видеокамерами, возможными сочетаниями из двух видеокамер и камерами по одиночке. В последних столбцах таблицы записываются эффективность ЭСБ и суммарная стоимость используемых видеокамер. Эффективность  $E$  представляет собой усреднённую для одного года вероятность правильной идентификации ситуации на перекрёстке.

6. Меняя при необходимости места установки видеокамер, а также используя элементы управления видеокамерами и варьируя параметры их установки, получить последовательно ещё девять проектов ЭСБ для последующего анализа их удачности в домашней обстановке.

7. Спланировать и выполнить исследования для получения ответа на следующий вопрос: как влияет на относительную эффективность функционирования ЭСБ фокусное расстояние объектива видеокамеры при фиксированном месте её установки (в предположении использования в составе ЭСБ лишь одной видеокамеры)?

Под относительной эффективностью функционирования ЭСБ, включающей  $i$ -е фокусное расстояние видеокамеры (обозначим эту эффективность через  $E_{\text{отн.}i}$ ), будем понимать величину, определяемую как

$$E_{\text{отн.}i} = \frac{E(t, F_i)}{E(t, F)_{\text{max}}}, \quad (1.21)$$

где  $E(t, F_i)$  – эффективность функционирования ЭСБ в течение времени  $t$ , соответствующая  $i$ -му фокусному расстоянию видеокамеры;

$E(t, F)_{\text{max}}$  – максимальная эффективность функционирования ЭСБ в течение времени  $t$ , соответствующая одному из фокусных расстояний из числа рассматриваемых в учебной программе для ЭВМ.

*Примечание.* Учебная программа для ЭВМ функционирует, если в состав ЭСБ включено три видеокамеры. Для исследования влияния на эффективность функционирования ЭСБ лишь одной камеры рекомендуется две видеокамеры из трёх установить так, чтобы угол их обзора не захватывал выделенную зону контроля на перекрёстке. В этом случае вклад в эффективность функционирования ЭСБ будет вносить лишь третья видеокамера. При этом горизонтальный поворот и угол наклона третьей видеокамеры следует выбирать так, чтобы обеспечивалось большее перекрытие зоны контроля и, следовательно, наибольшее значение показателя эффективности функционирования ЭСБ при рассматриваемом ( $i$ -м) фокусном расстоянии этой видеокамеры.

8. В строке «Меню» главного окна программы для ЭВМ выбрать «Настройки», после чего будет обеспечен доступ к параметрам видеокамер. Далее получить данные о зависимости стоимости видеокамеры от фокусного расстояния её объектива.

## 1.6. Содержание отчёта

1. Цель лабораторной работы.
2. Описание показателя эффективности функционирования ЭСБ и пояснение его смысла.
3. Таблица с информацией о десяти проектных решениях ЭСБ, анализом успешности решений, указанием выбора лучшего решения и его аргументацией.
4. График зависимости эффективности функционирования ЭСБ от фокусного расстояния  $F$  видеокамеры.
5. График зависимости стоимости видеокамеры от фокусного расстояния её объектива.
6. Выводы по работе с обязательным объяснением вида графика зависимости относительной эффективности функционирования ЭСБ от фокусного расстояния объектива видеокамеры при фиксированном месте её установки.

## 1.7. Контрольные вопросы

1. Что в общем случае понимают под показателем эффективности функционирования ЭСБ?
2. Какие факторы принимают во внимание при построении показателя эффективности функционирования ЭСБ, включающей видеокамеры?
3. Чем объясняется переход ЭСБ из одного технического состояния в другое?
4. Объясните смысл коэффициента эффективности  $i$ -го состояния ЭСБ.
5. Какие факторы оказывают влияние на коэффициент эффективности  $i$ -го состояния ЭСБ?
6. Как влияет фокусное расстояние объективов видеокамер на вероятность идентификации объектов?
7. Объясните полученный в лабораторной работе график влияния фокусного расстояния объектива видеокамеры на относительную эффективность функционирования ЭСБ.
8. Предложите относительно простые, но эффективные пути повышения показателя эффективности функционирования ЭСБ, рассматриваемой в лабораторной работе.

### Литература

1. Надёжность технических систем : справочник / Ю. К. Беляев [и др.]; под ред. И. А. Ушакова. – М. : Радио и связь, 1985. – 608 с.
2. Надёжность в технике. Основные понятия. Термины и определения. ГОСТ 27.002–89. – Введ. 1990–07–01. – М. : Изд-во стандартов, 1990. – 38 с.

## ЛАБОРАТОРНАЯ РАБОТА №2 ОЦЕНКА УЯЗВИМОСТИ ЭСБ МЕТОДОМ АНАЛИЗА ПУТЕЙ ПРОНИКНОВЕНИЯ К ОХРАНЯЕМЫМ РЕСУРСАМ

### 2.1. Цель работы

Оценить (спрогнозировать) уязвимость ЭСБ методом рассмотрения возможных путей проникновения к охраняемым ресурсам и применения технических средств для обеспечения защиты (исследования проводятся на примере ЭСБ, обеспечивающей безопасность небольшого банковского учреждения).

### 2.2. Теоретические сведения

Под уязвимостью ЭСБ будем понимать степень её слабости с точки зрения выполнения предписанных функций, в качестве которых обычно рассматривается обеспечение защиты объекта или охраняемых ресурсов [1–3]. Удобно в качестве количественной характеристики описания уязвимости (обозначим её как  $U$ ) использовать вероятность незащиты объекта и охраняемых ресурсов (далее просто охраняемых ресурсов), т. е.

$$U = P(\bar{Z}), \quad (2.1)$$

где  $\bar{Z}$  – событие, состоящее в незащите охраняемых ресурсов; является событием, противоположным событию  $Z$ , состоящему в обеспечении защиты охраняемых ресурсов;

$P$  – символ, используемый здесь и далее для обозначения соответствующих вероятностей.

Очевидным, как известно из теории вероятностей [4], является выражение

$$P(Z) + P(\bar{Z}) = 1, \quad (2.2)$$

где  $P(Z)$  – вероятность обеспечения защиты охраняемых ресурсов.

Во многих случаях в качестве показателя эффективности функционирования ЭСБ (обозначим через  $E$ ) используют вероятность обеспечения защиты охраняемых ресурсов  $P(Z)$ , т. е.

$$E = P(Z). \quad (2.3)$$

Для таких случаев с учётом выражений (2.1)–(2.3) для уязвимости  $U$  справедливо равенство

$$U = 1 - E = 1 - P(Z). \quad (2.4)$$

Уязвимость  $U$  может быть оценена (спрогнозирована) по формуле полной вероятности [4]:

$$U = P(\bar{Z}) = \sum_{j=1}^m P(H_j)P(\bar{Z}|H_j), \quad (2.5)$$

где  $j$  – конкретный возможный путь проникновения к охраняемым ресурсам;

$m$  – число возможных путей проникновения к охраняемым ресурсам;

$P(H_j)$  – вероятность того, что злоумышленником (нарушителем) для проникновения к охраняемым ресурсам будет выбран  $j$ -й путь;

$H_j$  – событие, состоящее в выборе злоумышленником  $j$ -го пути;

$P(\bar{Z}|H_j)$  – вероятность незащиты охраняемых ресурсов при условии, что злоумышленник выберет для проникновения  $j$ -й путь.

Подчеркнём, что события  $H_1, H_2, \dots, H_m$  представляют собой полную группу несовместных событий, т. е. предполагается, что какой-либо путь проникновения злоумышленником будет выбран обязательно, при этом два и более пути не могут быть выбраны одновременно. Следовательно, должно выполняться условие

$$P(H_1) + P(H_2) + \dots + P(H_m) = 1. \quad (2.6)$$

Вероятности событий  $H_1, H_2, \dots, H_m$ , т. е. вероятности вида  $P(H_j)$  ( $j = 1, 2, \dots, m$ ), оцениваются на основе анализа возможных путей проникновения к охраняемым ресурсам. Хорошие результаты в этих случаях даёт прогнозирование с использованием метода опроса экспертов. Такое прогнозирование является разновидностью эвристического прогнозирования [5].

Для получения эвристического прогноза формируется группа специалистов-экспертов в количестве  $n$  человек из числа разработчиков ЭСБ и её составных частей, специалистов предприятий – изготовителей компонентов ЭСБ, специалистов по безопасности и надёжности, сотрудников силовых структур, лиц, эксплуатирующих ЭСБ в составе охранных комплексов, и т. д. Сформированной группе экспертов предлагается дать количественную оценку привлекательности (обозначим через  $W$ ) для злоумышленников того или иного возможного пути проникновения к охраняемым ресурсам на основе имеющейся количественной и качественной информации об объекте и охраняемых ресурсах. Причём оценка должна быть дана каждым экспертом независимо от других экспертов, например в процентах от 0 до 100. Оценка в 100 % соответствует максимальной привлекательности для злоумышленника возможного пути, а оценка 0 % – случаю, когда теоретически возможный путь проникновения никогда не будет выбран злоумышленником для проникновения к охраняемым ресурсам. Оценки в процентах привлекательности путей проникновения могут даваться, не принимая во внимание условие (2.6). Условие (2.6) обеспечивается «автоматически» на этапе расчёта вероятностей, соответствующих тому или иному пути проникновения.

Имея прогнозные оценки, сделанные разными экспертами, далее получают результирующую прогнозную оценку привлекательности для злоумышленника  $j$ -го пути  $W_{\text{пр}}^{(j)}$ . В простейшем случае она может быть получена путём усреднения оценок, сделанных разными экспертами:

$$W_{\text{пр}}^{(j)} = \frac{\sum_{i=1}^n W_i^{(j)}}{n}, \quad (2.7)$$

где  $W_i^{(j)}$  – количественная оценка характеристики  $W^{(j)}$ , сделанная  $i$ -м экспертом;  
 $n$  – количество экспертов.

Для определения вероятностей  $P(H_1), P(H_2), \dots, P(H_m)$  по значениям привлекательностей  $W_{\text{пр}}^{(j)}$  ( $j = 1, 2, \dots, m$ ), исходя из обеспечения условия (2.6), может быть использовано выражение

$$P(H_j) = \frac{W_{\text{пр}}^{(j)}}{\sum_{j=1}^m W_{\text{пр}}^{(j)}}, \quad j = 1, 2, \dots, m. \quad (2.8)$$

В формулу (2.8) прогнозные значения привлекательностей  $W_{\text{пр}}^{(j)}$  должны подставляться в процентах ( $j = 1, 2, \dots, m$ ).

Вероятности вида  $P(\bar{Z}|H_j)$  зависят от характеристик и возможностей технических устройств ЭСБ: датчиков, исполнительных устройств и др. Принимая во внимание только возможности датчиков, вероятности  $P(\bar{Z}|H_j)$  можно определить как

$$P(\bar{Z}|H_j) = (1 - p_1)(1 - p_2)\dots(1 - p_l) = \prod_{i=1}^L (1 - p_i), \quad (2.9)$$

где  $p_i$  – вероятность восприятия сигнала о проникновении злоумышленника  $i$ -м датчиком, установленным на  $j$ -м возможном пути проникновения;

$L$  – количество датчиков, установленных на  $j$ -м возможном пути проникновения злоумышленника к охраняемым ресурсам.

Отметим, что величины  $(1 - p_1), (1 - p_2)$  и  $(1 - p_l)$  представляют собой соответственно вероятности невосприятия 1-м, 2-м и  $l$ -м датчиком сигнала о проникновении злоумышленника к охраняемым ресурсам.

Для учёта влияния вероятностей восприятия и/или правильной обработки сигналов о попытке проникновения злоумышленника (вероятностей вида  $p_i$ ) другими устройствами ЭСБ необходимо формулу (2.9) дополнить сомножителями вида  $(1 - p_i)$ , учитывающими «исполнительную» эффективность других устройств, обеспечивающих защиту охраняемых ресурсов в случае выбора злоумышленником  $j$ -го возможного пути проникновения.

### 2.3. Описание и анализ исследуемой ЭСБ

Исследуемая ЭСБ предназначена для защиты охраняемых ресурсов в большом банковском учреждении. Здание учреждения имеет шесть помещений, две наружные двери и три окна. Комната номер 2 представляет собой кассовый зал, включающий четыре кассы, каждая из которых обозначена номером 7 и является частью комнаты номер 2. Каждая касса имеет внутреннюю дверь для входа в служебное помещение – комнату номер 3. Охраняемые финансовые ресурсы размещены в комнате номер 4.

Допущения, принимаемые при выполнении лабораторной работы:

1) в качестве показателя уязвимости ЭСБ рассматривается вероятность незащиты охраняемых ресурсов, размещённых в комнате номер 4;

2) уязвимость ЭСБ определяется в предположении, что злоумышленник (нарушитель) является квалифицированным;

3) возможность разрушения злоумышленником капитальной стены считается пренебрежимо малой и в лабораторной работе не принимается во внимание;

4) все составные части ЭСБ с точки зрения работоспособности считаются идеальными, т. е. вероятность их работоспособного состояния в произвольный момент времени принимается равной единице. Незащита охраняемых ресурсов возникает только из-за не 100-процентного восприятия датчиками сигналов о проникновении, не 100-процентно правильной передачи сигналов по выбранным каналам связи и их обработки в микропроцессорном (МП) приёмно-контрольном устройстве, а также не 100-процентной эффективности исполнительных устройств.

### 2.4. Особенности учебной программы для ЭВМ

Особенностью программы для ЭВМ является наличие возможности устанавливать пользователем (студентом) датчики в нужные места стен, окон и дверей. Для выполнения этого реализована функция получения проекций элементов комнат (стен, окон, дверей), выбора типа датчика и его установки в любом месте по усмотрению студента. Для более эффективного выполнения этой части лабораторной работы предусмотрена инструкция, вызов которой выполняется во вкладке «Установка датчиков». В этой же вкладке имеется справка по датчикам, позволяющая ознакомиться с изображениями (фотографиями) датчиков, их эксплуатационно-техническими характеристиками, в частности вероятностью правильного восприятия сигналов об угрозах и стоимостью. Во вкладке «База» можно ознакомиться с «исполнительной» эффективностью как датчиков, так и других устройств, входящих в состав ЭСБ.

В программе также имеется возможность записи информации о проектном решении в документы Microsoft Excel. Проектное решение представляет собой информацию о типах, количестве и эффективности датчиков, видах используемых исполнительных устройств, характере используемых каналов связи, значении показателя уязвимости ЭСБ, стоимости устройств и некоторые другие сведения.

## 2.5. Задания на экспериментальную часть лабораторной работы

1. Ознакомиться с общей структурной схемой ЭСБ.

2. Выполнить синтез проектного решения электронной системы безопасности, предназначенной для защиты финансовых ресурсов банковского учреждения, для чего:

а) ознакомиться с возможными путями проникновения нарушителя к охраняемым ресурсам;

б) с помощью метода экспертного опроса специалистов зафиксировать для каждого  $i$ -го эксперта прогнозные значения привлекательности для злоумышленника  $j$ -го пути  $W_i^{(j)}$ , а затем, используя выражение (2.7), определить результирующую прогнозную оценку привлекательности  $j$ -го пути  $W_{пр}^{(j)}$ ; в качестве экспертов рассматриваются студенты бригады, выполняющей лабораторную работу;

в) по формуле (2.8), включённой в алгоритм работы программы для ЭВМ, рассчитать вероятности того, что злоумышленником (нарушителем) для проникновения к охраняемым ресурсам будет выбран  $j$ -й путь; эти вероятности в описании лабораторной работы выше были обозначены как  $P(H_1), P(H_2), \dots, P(H_m)$ , а во вкладке «Пути проникновения» программы для ЭВМ также как  $P_j$ ;

г) ознакомиться с базой данных о датчиках и выбрать типы датчиков, позволяющие с учётом указанных возможных путей проникновения эффективно фиксировать попытки движения злоумышленников к охраняемым ресурсам;

д) установить выбранные типы датчиков в комнатах, на дверях или окнах в таких местах, которые обеспечивают с точки зрения студента максимальную эффективность обнаружения злоумышленников, т. е. дают максимальную вероятность восприятия датчиками сигналов о проникновении злоумышленников к охраняемым ресурсам; при установке датчиков следует пользоваться указаниями программы для ЭВМ;

е) выбрать каналы связи между датчиками и МП приёмно-контрольным устройством, между МП приёмно-контрольным устройством и исполнительным блоком; выбор каналов связи должен быть сделан так, чтобы обеспечивалась достаточная уверенность (вероятность) правильной передачи сигналов от одних устройств ЭСБ к другим;

ж) выбрать одно или несколько исполнительных устройств, предназначенных для ликвидации попыток проникновения злоумышленников к охраняемым ресурсам.

3. Оценить уязвимость спроектированной ЭСБ.

*Примечания:* 1. Чем не удачнее будут установлены датчики, тем ниже значения вероятностей восприятия ими сигнала о проникновении злоумышленника и тем выше окажется уязвимость ЭСБ.

2. Совместно с оценкой уязвимости проектируемой ЭСБ программой для ЭВМ оценивается суммарная стоимость технических устройств, включаемых в состав ЭСБ (в проектное решение).

4. Выполнить анализ количественного показателя уязвимости ЭСБ и уточнить суммарную стоимость технических устройств, включаемых в состав проектного решения ЭСБ.

5. Принимая во внимания эффективность функционирования датчиков, каналов связи и исполнительных устройств, попытаться получить проектное решение ЭСБ, обеспечивающее меньшее значение показателя уязвимости. При этом необходимо учитывать экономические затраты, обусловленные техническими устройствами, включаемыми в состав проектного решения ЭСБ. Рекомендуется получить не менее десяти проектных решений.

6. Используя инструмент «Корреляция» пакета анализа Microsoft Excel, определить выборочный коэффициент корреляции между показателем уязвимости ЭСБ и суммарной стоимостью технических устройств, включаемых в состав ЭСБ.

7. Проверить статистическую значимость полученного выше коэффициента корреляции, пользуясь преобразованием Фишера (прил. 1 и 2) . Значение доверительной вероятности принять  $\gamma = 0,95$  [5].

Этот пункт задания может выполняться во вне учебных занятий.

## 2.6. Содержание отчёта

1. Формулировка цели лабораторной работы.

2. Схема банковского учреждения с указанием возможных путей проникновения злоумышленника к охраняемым ресурсам.

3. Таблица с указанием (по результатам экспертного опроса) результирующих прогнозных оценок привлекательности  $j$ -го пути  $W_{пр}^{(j)}$  и вероятностей того, что злоумышленником (нарушителем) для проникновения к охраняемым ресурсам будет выбран  $j$ -й путь,  $j = 1, 2, \dots, 5$ .

4. Таблица с описанием десяти проектных решений, соответствующим им показателями уязвимости и суммарной стоимости технических устройств, включаемых в состав ЭСБ. Описание проектного решения ЭСБ должно содержать данные о типах и количестве датчиков, устанавливаемых в каждой из комнат учреждения банка, используемых исполнительных устройствах и каналах связи.

5. Значение выборочного коэффициента корреляции между показателем уязвимости ЭСБ и суммарной стоимостью технических устройств, включаемых в состав ЭСБ, результаты проверки статистической значимости полученного коэффициента корреляции в виде нижней и верхней границ для преобразования Фишера  $F$  и коэффициента корреляции.

6. Аргументированное заключение о лучшем варианте ЭСБ из числа проектных решений, полученных студентом при выполнении экспериментальной части лабораторной работы.

7. Выводы по работе.

## 2.7. Контрольные вопросы

1. Что понимают под уязвимостью ЭСБ?
2. Как связаны между собой уязвимость и показатель эффективности функционирования ЭСБ?
3. Как на практике можно оценить (спрогнозировать) вероятности выбора злоумышленником того или иного пути проникновения к охраняемым ресурсам?
4. Как сказывается выбор типов датчиков и мест их установки на уязвимости ЭСБ? Ответ подготовить на основе анализа проектных решений ЭСБ, полученных в лабораторной работе.
5. Какая зависимость имеет место между показателем уязвимости ЭСБ и суммарной стоимостью технических устройств, включаемых в состав ЭСБ? Объяснить причины зависимости.
6. Сформулируйте основные рекомендации по снижению уязвимости ЭСБ, рассматриваемой в лабораторной работе.
7. Какими дополнительно показателями руководствуются при выборе варианта проектного решения ЭСБ, лучшего с точки зрения меньшей уязвимости?

### Литература

1. Барсуков, В. С. Современные технологии безопасности / В. С. Барсуков, В. В. Водолазкий. – М. : Нолидж, 2000. – 496 с.
2. Барсуков, В. С. Безопасность : технологии, средства, услуги / В. С. Барсуков. – М. : КУДИЦ – ОБРАЗ, 2001 – 496 с.
3. Ярочкин, В. И. Информационная безопасность : учебник для студ. вузов / В. И. Ярочкин. – 3-е изд. – М. : Академический проект : Трикта, 2005. – 544 с.
4. Вентцель, Е. С. Теория вероятностей : учебник / Е. С. Вентцель. – 9-е изд., стер. – М. : Академия, 2003. – 576 с.
5. Боровиков, С. М. Теоретические основы конструирования, технологии и надёжности : учебник для инж.-техн. спец. вузов / С. М. Боровиков. – Минск : Дизайн ПРО, 1998. – 336 с.

# ЛАБОРАТОРНАЯ РАБОТА №3

## ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЭСБ С УЧЁТОМ ЛОЖНЫХ ТРЕВОГ

### 3.1. Цель работы

На примере ЭСБ, обеспечивающей безопасность специального объекта (небольшого аэродрома и его инфраструктуры), исследовать влияние на эффективность функционирования ЭСБ возможных ложных срабатываний датчиков.

### 3.2. Теоретические сведения

Известно, что одной из важнейших характеристик датчиков является чувствительность. При высокой чувствительности датчик хорошо реагирует на возможные отклонения среды объекта от нормы, тем самым обеспечивает высокую вероятность восприятия сигналов об угрозах: нарушении периметра территории или проникновение в помещения зданий. Однако с повышением чувствительности возрастает интенсивность ложных срабатываний (ложных тревог). Типичная гипотетическая зависимость интенсивности ложных тревог ( $\lambda$ ) от вероятности правильного восприятия (детектирования) сигналов об угрозах ( $p$ ) представлена на рис. 3.1.

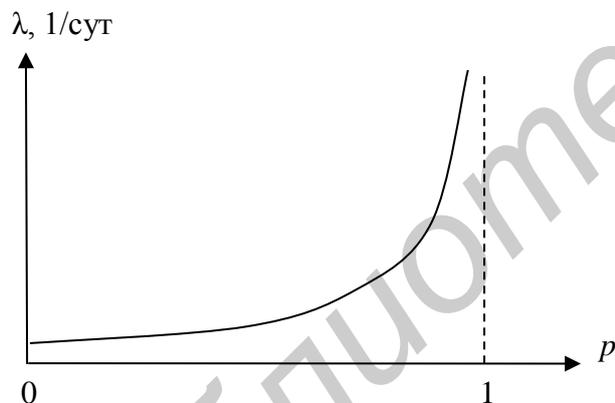


Рис. 3.1. Гипотетическая зависимость интенсивности ложных тревог от вероятности правильного детектирования сигналов об угрозах

По данным экспертного опроса специалистов сибирского региона России для внешней охраны нормальным считается интенсивность ложных тревог не более 0,3 1/сут, а по нормам проектирования – не более 3,0 1/сут. По данным иностранной печати средним считается интенсивность ложных тревог примерно 0,006...0,008 1/сут.

Ложные тревоги раздражают охрану объектов и в конечном итоге могут привести к тому, что технические средства защиты охраной будут отключены, что сделает объект незащищённым. Поэтому важно обеспечить высокий уровень защищённости объекта при приемлемом уровне ложных тревог.

В лабораторной работе уровень защищённости объекта будем описывать таким критерием, как показатель эффективности функционирования ЭСБ ( $E$ ), а уровень ложных срабатываний датчиков – интенсивностью ложных тревог ( $\lambda$ ).

В первом приближении поток ложных тревог датчика может рассматриваться как простейший или стационарный пуассоновский поток [1]. Название «пуассоновский» связано с тем, что для таких потоков число ложных тревог, по-

павших на любой фиксированный интервал времени  $\tau$ , распределено по закону Пуассона для дискретных случайных величин. Согласно этому закону вероятность того, что за какое-то время  $\tau$  возникнет  $m$  ложных тревог (рис. 3.2), равна

$$P_m(\tau) = \frac{(\lambda\tau)^m}{m!} \exp(-\lambda\tau), \quad (3.1)$$

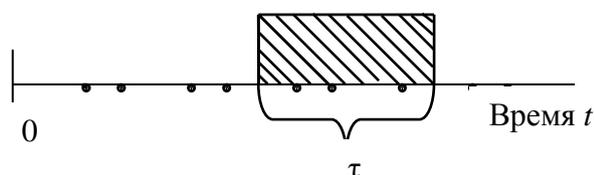


Рис. 3.2. К пояснению распределения Пуассона

где  $\lambda$  – плотность потока ложных тревог (среднее число ложных тревог, приходящихся на единицу времени).

Для краткости простейшие стационарные пуассоновские потоки часто называют простейшими потоками. Такой поток должен отвечать трём следующим условиям [1, 2]:

1) стационарности – количественные характеристики потока не зависят от рассматриваемого временного участка. В качестве этой характеристики можно использовать плотность возникновения ложной тревоги, представляющую собой среднее количество ложных тревог, приходящихся на единицу времени;

2) ординарности – ложные тревоги происходят по одиночке, а не парами, тройками и т. д.;

3) отсутствия последействия – время возникновения очередной ложной тревоги не зависит от времени наступления предыдущей ложной тревоги.

Следуя положениям теории вероятностей, можно принять, что для простейшего потока время  $t$  между возникновением двух ложных тревог распределено по экспоненциальному закону (рис. 3.3). Плотность распределения времени  $t$  в этом случае задается выражением

$$w(t) = \lambda \exp(-\lambda t), \quad t \geq 0, \quad (3.2)$$

где  $\lambda$  – плотность потока ложных тревог, совпадающая при экспоненциальном распределении с интенсивностью возникновения ложных тревог (поэтому плотность потока обозначена той же буквой, что и интенсивность ложных тревог).

С учётом выражения (3.2) наработка на ложную тревогу определяется по формуле

$$T_{\text{лт}} = \frac{1}{\lambda}, \quad (3.3)$$

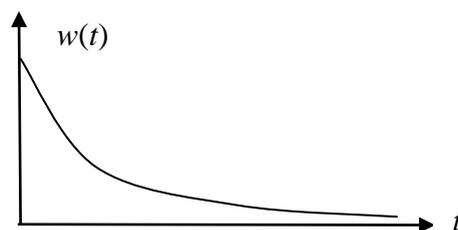


Рис. 3.3. Экспоненциальное распределение времени возникновения ложных тревог

а вероятность возникновения ложной тревоги за интересующее время  $t$  может быть найдена как

$$P_{лт}(t) = 1 - \exp(-\lambda t). \quad (3.4)$$

При наличии в ЭСБ нескольких датчиков суммарная интенсивность возникновения ложной тревоги  $\Lambda_{\Sigma}$  совокупности датчиков в случае независимой их работы определяется суммированием интенсивностей ложных тревог рассматриваемых датчиков:

$$\Lambda_{\Sigma} = \lambda_1 + \lambda_2 + \dots + \lambda_n, \quad (3.5)$$

где  $n$  – количество датчиков в ЭСБ;

$\lambda_i$  – интенсивность ложной тревоги  $i$ -го датчика,  $i = 1, 2, \dots, n$ .

Наработка на ложную тревогу ЭСБ в целом определяется как

$$T_{лт.ЭСБ} = \frac{1}{\Lambda_{\Sigma}}. \quad (3.6)$$

По отечественным (страны СНГ) и зарубежным данным в настоящее время приемлемым считается наработка на ложную тревогу, составляющая примерно 700...2000 ч [3, 4]. В предположении экспоненциального закона распределения наработки на ложную тревогу это соответствует интенсивности ложных тревог примерно равной 0,012...0,033 1/сут.

### 3.3. Описание и анализ исследуемой ЭСБ

Исследуемая ЭСБ предназначена для обеспечения безопасности небольшого аэродрома совместно с его инфраструктурой. ЭСБ является трёхрубежной. Рубежи защиты:

– *внешнее ограждение* является первым рубежом защиты; здесь используются заградительные средства обнаружения (СО);

– *второй рубеж защиты* расположен на незначительном расстоянии (5...10 м) от первого рубежа; здесь использованы маскирующие СО; вероятность обнаружения нарушителя этими СО выше, нежели заградительными СО;

– *третий рубеж защиты* – это СО, установленные непосредственно на охраняемых ангарах, в которых размещена военная техника (самолёты).

Каждому из указанных рубежей защиты соответствуют свои СО, которые собирательно названы как система датчиков конкретного рубежа:  $D1$ ,  $D2$  и  $D3$ .

При выполнении исследований имеется возможность выбирать как количество рубежей защиты (один, два и три), так и их сочетание в случае двух рубежей защиты.

Допущения, принимаемые при выполнении лабораторной работы:

1) в качестве эффективности функционирования ЭСБ в целом рассматривается эффективность, определяемая только системами датчиков  $D1, D2, D3$ ;

2) эффективность функционирования ЭСБ определяется в предположении, что злоумышленник (нарушитель) является квалифицированным;

3) исследуемая ЭСБ рассматривается как система, выполняющая задачу в течение времени  $t$ , начиная с некоторого момента времени;

4) все составные части ЭСБ, кроме систем датчиков  $D1, D2$  и  $D3$ , с точки зрения работоспособности являются идеальными, т. е. вероятности их работоспособного состояния в течение рассматриваемого времени функционирования ЭСБ [5] равны единице;

5) оператор (охрана) всегда воспринимает сигналы об угрозах при их поступлении от систем датчиков и во всех случаях устраняет эти угрозы.

При наличии указанных допущений возможные состояния ЭСБ определяются работоспособностью или неработоспособностью только систем датчиков  $D1, D2$  и  $D3$  (табл. 3.1).

Таблица 3.1

Возможные технические состояния рассматриваемой ЭСБ

Номер технического состояния ЭСБ, $i$	Описание технического состояния ЭСБ (состояние работоспособности систем датчиков)			Условное обозначение состояния	Формула определения вероятности технического состояния ЭСБ в целом $h_i(t)$
	$D1$	$D2$	$D3$		
1	1	1	1	111	$h_1(t) = r_1(t) r_2(t) r_3(t)$
2	1	1	0	110	$h_2(t) = r_1(t) r_2(t) [(1 - r_3(t))]$
3	1	0	1	101	$h_3(t) = r_1(t) [(1 - r_2(t))] r_3(t)$
4	1	0	0	100	$h_4(t) = r_1(t) [(1 - r_2(t))] [(1 - r_3(t))]$
5	0	1	1	011	$h_5(t) = [(1 - r_1(t))] r_2(t) r_3(t)$
6	0	1	0	010	$h_6(t) = [(1 - r_1(t))] r_2(t) [(1 - r_3(t))]$
7	0	0	1	001	$h_7(t) = [(1 - r_1(t))] [(1 - r_2(t))] r_3(t)$
8	0	0	0	000	$h_8(t) = [(1 - r_1(t))] [(1 - r_2(t))] [(1 - r_3(t))]$

*Примечания:* 1. Обозначения, принятые в таблице:  $D1, D2, D3$  – номера систем датчиков; 1 – работоспособное состояние; 0 – неработоспособное состояние;  $r_j(t)$  – вероятность работоспособного состояния в течение рассматриваемого времени  $t$   $j$ -й системы датчиков ( $j = 1, 2, 3$ ).

2. Выражения вида  $[(1 - r_j(t))]$  представляют собой вероятности неработоспособного состояния за время  $t$  для  $j$ -й системы датчиков ( $j = 1, 2, 3$ ).

С учётом принятых допущений коэффициент эффективности  $\Phi_i$   $i$ -го состояния ЭСБ определится как

$$\Phi_i = 1 - (1 - p_1) (1 - p_2) (1 - p_3), \quad (3.7)$$

где  $p_1, p_2, p_3$  – вероятность правильного восприятия сигнала об угрозе системой датчиков  $D1, D2$  и  $D3$ .

Если ЭСБ включает менее трёх рубежей защиты, то соответствующий сомножитель вида  $(1 - p_j)$  в формуле (3.7) удаляется, где  $j$  означает номер системы датчиков.

Для подсчёта коэффициента эффективности  $\Phi_i$ , соответствующего  $i$ -му состоянию ЭСБ, используется формула (3.7), в которую необходимо подставлять  $p_j$ , соответствующее вероятности правильного определения угрозы, если  $j$ -я система датчиков работоспособна, и  $p_j = 0$ , если  $j$ -я система датчиков будет неработоспособна ( $j = 1, 2, 3$ ).

Показатель эффективности функционирования ЭСБ в целом, соответствующий времени  $t$ , в лабораторной работе определяется как

$$E(t) = \sum_i h_i(t) \Phi_i, \quad (3.8)$$

где  $h_i(t)$  – вероятность того, что ЭСБ в течение времени  $t$  будет находиться в  $i$ -м состоянии.

### 3.4. Особенности учебной программы для ЭВМ

Особенностью программы для ЭВМ является использование графиков зависимости интенсивности ложных тревог от вероятности правильного определения угрозы, т. е. вероятности правильного детектирования. Эта вероятность зависит от чувствительности датчиков. Изменяя чувствительность, можно в определённых пределах изменять вероятность правильного детектирования, и как следствие будет изменяться интенсивность ложных тревог. В программе для ЭВМ для выбора требуемой вероятности правильного детектирования следует левой клавишей мыши щёлкнуть в любой точке горизонтальной оси, соответствующей заданной вероятности правильного детектирования (лучше всего в точках, расположенных непосредственно на графике зависимости интенсивности ложных тревог от вероятности правильного детектирования).

Второй особенностью программы для ЭВМ является наличие тестовых заданий. При вводе в ЭВМ результата выполнения тестового задания следует принять во внимание количество знаков после десятичной запятой, указываемое программой для ЭВМ. При этом следует применять общепринятые правила округления чисел.

### 3.5. Задания на экспериментальную часть лабораторной работы

1. Ознакомиться со структурой программы для ЭВМ и опциями, указанными в строке «Меню».

2. Используя программу, ознакомиться с объектом защиты, назначением ЭСБ и её составными виртуальными частями (рубежами защиты и используемыми системами датчиков  $D1$ ,  $D2$  и  $D3$ ).

**3.** Выяснить и осмыслить суть показателя эффективности функционирования ЭСБ в целом.

**4.** Используя программу для ЭВМ, получить данные для построения графика зависимости эффективности функционирования ЭСБ от вероятности ложного срабатывания в предположении, что ЭСБ имеет один рубеж защиты.

*Рекомендации:*

а) временной интервал, для которого определяется эффективность функционирования ЭСБ и вероятность возникновения ложных срабатываний, по умолчанию принимается равным 30 суткам, если преподавателем не указано другое значение;

б) задание 4 последовательно выполнить для каждого из трёх рубежей защиты;

в) проектные решения здесь и далее следует записывать в Microsoft Excel с целью дальнейшего их анализа; одно проектное решение позволяет получить одну точку для построения графика;

г) число точек для построения графика следует брать равным 5...7;

д) программа предоставляет возможность получения столбиковых диаграмм для показателя эффективности функционирования ЭСБ и вероятности ложного срабатывания по всем проектным решениям, следует воспользоваться этой возможностью.

**5.** С помощью программы для ЭВМ получить данные для построения графика зависимости эффективности функционирования ЭСБ от вероятности ложного срабатывания для вариантов, когда ЭСБ имеет два рубежа защиты.

Это задание последовательно выполнить для всех возможных сочетаний рубежей защиты.

**6.** С помощью программы для ЭВМ получить данные для построения графика зависимости показателя эффективности функционирования ЭСБ от вероятности ложного срабатывания для случая, когда ЭСБ имеет три рубежа защиты.

**7.** Выполнить анализ полученных проектных решений ЭСБ и принять решение о выборе рабочего проекта с учётом требований к допустимой вероятности ложного срабатывания, заданных преподавателем.

*Примечания:* 1. При выполнении заданий 4...6 следует руководствоваться интуитивно понятными указаниями, выдаваемыми программой для ЭВМ.

2. С целью осмысливания математических подходов, используемых для анализа ложных тревог, студенту при выполнении каждого из вариантов, определяющих состав ЭСБ, предлагается дать ответ на несложные тестовые задания. Результат должен быть подсчитан до четвертого знака после запятой, если ЭВМ не указывает иные требования.

### **3.6. Содержание отчёта**

1. Формулировка цели лабораторной работы.

2. Описание состава исследуемых ЭСБ (в зависимости от выполняемого варианта) и результаты проектных решений в виде таблицы и столбиковых диаграмм (данные приводятся по всем выполняемым вариантам).

3. Графики зависимости показателя эффективности функционирования ЭСБ от вероятности ложного срабатывания (приводятся для всех выполненных вариантов).

4. Аргументированное заключение о рекомендуемом рабочем проекте ЭСБ.

5. Выводы по работе.

### 3.7. Контрольные вопросы

1. Чем объясняется негативное действие ложных тревог?

2. Как гипотетически интенсивность ложных тревог связана с чувствительностью датчиков?

3. Нарисуйте типичную зависимость интенсивности ложных тревог от вероятности правильного детектирования сигналов об угрозах.

4. Как с помощью математических методов могут быть описаны ложные тревоги ЭСБ?

5. Какую характеристику ложных тревог можно рассчитать с помощью закона Пуассона для дискретных величин?

6. Что понимают под наработкой ЭСБ на ложную тревогу?

7. Как рассчитать наработку датчика на ложную тревогу?

8. Укажите уровень интенсивности ложных тревог или наработки на ложную тревогу, считаемые приемлемыми для современных ЭСБ.

9. Обоснуйте заключение о рекомендуемом рабочем проекте ЭСБ из числа проектов, рассматриваемых в лабораторной работе.

10. Предложите пути (методы) снижения уровня ложных тревог для проектов ЭСБ, рассматриваемых в лабораторной работе.

### Литература

1. Боровиков, С. М. Теоретические основы конструирования, технологии и надёжности : учебник для инж.-техн. спец. вузов / С. М. Боровиков. – Минск : Дизайн ПРО, 1998. – 336 с.

2. Вентцель, Е. С. Теория вероятностей : учебник / Е. С. Вентцель. – 9-е изд., стер. – М. : Академия, 2003. – 576 с.

3. Магауенов, Р. Г. Системы охранной сигнализации : основы теории и принципы построения / Р. Г. Магауенов. – М. : Горячая линия – Телеком, 2004. – 367 с.

4. Звездинский, С. С. Победа любой ценой? Эффективность и результативность средств обнаружения / С. С. Звездинский, В. Иванов // «БДИ», 2005. – №5 (62). – С. 64–70.

5. Надёжность технических систем : справочник / Ю. К. Беляев [и др.]; под ред. И. А. Ушакова. – М. : Радио и связь, 1985. – 608 с.

# ЛАБОРАТОРНАЯ РАБОТА №4 ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ЭСБ МЕТОДОМ ДЕКОМПОЗИЦИИ

## 4.1. Цель работы

Методом декомпозиции определить показатель эффективности функционирования сложной электронной системы безопасности (ЭСБ) и исследовать изменение эффективности ЭСБ в зависимости от состава её аппаратных частей.

## 4.2. Описание исследуемой ЭСБ

### 4.2.1. План объекта

В качестве объекта защиты рассматривается одноэтажное здание инновационной компании (рис. 4.1). Охране подлежат материальные и информационные ресурсы, находящиеся в комнатах здания – помещениях 1...24.

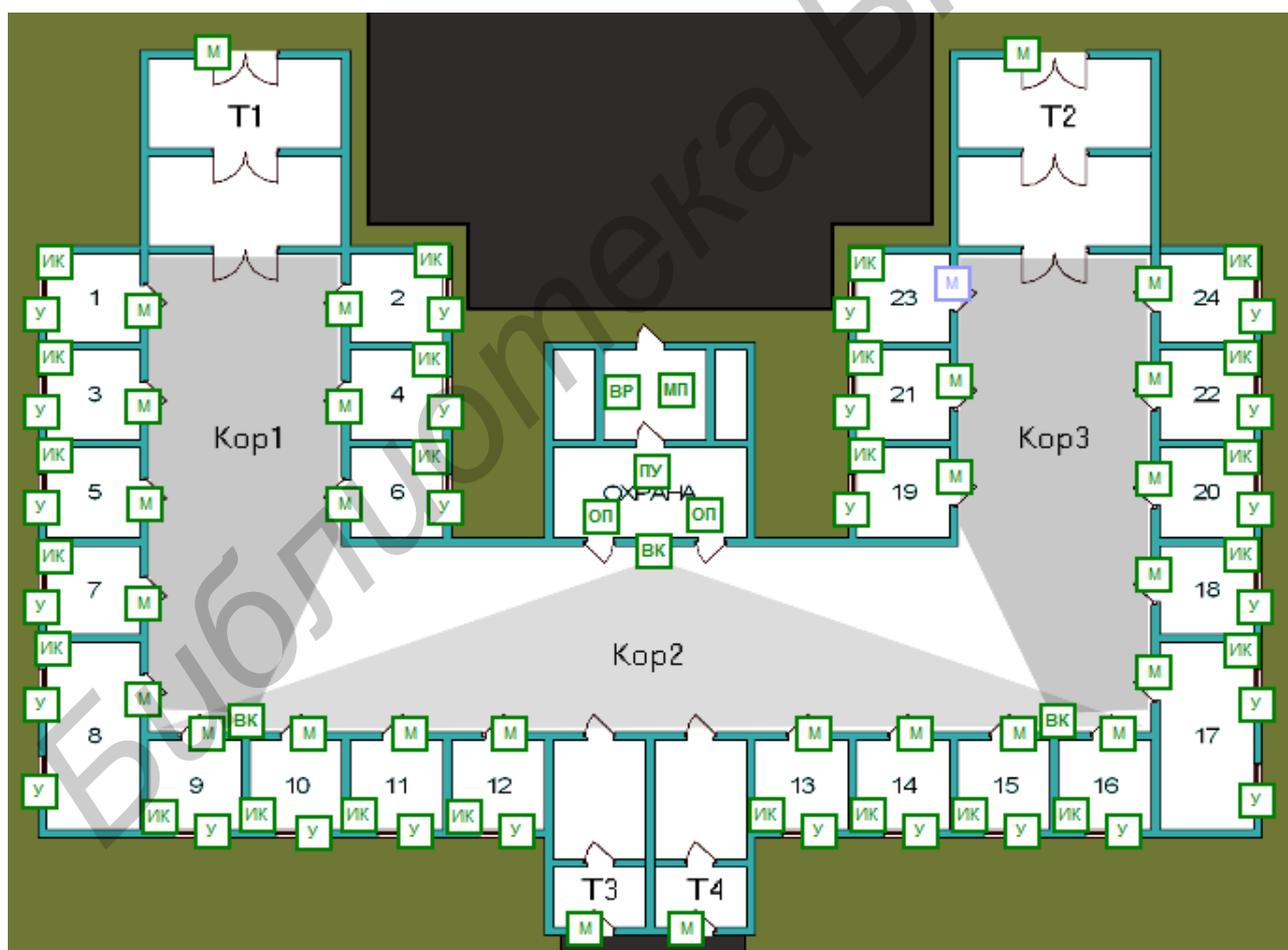
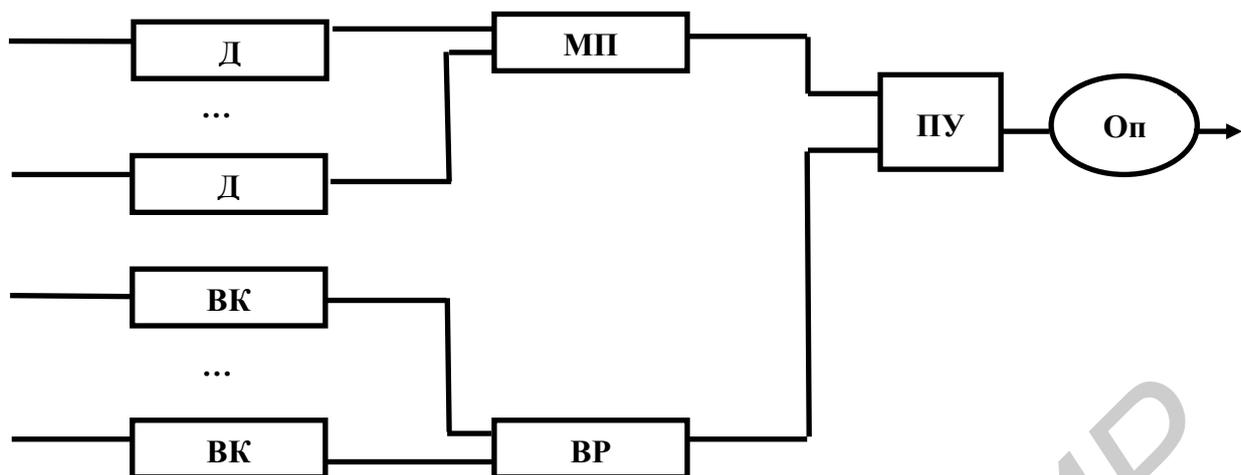


Рис. 4.1. План объекта защиты

Структурная схема ЭСБ, выполняющей функции по защите объекта, приведена на рис. 4.2.



Д – датчики (устанавливаются на окнах, дверях и в комнатах); ВК – видеокамеры (устанавливаются в коридорах, могут рассматриваться как разновидность датчиков); МП – микропроцессорное приёмно-контрольное устройство; ВР – видеорегистрирующее устройство; ПУ – пульт управления; Оп – операторы (охрана)

Рис. 4.2. Структурная схема исследуемой ЭСБ

#### 4.2.2. Цель злоумышленника

Предполагается, что злоумышленник через тамбуры или окна может проникнуть в ту или иную комнату здания и похитить хранящиеся там материальные или информационные ресурсы.

#### 4.2.3. Датчики, используемые в ЭСБ

В исследуемой ЭСБ планируется использовать следующие датчики (см. рис. 4.1):

- ударозвуковые (разбития стекла), устанавливаются на окна (**У**);
- магнитоконтактные, устанавливаются на двери (**М**);
- инфракрасные, устанавливаются в комнатах (**ИК**);
- видеокамеры, устанавливаются в коридорах (**ВК**).

#### 4.2.4. Показатель эффективности функционирования ЭСБ

В качестве показателя эффективности функционирования ЭСБ рассматривается вероятность защиты объекта от проникновения нарушителя во внутрь комнат с целью хищения материальных или информационных ресурсов, хранящихся в них. Защита объекта заключается в обнаружении датчиками факта проникновения нарушителя, передаче сигналов, сформированных датчиками, для обработки в устройства МП и ВР с последующей выдачей управляющих сигналов операторам (охране) на устройство ПУ и ликвидацией угрозы действиями охраны.

#### 4.2.5. Допущения, принимаемые при анализе эффективности функционирования ЭСБ

При исследовании эффективности функционирования ЭСБ принимаются следующие допущения:

- исследуемая ЭСБ рассматривается как система, выполняющая требуемую задачу, продолжительность которой такова, что за это время система останется наверняка в одном и том же состоянии;
- устройства, входящие в состав ЭСБ, являются восстанавливаемыми;
- видеокамеры рассматриваются как разновидность датчиков;
- проникновения нарушителей на объект (в здание и его комнаты) возможны только через окна и двери; проникновения путём пролома стен, подкопа и через крышу не рассматриваются;
- ложные тревоги, обусловленные срабатыванием датчиков при отсутствии нарушителя, не принимаются во внимание;
- одиночные нарушители или их группы в конкретный момент времени пытаются проникнуть в здание в одном месте;
- если нарушитель проник в любую из комнат незамеченным датчиками, установленными на пути его движения, то считается, что он похитил ресурсы и покинул помещение также незамеченным;
- МП, ВР, ПУ и Оп с точки зрения восприятия и дальнейшей обработки сигналов о проникновении в помещения объекта (тамбуры, коридоры, комнаты) являются идеальными, т. е. вероятности правильной обработки ими сигналов о проникновении равны единице;
- охрана объекта (функциональная часть Оп) в случае поступления сигнала о проникновении нарушителя на ПУ во всех случаях решает задачу по ликвидации угрозы;
- гипотетические пути проникновения в комнаты здания соответствуют данным табл. 4.1;
- привлекательности тамбуров для проникновения нарушителя в здание с выбранной им стороны одинаковы;
- привлекательности комнат для проникновения в них нарушителя из конкретного коридора одинаковы (см. табл. 4.1);
- привлекательности окон для проникновения нарушителя в здание с выбранной им стороны одинаковы.

Таблица 4.1

Рассматриваемые пути проникновения нарушителя в комнаты здания

Сторона здания	Наименование и номера помещений, в которые может проникнуть нарушитель				
	тамбур	коридор	комната (проникновение через дверь)	комната (проникновение через окно)	Примечание
Запад	–	–	–	1, 3, 5, 7, 8	–
Север	T1 T2	Кор1 Кор3	1...8 17...24	–	Сторона не включает двор
Двор	–	–	–	2, 4, 6, 19, 21, 23	–
Восток	–	–	–	17, 18, 20, 22, 24	–
Юг	T3, T4 –	Кор2 –	9...16 –	– 9...16	Фасад здания

### 4.3. Методические указания по исследованию эффективности функционирования ЭСБ

#### 4.3.1. Подсистемы, выделяемые при анализе эффективности функционирования ЭСБ

Оценка эффективности функционирования сложных ЭСБ путём рассмотрения системы в целом на практике вызывает много затруднений из-за чрезмерно большого числа возможных технических состояний системы  $S$ , определяемого как

$$S = 2^n,$$

где  $n$  – суммарное количество технических устройств, входящих в ЭСБ.

Например, при наличии лишь по одному датчику на каждой входной двери и на каждом окне комнат здания, рассматриваемого в лабораторной работе (24 комнаты), число возможных технических состояний ЭСБ составит

$$2^{24+24} > 2,8 \cdot 10^{14}.$$

Причём это число не учитывает другие устройства ЭСБ.

Поэтому в инженерной практике приходится прибегать к различным методам упрощения анализа эффективности функционирования ЭСБ. Одним из таких методов является *декомпозиция*. Суть её состоит в разделении исследуемой ЭСБ на меньшие по размеру подсистемы, анализ каждой из которых значительно проще анализа исходной системы. Получив показатели эффективности функционирования подсистем, можно относительно несложно найти показатель эффективности функционирования ЭСБ в целом.

При анализе эффективности функционирования ЭСБ подсистемы, входящие в систему, следует выделять исходя из возможных путей проникновения нарушителя к охраняемым ресурсам, находящимся в комнатах здания. Рекомендуется выделить такие подсистемы, функционирование которых противодействует проникновению нарушителя к ресурсам.

Для ЭСБ, рассматриваемой в лабораторной работе, логично выделить следующие подсистемы:

- подсистема «Тамбур – коридор», условно далее называемая подсистемой «Тамбур» (четыре подсистемы). В состав подсистемы «Тамбур» входят: датчик М, установленный на входной двери тамбура, видеокамера ВК, установленная в коридоре и контролирующая вход в комнаты согласно табл. 4.2, а также устройства МП и ВР, обрабатывающие сигналы, поступающие от датчиков;
- подсистема «Дверь – комната» (24 подсистемы). Эта подсистема включает датчик М, устанавливаемый на входной двери комнаты, датчик ИК, установленный в самой комнате, и устройство МП, обрабатывающее сигналы, поступающие от датчиков;

– подсистема «Окно – малая комната», условно далее называемая подсистемой «Окно – комната» (22 подсистемы). Эта подсистема включает датчик У, устанавливаемый на окне, датчик ИК, установленный в самой комнате, и устройство МП, обрабатывающее сигналы, поступающие от датчиков;

– подсистема «Два окна – большая комната», условно далее обозначаемая как «Два окна – комната» (две подсистемы). Эта подсистема включает датчики У, установленные на окнах комнаты, датчик ИК, установленный непосредственно в самой комнате, и устройство МП, обрабатывающее сигналы, поступающие от датчиков. Какой из датчиков У на окнах большой комнаты будет обозначен в формулах анализа как У1, а какой как У2 – не играет принципиальной роли.

Таблица 4.2

Зоны, контролируемые видеокамерами

Условный номер видеокамеры ВК	Контролируемый коридор	Номера комнат, дверь которых контролируется
ВК1	Кор1	1...8
ВК2	Кор2	9...16
ВК3	Кор3	17...24

#### 4.3.2. Рассмотрение подсистемы «Тамбур»

План помещений, защита которых осуществляется функционированием подсистемы «Тамбур», представлен на рис. 4.3.

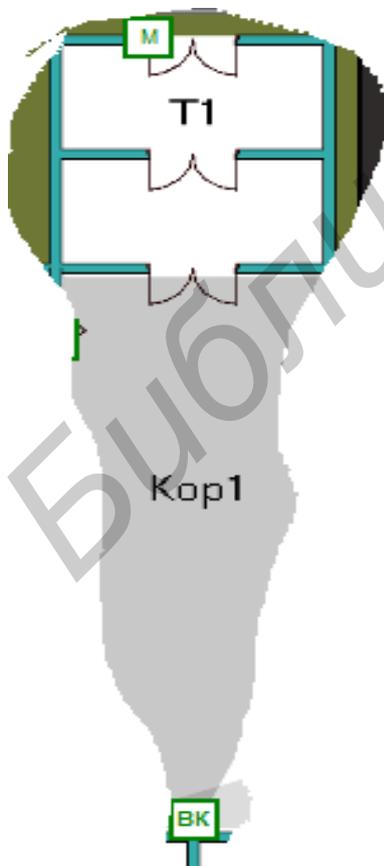


Рис. 4.3. Подсистема «Тамбур» на примере тамбура Т1 и коридора Кор1 левого крыла здания (устройства МП и ВР, входящие в состав подсистемы, установлены в помещении охраны и здесь не показаны)

Как было отмечено, в состав подсистемы «Тамбур» входят датчик М, установленный на входной двери тамбура, видеокамера ВК, установленная в коридоре и контролирующая вход в комнаты согласно табл. 4.2, а также устройства МП и ВР, обрабатывающие сигналы, поступающие от датчиков. Устройства МП и ВР установлены в помещении охраны.

Видеокамера ВК контролирует проникновение нарушителя в тот или иной коридор, а затем через дверь в комнату, поэтому рассматривается как часть соответствующей подсистемы «Тамбур».

В состав каждой из подсистем «Тамбур» также должны быть включены устройства МП и ВР, которые обрабатывают сигналы, поступающие от датчиков, входящих в состав подсистемы «Тамбур». Видеокамера ВК рассматривается как разновидность датчиков. Схема (модель, условность) соединения датчиков М и ВК, устройств МП и ВР с точки зрения восприятия факта проникновения нарушителя в коридор показана на рис. 4.4.

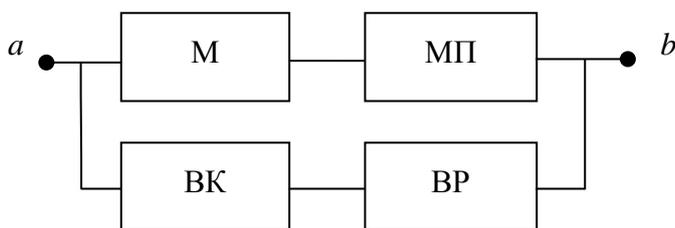


Рис. 4.4. Модель соединения датчиков М и ВК, устройств МП и ВР подсистемы «Тамбур» с точки зрения восприятия факта проникновения нарушителя в коридор здания

Невосприятие датчиком М или ВК факта проникновения нарушителя, неправильная обработка устройством МП или ВР сигналов, поступающих от датчиков, означают появление обрыва в соответствующем месте схемы. Подсистема «Тамбур» полностью теряет способность воспринять сигнал о проникновении нарушителя, если на схеме

(модели) от точки *a* до точки *b* нет замкнутого пути.

Формула расчёта вероятности обнаружения нарушителя подсистемой «Тамбур» (обозначим эту вероятность через  $p_T$ ) определяется как

$$\begin{aligned} p_T = 1 - q_T = 1 - q_{M,MP} q_{BK,VR} &= 1 - (1 - p_{M,MP})(1 - p_{BK,VR}) = \\ &= 1 - (1 - p_M p_{MP})(1 - p_{BK} p_{VR}), \end{aligned} \quad (4.1)$$

причём

$$q_{M,MP} = 1 - p_{M,MP},$$

$$q_{BK,VR} = 1 - p_{BK,VR},$$

$$p_{M,MP} = p_M p_{MP},$$

$$p_{BK,VR} = p_{BK} p_{VR},$$

где символы  $p$  и  $q$  означают вероятности обнаружения и необнаружения нарушителя, а по нижним индексам интуитивно понятна суть соответствующих вероятностей; нижние индексы «М,МП» и «ВК,ВР» означают, что вероятности относятся к цепочке, включающей указанные устройства.

*Определение вероятностей состояний подсистемы «Тамбур» и коэффициентов эффективности состояний*

Возможные состояния любой системы определяются состояниями работоспособности и неработоспособности устройств, входящих в рассматриваемую систему.

Подсистему «Тамбур» образуют четыре устройства: М, ВК, МП и ВР. Каждое устройство в любой произвольный момент времени может находиться в одном из двух состояний: состоянии работоспособности или состоянии неработоспособности. Поэтому общее количество возможных состояний подсистемы определится как  $2^n$ , где  $n$  – количество устройств, входящих в подсистему «Тамбур». Общее число состояний подсистемы «Тамбур»  $S = 2^4 = 16$ .

Формула расчёта вероятности  $i$ -го состояния подсистемы «Тамбур» принимает вид

$$h_i = s(\text{М}) \cdot s(\text{ВК}) \cdot s(\text{МП}) \cdot s(\text{ВР}), \quad (4.2)$$

где  $s(j)$  – вероятность, характеризующая техническое состояние (работоспособное или неработоспособное)  $j$ -го устройства подсистемы «Тамбур»,  $j \rightarrow \text{М, ВК, МП, ВР}$ .

Для выполнения расчётов по формуле (4.2) удобно пользоваться символическими обозначениями состояний подсистемы (табл. 4.3). В табл. 4.3 вероятность работоспособного состояния устройств, входящих в подсистему, обозначена через  $r(j)$ ,  $j \rightarrow \text{М, ВК, МП, ВР}$ . В теории надёжности технических изделий показатель  $r(j)$  называют стационарным коэффициентом готовности, кратко просто коэффициентом готовности [4, 5]. Слово стационарный подчёркивает то, что значение этого коэффициента не зависит от рассматриваемого момента времени. Вероятностям неработоспособного состояния устройств, входящих в подсистему, соответствуют величины  $[1 - r(j)]$ ,  $j \rightarrow \text{М, ВК, МП, ВР}$ .

В формулу (4.2) в качестве значений вероятностей вида  $s(j)$  необходимо подставить вероятность  $r(j)$ , если  $j$ -е устройство находится в работоспособном состоянии, и вероятность  $[1 - r(j)]$ , если – в неработоспособном состоянии.

Если в табл. 4.3 состоянию данного устройства отвечает цифра «1» (состояние работоспособности), в формулу (4.2) для данного устройства необходимо подставлять вероятность  $r(j)$ , если цифра «0» – вероятность  $[1 - r(j)]$ . С учётом этого в табл. 4.3 в качестве примеров приводятся рабочие расчётные формулы, полученные для некоторых состояний подсистемы «Тамбур».

Коэффициент эффективности технического состояния (условный коэффициент эффективности)  $\Phi_i$  представляет собой вероятность того, что подсистема, находясь в состоянии  $h_i$ , воспримет факт проникновения нарушителя на объект. Коэффициент эффективности технического состояния определяется по формуле

$$\Phi_i = p_{Ti}$$

где  $p_{Ti}$  – вероятность обнаружения нарушителя подсистемой «Тамбур», определяемая по формуле (4.1) для случая, когда подсистема находится в состоянии  $h_i$ .

При расчёте  $p_{Ti}$  по формуле (4.1) вероятность  $p$ , соответствующую конкретному устройству подсистемы, необходимо принять равной нулю, если это устройство находится в неработоспособном состоянии.

Коэффициент эффективности технических состояний  $\Phi_i$  подсистемы «Тамбур» определяется как вероятностями восприятия сигнала о проникновении датчиками М и ВК, вероятностями правильной обработки этих сигналов устройствами МП и ВР, так и работоспособностью датчиков М и ВК, устройств МП и ВР.

Таблица 4.3

Возможные состояния подсистемы «Тамбур»

Но- мер со- стоя- ния	Символи- ческое обозначе- ние со- стояния	Состояние работоспо- собности устройств подсистемы				Формула определения вероятности состояния $h_i$	Определение ко- эффициента эффек- тивности состояния $\Phi_i = \Phi(XX/XX)$ , где $X = 1$ или $X = 0$
		М	ВК	МП	ВР		
1	11/11	1	1	1	1	$r(M) \cdot r(BK) \cdot r(MP) \cdot r(BP)$	*
2	11/10	1	1	1	0	$r(M) \cdot r(BK) \cdot r(MP) \cdot [1 - r(BP)]$	**
3	11/01	1	1	0	1	$r(M) \cdot r(BK) \cdot [(1 - r(MP)) \cdot r(BP)]$	***
...	...					...	...
9	01/11	0	1	1	1	$[1 - r(M)] \cdot r(BK) \cdot r(MP) \cdot r(BP)$	****
...	...					...	...
16	00/00	0	0	0	0	$[1 - r(M)] \cdot [1 - r(BK)] \times$ $\times [1 - r(MP)] \cdot [1 - r(BP)]$	0

**Примечания:**

1. Цифра «1» в символическом обозначении состояния подсистемы и обозначении состояний работоспособности входящих в подсистему устройств отвечает работоспособному состоянию соответствующего устройства, а цифра «0» – неработоспособному состоянию устройства.

2. Символическое обозначение состояния XX/XX (где  $X = 1$  или  $X = 0$ ) фактически есть состояние XXXX. Например, состояние 01/11 – это то же самое, что и состояние 0111. С учётом принятых условий  $p_{MP} = 1$  и  $p_{BP} = 1$  запись XX/XX использована для того, чтобы подчеркнуть то, что коэффициент эффективности состояния подсистемы зависит лишь от вероятностей восприятия сигнала о нарушении датчиками М и ВК, но эти вероятности далее в ЭСБ «реализуются» или «не реализуются» в зависимости от состояния работоспособности как самих датчиков М и ВК, так и устройств МП и ВР. Знак «/» в символическом обозначении состояния подсистемы XX/XX заменяет слова «при условии, что имеет место», а после черты указывается уровень работоспособности устройств МП и ВР.

3. Принятые обозначения:

\*  $\Phi(11/11)$  определяется по формуле (4.1) путём подстановки в неё соответствующих вероятностей  $p$  устройств М, ВК, МП и ВР.

\*\*  $\Phi(11/10)$  определяется по формуле (4.1), но в этом случае, несмотря на работоспособность ВК, сигнал о восприятии нарушителя этим датчиком не будет далее передан для обработки ввиду отказа (состояния неработоспособности) устройства ВР, т. е. для определения  $\Phi(11/10)$  в формуле (4.1) необходимо принять  $p_{BP} = 0$  и, следовательно,  $\Phi(11/10) = p_M p_{MP}$ .

\*\*\*  $\Phi(11 / 01) = p_{BK} p_{BP}$ . Здесь, несмотря на работоспособность М, сигнал о восприятии этим датчиком нарушителя не будет передан далее для обработки ввиду состояния неработоспособности устройства МП ( $p_{MP} = 0$ ).

\*\*\*\*  $\Phi(01/11)$  определяется по формуле (4.1). Здесь сигнал о проникновении нарушителя не будет воспринят датчиком М ввиду состояния его неработоспособности, т. е. при определении  $\Phi(01/11)$  по формуле (4.1) необходимо принять  $p_M = 0$ .

$r(j)$ ,  $[1 - r(j)]$  – вероятность работоспособного и вероятность неработоспособного состояний  $j$ -го устройства в любой момент времени,  $j \rightarrow M, BK, MP, BP$ .

Отметим, что для всех состояний вида (.../00) условный коэффициент эффективности  $\Phi_i$  равен нулю, независимо от состояния работоспособности датчиков М и ВК, т. к. при одновременной неработоспособности устройств МП и ВР сигналы (если они получены) о проникновении нарушителя не могут быть далее обработаны.

Показатель эффективности функционирования  $k$ -й подсистемы «Тамбур» ( $k = 1, \dots, 4$ ) определяется формулой

$$E_T = \sum_{i=1}^{16} h_i \Phi_i. \quad (4.3)$$

### 4.3.3. Рассмотрение подсистемы «Дверь – комната»

План помещений, защита которых осуществляется функционированием подсистемы «Дверь – комната», показан на рис. 4.5.

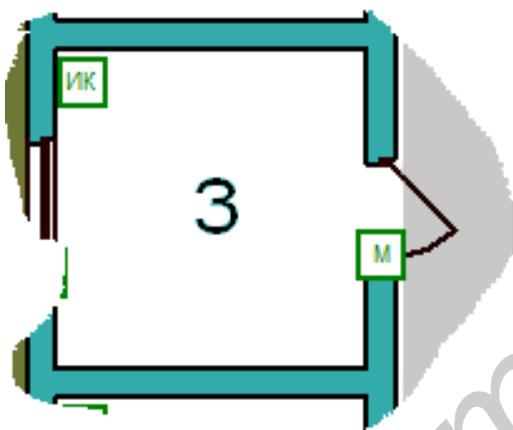


Рис. 4.5. Подсистема «Дверь – комната» на примере комнаты №3 (устройство МП, входящее в состав подсистемы, установлено в помещении охраны и здесь не показано)

Эта подсистема включает датчик М, установленный на дверях комнаты, датчик ИК, установленный в самой комнате, и устройство МП, обрабатывающее сигналы, поступающие от датчиков.

Модель соединения датчиков М, ИК и устройства МП с точки зрения восприятия факта проникновения нарушителя в комнату через дверь приведена на рис. 4.6.

Невосприятие датчиком М и ИК факта проникновения или неправильная обработка устройством МП сигналов, поступающих от датчиков, означает появление обрыва в соответствующем месте схемы. Подсистема «Дверь – комната» полностью теряет способность воспринять сигнал о проникновении в комнату, если на схеме от точки  $a$  до точки  $b$  нет ни одного пути (см. рис. 4.6).

Применяя формулы (теоремы) теории вероятностей, можно получить формулу для расчёта вероятности обнаружения нарушителя при его попытке проникнуть через дверь во внутрь комнаты ( $p_{дк}$ ). Итоговая формула расчёта вероятности  $p_{дк}$  принимает вид

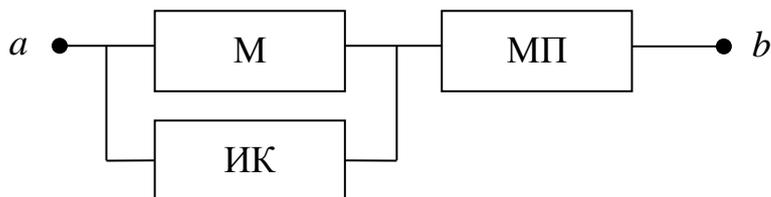


Рис. 4.6. Модель соединения датчиков М, ИК и устройства МП подсистемы «Дверь – комната» с точки зрения проникновения нарушителя в комнату через дверь

$$p_{\text{лк}} = p_{\text{М,ИК}} p_{\text{МП}} = (1 - q_{\text{М,ИК}}) p_{\text{МП}} = (1 - q_{\text{М}} q_{\text{ИК}}) p_{\text{МП}} = [1 - (1 - p_{\text{М}})(1 - p_{\text{ИК}})] p_{\text{МП}}, \quad (4.4)$$

причём

$$p_{\text{М,ИК}} = 1 - q_{\text{М,ИК}},$$

$$q_{\text{М,ИК}} = q_{\text{М}} q_{\text{ИК}},$$

$$q_{\text{М}} = 1 - p_{\text{М}},$$

$$q_{\text{ИК}} = 1 - p_{\text{ИК}},$$

где символы  $p$  и  $q$  означают вероятности обнаружения и необнаружения нарушителя, а по нижним индексам интуитивно понятна суть соответствующих вероятностей; нижний индекс «М,ИК» означает, что вероятности относятся к параллельной цепочке, включающей датчики М и ИК.

*Определение вероятностей состояний подсистемы «Дверь – комната» и коэффициентов эффективности состояний*

Подсистема «Дверь – комната» включает три устройства: датчики М и ИК и устройство МП. Отметим, что общее число состояний подсистемы «Дверь – комната» составляет  $S = 2^3 = 8$ .

С определением вероятностей возможных состояний подсистемы «Дверь – комната» и коэффициентов эффективности этих состояний (условных коэффициентов эффективности  $\Phi_i$ ) можно ознакомиться, используя данные табл. 4.4.

Таблица 4.4

Возможные состояния подсистемы «Дверь – комната»

Номер состояния	Символическое обозначение состояния	Состояние работоспособности устройств подсистемы			Формула определения вероятности состояния $h_i$	Определение коэффициента эффективности состояния $\Phi_i = \Phi(\text{XX}/\text{X})$ , где $\text{X} = 1$ или $\text{X} = 0$
		М	ИК	МП		
1	11/1	1	1	1	$r(\text{М}) \cdot r(\text{ИК}) \cdot r(\text{МП})$	*
2	11/0	1	1	0	$r(\text{М}) \cdot r(\text{ИК}) \cdot [1 - r(\text{МП})]$	0
3	10/1	1	0	1	$r(\text{М}) \cdot [1 - r(\text{ИК})] \cdot r(\text{МП})$	**
4	10/0	1	0	0	$r(\text{М}) \cdot [1 - r(\text{ИК})] \cdot [1 - r(\text{МП})]$	0
5	01/1	0	1	1	$[1 - r(\text{М})] \cdot r(\text{ИК}) \cdot r(\text{МП})$	***
6	01/0	0	1	0	$[1 - r(\text{М})] \cdot r(\text{ИК}) \cdot [1 - r(\text{МП})]$	0
7	00/1	0	0	1	$[1 - r(\text{М})] \cdot [1 - r(\text{ИК})] \cdot r(\text{МП})$	****
8	00/0	0	0	0	$[1 - r(\text{М})] \cdot [1 - r(\text{ИК})] \cdot [1 - r(\text{МП})]$	0

*Примечания:*

1. Цифра «1» в символическом обозначении состояния подсистемы и обозначении состояний работоспособности входящих в подсистему устройств отвечает работоспособному состоянию соответствующего устройства, а цифра «0» – неработоспособному состоянию устройства.

2. Символическое обозначение состояния  $\text{XX}/\text{X}$  (где  $\text{X} = 1$  или  $\text{X} = 0$ ) фактически есть состояние  $\text{XXX}$ . Например, состояние 01/1 – это то же самое, что и состояние 011.

С учётом принятого условия  $p_{МП} = 1$  запись XX/X использована для того, чтобы подчеркнуть то, что коэффициент эффективности состояния подсистемы зависит лишь от вероятностей восприятия сигнала о нарушении датчиками М и ИК, но эти вероятности далее в ЭСБ «реализуются» или «не реализуются» в зависимости от состояния работоспособности как самих датчиков М и ИК, так и устройства МП. Знак «/» в символическом обозначении состояния подсистемы XX/X заменяет слова «при условии, что имеет место», а после черты указывается уровень работоспособности устройства МП.

3. Принятые обозначения:

\*  $\Phi(11/1)$  определяется по формуле (4.4) путём подстановки в неё вероятностей  $p$  устройств М, ИК и МП.

\*\*  $\Phi(10/1)$  определяется по формуле (4.4). Но здесь сигнал о проникновении не будет воспринят датчиком ИК ввиду его неработоспособности, т. е. при определении  $\Phi(10/1)$ , используя формулу (4.4), необходимо принять  $p_{ИК} = 0$ .

\*\*\*  $\Phi(01/1)$  определяется по формуле (4.4). Здесь сигнал о проникновении не будет воспринят датчиком М ввиду его неработоспособности, т. е. при определении  $\Phi(01/1)$  по формуле (4.4) необходимо принять  $p_M = 0$ .

\*\*\*\*  $\Phi(00/1) = 0$ . Здесь, несмотря на работоспособность устройства МП, коэффициент эффективности, определяемый по формуле (4.4), оказывается равным нулю из-за состояния неработоспособности обоих датчиков М и ИК ( $p_M = 0, p_{ИК} = 0$ ).

$r(j), [1 - r(j)]$  – вероятность работоспособного и вероятность неработоспособного состояний  $j$ -го устройства подсистемы «Дверь – комната» в любой момент времени,  $j \rightarrow$  М, ИК, МП.

Отметим, что для всех состояний вида (.../0) условный коэффициент эффективности  $\Phi_i$  равен нулю, независимо от состояния работоспособности датчиков М и ИК, т. к. при неработоспособности устройства МП сигналы о проникновении нарушителя, если они получены датчиками, не могут быть обработаны ( $p_{МП} = 0$ ).

Показатель эффективности функционирования  $k$ -й подсистемы «Дверь – комната» ( $k = 1, \dots, 24$ ) определяется формулой

$$E_{\text{дк}} = \sum_{i=1}^8 h_i \Phi_i. \quad (4.5)$$

#### 4.3.4. Рассмотрение подсистемы «Окно – комната»

План комнаты, связанной с подсистемой вида «Окно – комната», показан на рис. 4.7.

Подсистема «Окно – комната» включает датчик У, устанавливаемый на окне, датчик ИК, установленный в самой комнате, и устройство МП, обрабатывающее сигналы, поступающие от датчиков.

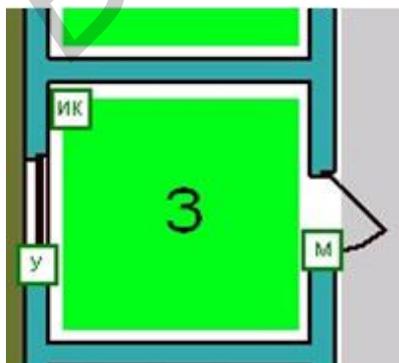


Рис. 4.7. Подсистема «Окно – комната» на примере комнаты №3 (датчик М не входит в состав подсистемы; устройство МП, входящее в состав подсистемы, установлено в помещении охраны и здесь не показано)

Схема (модель) соединения датчиков У, ИК и устройства МП с точки зрения восприятия факта проникновения нарушителя в комнату через окно приведена на рис. 4.8.

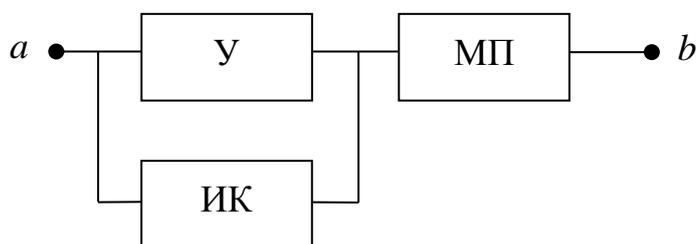


Рис. 4.8. Модель соединения датчиков У, ИК и устройства МП подсистемы «Окно – комната» с точки зрения проникновения нарушителя в комнату через окно

Невосприятие датчиком У, ИК факта проникновения или неправильная обработка устройством МП сигналов, поступающих от датчиков, означает появление обрыва в соответствующем месте схемы. Подсистема «Окно – комната» полностью теряет способность воспринять сигнал о проникновении в комнату, если на схеме от точки *a* до точки *b* нет ни одного пути.

Применяя формулы (теоремы) теории вероятностей, можно получить формулу для расчёта вероятности обнаружения нарушителя при его попытке проникнуть через окно во внутрь комнаты. Обозначим эту вероятность через  $p_{ок}$ .

Итоговая интересующая формула расчёта вероятности  $p_{ок}$  имеет вид:

$$p_{ок} = p_{У,ИК} p_{МП} = (1 - q_{У,ИК}) p_{МП} = (1 - q_U q_{ИК}) p_{МП} = [1 - (1 - p_U)(1 - p_{ИК})] p_{МП}, \quad (4.6)$$

причём

$$p_{У,ИК} = 1 - q_{У,ИК},$$

$$q_{У,ИК} = q_U q_{ИК},$$

$$q_U = 1 - p_U,$$

$$q_{ИК} = 1 - p_{ИК},$$

где символы  $p$  и  $q$  означают вероятности обнаружения и необнаружения нарушителя, а по нижним индексам интуитивно понятна суть соответствующих вероятностей; нижний индекс «У,ИК» означает, что вероятности относятся к параллельной цепочке, включающей датчики У и ИК.

Коэффициент эффективности технических состояний подсистемы «Окно – комната» определяется как работоспособностью датчиков У и ИК, так и работоспособностью устройства МП, формально входящего во все выделяемые подсистемы «Окно – комната». Данный коэффициент рассчитывается по формуле

$$\Phi_i = p_{ок i},$$

где  $p_{ок i}$  – вероятность восприятия сигнала о проникновении нарушителя в случае, когда подсистема «Окно – комната» находится в состоянии  $h_i$ .

*Определение вероятностей состояний подсистемы «Окно – комната» и коэффициентов эффективности состояний*

Подсистема «Окно – комната» включает три устройства: датчики У и ИК и устройство МП. Отметим, что общее число состояний подсистемы «Окно – комната» составляет  $S = 2^3 = 8$ .

С определением вероятностей возможных состояний подсистемы «Окно – комната» и коэффициентов эффективности этих состояний (условных коэффициентов эффективности)  $\Phi_i$  можно ознакомиться, используя данные табл. 4.5.

Таблица 4.5

Возможные состояния подсистемы «Окно – комната»

Номер состояния	Символическое обозначение состояния	Состояние работоспособности устройств подсистемы			Формула определения вероятности состояния $h_i$	Определение коэффициента эффективности состояния $\Phi_i = \Phi(XX/X)$ , где $X = 1$ или $X = 0$
		У	ИК	МП		
1	11/1	1	1	1	$r(У) \cdot r(ИК) \cdot r(МП)$	*
2	11/0	1	1	0	$r(У) \cdot r(ИК) \cdot [1-r(МП)]$	0
3	10/1	1	0	1	$r(У) \cdot [1-r(ИК)] \cdot r(МП)$	**
4	10/0	1	0	0	$r(У) \cdot [1-r(ИК)] \cdot [1-r(МП)]$	0
5	01/1	0	1	1	$[1-r(У)] \cdot r(ИК) \cdot r(МП)$	***
6	01/0	0	1	0	$[1-r(У)] \cdot r(ИК) \cdot [1-r(МП)]$	0
7	00/1	0	0	1	$[1-r(У)] \cdot [1-r(ИК)] \cdot r(МП)$	****
8	00/0	0	0	0	$[1-r(У)] \cdot [1-r(ИК)] \cdot [1-r(МП)]$	0

*Примечания:*

1. Цифра «1» в символическом обозначении состояния подсистемы и обозначении состояний работоспособности входящих в подсистему устройств отвечает работоспособному состоянию соответствующего устройства, а цифра «0» – неработоспособному состоянию устройства.

2. Символическое обозначение состояния  $XX/X$  (где  $X = 1$  или  $X = 0$ ) фактически есть состояние  $XXX$ . Например, состояние 01/1 – это то же самое, что и состояние 011. С учётом принятого условия  $r_{МП} = 1$  запись  $XX/X$  использована для того, чтобы подчеркнуть то, что коэффициент эффективности состояния подсистемы зависит лишь от вероятностей восприятия сигнала о нарушении датчиками У и ИК, но эти вероятности далее в ЭСБ «реализуются» или «не реализуются» в зависимости от состояния работоспособности как самих датчиков У и ИК, так и устройства МП. Знак «/» в символическом обозначении состояния подсистемы  $XX/X$  заменяет слова «при условии, что имеет место», а после черты указывается уровень работоспособности устройства МП.

3. Принятые обозначения:

\*  $\Phi(11/1)$  определяется по формуле (4.6) путём подстановки в неё вероятностей  $r$  устройств У, ИК и МП.

\*\*  $\Phi(10/1)$  определяется по формуле (4.6). Здесь сигнал о проникновении не будет воспринят датчиком ИК ввиду его неработоспособности, т. е. при определении  $\Phi(10/1)$ , используя формулу (4.6), необходимо принять  $r_{ИК} = 0$ .

\*\*\*  $\Phi(01/1)$  определяется по формуле (4.6). Здесь сигнал о проникновении не будет воспринят датчиком У ввиду его неработоспособности, т. е. при определении  $\Phi(01/1)$  по формуле (4.6) необходимо принять  $r_U = 0$ .

\*\*\*\*  $\Phi(00/1) = 0$ . Здесь, несмотря на работоспособность устройства МП, коэффициент эффективности состояния оказывается равным нулю из-за неработоспособности обоих датчиков (У и ИК).

$r(j)$ ,  $[1 - r(j)]$  – обозначения соответственно вероятностей работоспособного и неработоспособного состояний  $j$ -го устройства подсистемы «Окно – комната» в любой момент времени,  $j \rightarrow У, ИК, МП$ .

Отметим, что для всех состояний вида (.../0) условный коэффициент эффективности  $\Phi_i$  равен нулю, независимо от состояния работоспособности датчиков У и ИК, т. к. при неработоспособности устройства МП сигналы о проникновении нарушителя, если они получены датчиками, не могут быть обработаны ( $p_{МП} = 0$ ).

Показатель эффективности функционирования  $k$ -й подсистемы «Окно – комната» ( $k = 1, \dots, 22$ ) определяется формулой

$$E_{ок} = \sum_{i=1}^8 h_i \Phi_i. \quad (4.7)$$

#### 4.3.5. Рассмотрение подсистемы «Два окна – комната»

Применительно к охраняемому объекту и рассматриваемой ЭСБ можно выделить две подсистемы «Два окна – комната». Подсистема этого вида включает два датчика У (условно обозначаемые как У1 и У2), контролирующие разбитие двух окон комнаты, датчик ИК, устанавливаемый непосредственно в самой комнате, и устройство МП, обрабатывающее сигналы, поступающие от датчиков. Состав подсистемы «Два окна – комната» на примере комнаты №8 понятен из рис. 4.9.

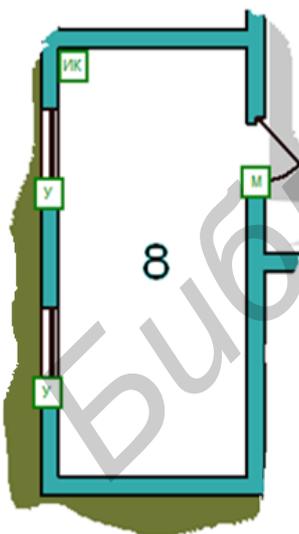


Схема соединения датчиков и устройства МП подсистемы «Два окна – комната» с точки зрения восприятия факта проникновения нарушителя в комнату через окна показана на рис. 4.10. Как отмечалось ранее, какой из датчиков У на окнах большой комнаты будет обозначен в формулах анализа как У1, а какой как У2 – не играет принципиальной роли.

Рис. 4.9. Подсистема «Два окна – комната» на примере комнаты №8 (датчик М не входит в состав подсистемы; устройство МП, входящее в состав подсистемы, установлено в помещении охраны и здесь не показано)

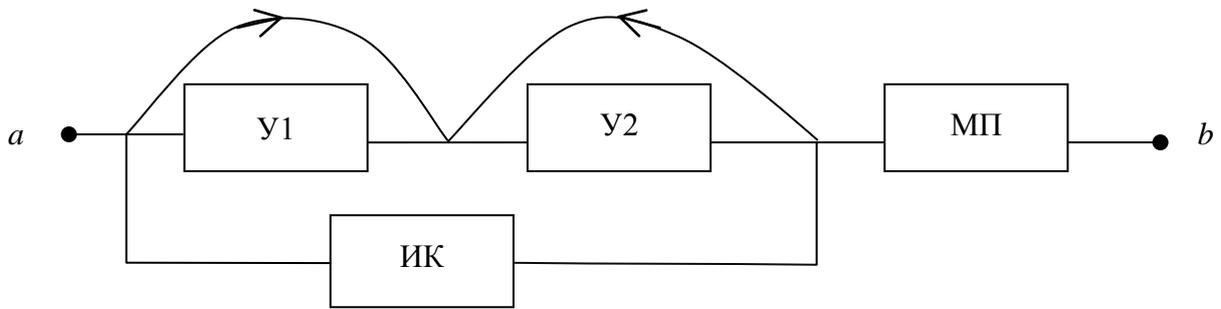


Рис. 4.10. Модель соединения датчиков У1, У2, ИК и устройства МП подсистемы «Два окна – комната» с точки зрения проникновения нарушителя в комнату через окна

Невосприятие конкретным датчиком факта проникновения или неправильная обработка устройством МП сигналов, поступающих от датчиков, означает появление обрыва в соответствующем месте схемы. Кривые линии с однонаправленной стрелкой означают то, что при отказе датчиков, соединённых этими линиями, не всегда возникает обрыв между точками *a* и *b*. Например, при невосприятии факта проникновения датчиками У1 и ИК не происходит полной потери способности воспринять сигнал о проникновении, о чём говорит путь на схеме от точки *a* по однонаправленной кривой и далее через датчик У2 к точке *b*. При установлении факта обрыва между *a* и *b* необходимо проверить пути от точки *a* к точке *b* и наоборот от *b* к *a*. При этом следует учитывать, что кривые линии являются однонаправленными, т. е. движение (путь) по ним возможно только в направлении, указанном стрелками. Если при определении возможного пути от *a* к *b* или от *b* к *a* мы упираемся в острие какой-либо стрелки, то это свидетельствует о возникновении обрыва между точками *a* и *b* (при условии, что между *a* и *b* или *b* и *a* нет другого пути). Подсистема «Два окна – комната» полностью теряет способность воспринять сигнал о проникновении, если на схеме от точки *a* до точки *b* при движении в прямом или обратном направлении нет ни одного пути.

Применяя формулы (теоремы) теории вероятностей, можно получить формулу для расчёта вероятности обнаружения нарушителя подсистемой «Два окна – комната». Эту вероятность обозначим через  $p_{\text{оок}}$ . При получении формулы приняты во внимание вероятности гипотез о том, что нарушитель попытается проникнуть через окно 1 ( $p_1$ ) или через окно 2 ( $p_2$ ). При получении итоговой интересующей формулы для вероятности  $p_{\text{оок}}$  использовано выражение

$$p_{y_1, y_1} = p_1 p_{y_1} + p_2 p_{y_2}, \quad (4.8)$$

здесь

$$p_1 = p(Y1/\text{ок}1), \text{ а } p_2 = p(Y2/\text{ок}2),$$

где  $p(Y1/\text{ок}1)$  и  $p(Y2/\text{ок}2)$  – вероятности восприятия сигнала о проникновении в комнату при условии, что нарушитель попытается проникнуть соответственно через первое и второе окна комнаты. При этом должно выполняться условие  $p_1 + p_2 = 1$ .

Вероятность обнаружения нарушителя с учётом трёх датчиков (У1, У2 и ИК) определяется формулой

$$p_{У1,У2,ИК} = 1 - [1 - (p_1 p_{У1} + p_2 p_{У2})] (1 - p_{ИК}). \quad (4.9)$$

Следовательно, вероятность обнаружения нарушителя при попытке проникновения в комнату с двумя окнами ( $p_{оок}$ ) имеет вид

$$p_{оок} = p_{У1,У2,ИК,МП} = \{1 - [1 - (0,5p_{У1} + 0,5p_{У2})] (1 - p_{ИК1})\} p_{МП}. \quad (4.10)$$

При получении выражения (4.10) учтено устройство МП и принято во внимание ранее указанное допущение, согласно которому  $p_1 = p_2 = 0,5$ .

Коэффициент эффективности технических состояний подсистемы «Два окна – комната» ( $\Phi_i$ ) определяется как вероятностями  $p$  устройств У1, У2, ИК и МП (см. формулу (4.10)), так и работоспособностью У1, У2, ИК и МП. Данный коэффициент рассчитывается по формуле

$$\Phi_i = p_{оок i},$$

где  $p_{оок i}$  – вероятность обнаружения нарушителя в случае, когда подсистема «Два окна – комната» находится в состоянии  $h_i$ .

#### *Определение вероятностей состояний подсистемы «Два окна – комната» и коэффициентов эффективности состояний*

С определением вероятностей возможных состояний подсистемы «Два окна – комната» и коэффициентов эффективности этих состояний можно ознакомиться, используя данные табл. 4.6. Отметим, что общее число состояний подсистемы  $S = 2^4 = 16$ , т. к. в состав подсистемы входят четыре устройства.

Таблица 4.6

Возможные состояния подсистемы «Два окна – комната»

Но- мер состо- яния	Символи- ческое обозначе- ние состо- яния	Состояние рабо- тоспособности устройств под- системы				Формула определения вероятности состояния $h_i$	Определение ко- эффициента эф- фективности со- стояния $\Phi_i = \Phi(\text{XXX}/\text{X})$ , где X = 1 или X = 0
		У1	У2	ИК	МП		
1	111/1	1	1	1	1	$r(У1) \cdot r(У2) \cdot r(ИК) \cdot r(МП)$	*
2	111/0	1	1	1	0	$r(У1) \cdot r(У2) \cdot r(ИК) \cdot [1 - r(МП)]$	**
3	110/1	1	1	0	1	$r(У1) \cdot r(У2) \cdot [(1 - r(ИК)) \cdot r(МП)]$	***
...	...					...	...
9	011/1	0	1	1	1	$[1 - r(У1)] \cdot r(У2) \cdot r(ИК) \cdot r(МП)$	****
...	...					...	...
16	000/0	0	0	0	0	$[1 - r(У1)] \cdot [1 - r(У2)] \cdot [1 - r(ИК)] \cdot [1 - r(МП)]$	0

#### *Примечания:*

1. Цифра «1» в символическом обозначении состояния подсистемы и обозначении состояний работоспособности, входящих в подсистему устройств, отвечает работоспособному состоянию соответствующего устройства, а цифра «0» – неработоспособному состоянию устройства.

2. Символическое обозначение состояния XXX/X (где  $X = 1$  или  $X = 0$ ) фактически есть состояние XXXX. Например, состояние 011/1 – это то же самое, что и состояние 0111. С учётом принятого условия  $p_{МП} = 1$  запись XXX/X использована для того, чтобы подчеркнуть то, что коэффициент эффективности состояния подсистемы зависит лишь от вероятностей восприятия сигнала о проникновении нарушителя датчиками У1, У2 и ИК, но эти вероятности «реализуются» или «не реализуются» в зависимости от состояния работоспособности как самих датчиков У1, У2 и ИК, так и устройства МП. Знак «/» в символическом обозначении состояния подсистемы XXX/X заменяет слова «при условии, что имеет место», а после черты указывается уровень работоспособности устройства МП.

3. Принятые обозначения:

\*  $\Phi(111/1)$  определяется по формуле (4.10) путём подстановки в неё вероятностей  $p$  устройств У1, У2, ИК и МП.

\*\*  $\Phi(111/0) = 0$ . Здесь, несмотря на работоспособность У1, У2 и ИК, сигнал о восприятии этими датчиками нарушителя не будет далее обработан устройством МП ввиду состояния его неработоспособности, т. е. при определении  $\Phi(111/0)$  по формуле (4.10) необходимо принять  $p_{МП} = 0$ .

\*\*\*  $\Phi(110/1)$  определяется по формуле (4.10), но в этом случае сигнал о проникновении нарушителя датчиком ИК не будет воспринят ввиду состояния его неработоспособности, т. е. для определения  $\Phi(110/1)$  в формуле (4.10) необходимо принять  $p_{ИК} = 0$ .

\*\*\*\*  $\Phi(011/1)$  определяется по формуле (4.10). Здесь сигнал о проникновении нарушителя не будет воспринят датчиком У1 ввиду состояния его неработоспособности, т. е. при определении  $\Phi(011/1)$  по формуле (4.10) необходимо принять  $p_{У1} = 0$ .

$r(j)$ ,  $[1 - r(j)]$  – вероятность работоспособного и вероятность неработоспособного состояний в любой момент времени  $j$ -го устройства подсистемы «Два окна – комната»,  $j \rightarrow У1, У2, ИК, МП$ .

Отметим, что для всех состояний вида (.../0) условный коэффициент эффективности  $\Phi_i$  подсистемы «Два окна – комната» равен нулю, независимо от состояния работоспособности датчиков У1, У2 и ИК, т. к. при отказе устройства МП сигналы о проникновении нарушителя (если они получены) не могут быть обработаны устройством МП.

Показатель эффективности функционирования  $k$ -й подсистемы «Два окна – комната» ( $k = 1, 2$ ), т. е. подсистем, обеспечивающих защиту больших комнат, имеющих два окна, определяется формулой

$$E_{оок} = \sum_{i=1}^{16} h_i \Phi_i. \quad (4.11)$$

Заканчивая рассмотрение выделенных подсистем, отметим, что показатель эффективности их функционирования ( $E_T, E_{дк}, E_{ок}, E_{оок}$ ) представляет собой вероятность защиты помещения (коридора или комнаты) с помощью данной подсистемы.

#### 4.3.6. Определение показателя эффективности функционирования ЭСБ в целом

В качестве показателя эффективности функционирования ЭСБ используется полная вероятность того, что защита ресурсов, хранящихся в комнатах

здания, будет обеспечена. Для этого факт проникновения нарушителя на объект должен быть воспринят хотя бы одним из датчиков, обработан устройствами МП и/или ВР и далее передан операторам (Оп) для ликвидации угрозы.

Очевидным является то, что вероятности того, что нарушитель попытается проникнуть через ту или иную сторону здания будут разные. Так, вероятности того, что нарушитель попытается проникнуть через фасадную часть здания (условно сторону «Юг») или двор, к которому примыкает помещение охраны, заметно меньше, нежели вероятности, соответствующие другим сторонам.

Используя формулу полной вероятности, показатель эффективности функционирования ЭСБ ( $E$ ) можно записать в виде

$$E = P(A) = p_{\text{зап}}p(A/\text{зап}) + p_{\text{сев}}p(A/\text{сев}) + \\ + p_{\text{двор}}p(A/\text{двор}) + p_{\text{вост}}p(A/\text{вост}) + p_{\text{юг}}p(A/\text{юг}), \quad (4.12)$$

где  $A$  – событие, состоящее в том, что защита ресурсов, хранящихся в комнатах здания, будет обеспечена;

$p(A/l)$  – вероятность события  $A$  при условии, что нарушитель попытается проникнуть в комнату через  $l$ -ю сторону,  $l \rightarrow$  запад, север, двор, восток, юг;

$p_l$  – вероятность того, что нарушитель попытается проникнуть в комнату через  $l$ -ю сторону (вероятности гипотез),  $l \rightarrow$  запад, север, двор, восток, юг, причём должно выполняться условие

$$p_{\text{зап}} + p_{\text{сев}} + p_{\text{двор}} + p_{\text{вост}} + p_{\text{юг}} = 1. \quad (4.13)$$

Покажем, как определять вероятности вида  $p(A/l)$ . Вначале рассмотрим сторону «Запад». Защита с этой стороны будет обеспечена в случае защиты комнат, окна которых выходят на запад. Согласно принятым допущениям, привлекательности окон для проникновения в здание с конкретной рассматриваемой стороны одинаковы. Поэтому с учётом числа комнат и количества в них окон формула вероятности  $p(A/\text{зап})$  запишется в виде

$$p(A/\text{зап}) = (4/6)E_{\text{ок}} + (2/6)E_{\text{оок}}, \quad (4.14)$$

где  $E_{\text{ок}}$  – показатель эффективности функционирования подсистемы типа «Окно – комната»;

$E_{\text{оок}}$  – показатель эффективности функционирования подсистемы типа «Два окна – комната».

Числа 4/6 и 2/6, стоящие перед показателями эффективности  $E_{\text{ок}}$  и  $E_{\text{оок}}$ , представляют собой вероятности событий (гипотез), состоящих в том, что для проникновения нарушитель выберет комнату, имеющую соответственно одно или два окна.

Со стороны «Север» одинакова привлекательность тамбуров для проникновения в здание с этой стороны. Одинаковы также привлекательности комнат

для проникновения из конкретного коридора (после прохождения соответствующего тамбура).

Согласно принятому в работе допущению, одиночные нарушители или их группы в конкретный момент времени пытаются проникнуть в здание в одном месте. Поэтому схема соединения подсистем «Тамбур» и «Дверь – комната» с точки зрения защиты ресурсов со стороны «Север» примет вид, показанный на рис. 4.11.

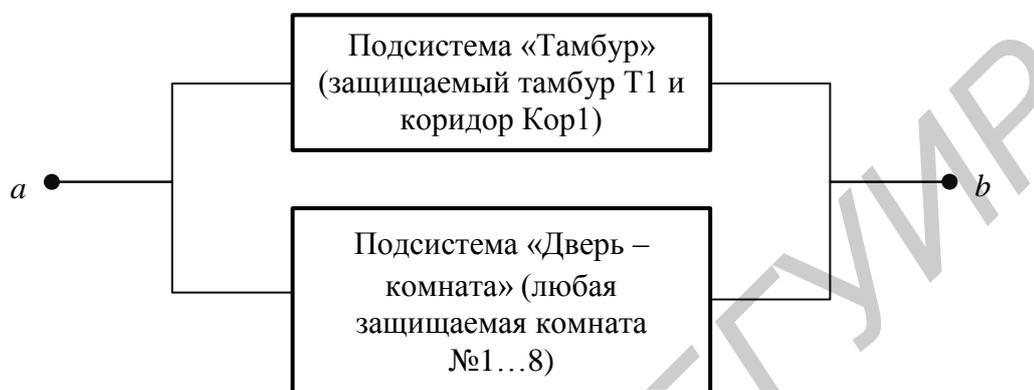


Рис. 4.11. Схема (модель) соединения подсистем с точки зрения обеспечения защиты объекта со стороны «Север»

На рис. 4.11 показана схема соединения подсистем «Тамбур» и «Дверь – комната» применительно к левой части здания стороны «Север». Аналогичная схема соединения справедлива также для подсистем «Тамбур» и «Дверь – комната» для правой части здания стороны «Север» (для тамбура Т2, коридора Кор3 и любой из комнат №17...24). Для получения формулы расчёта вероятности того, что защита объекта со стороны «Север» будет обеспечена, может быть использована любая из схем.

Согласно теоремам теории вероятностей и с учётом схемы (см. рис. 4.11) формула расчёта вероятности защиты объекта со стороны «Север» запишется в виде

$$p(A/\text{север}) = 1 - (1 - E_T)(1 - E_{\text{дк}}). \quad (4.15)$$

Аналогично, принимая во внимание указанные допущения, можно записать формулы расчёта вероятностей того, что защита объекта будет обеспечена со стороны «Двор» и стороны «Восток»:

$$p(A/\text{двор}) = E_{\text{ок}}; \quad (4.16)$$

$$p(A/\text{вост}) = (4/6)E_{\text{ок}} + (2/6)E_{\text{оок}}. \quad (4.17)$$

С учётом принятых в работе допущений схема соединения подсистем «Тамбур», «Дверь – комната» и «Окно – комната» с точки зрения защиты ресурсов со стороны «Юг» имеет вид, показанный на рис. 4.12.

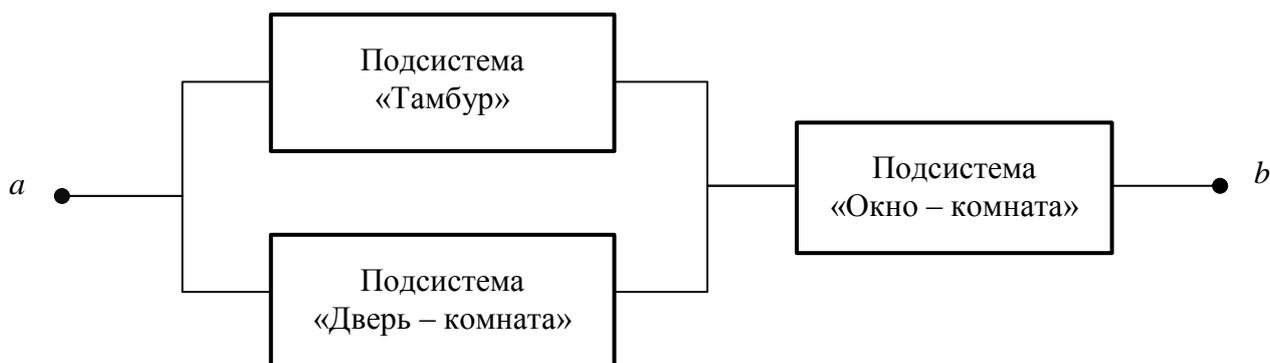


Рис. 4.12. Схема (модель) соединения подсистем с точки зрения обеспечения защиты объекта со стороны «Юг»

Формула расчёта вероятности защиты объекта со стороны «Юг» запишется в виде

$$p(A/\text{Юг}) = [1 - (1 - E_T)(1 - E_{\text{дк}})] E_{\text{ок}}. \quad (4.18)$$

#### 4.4. Задания на экспериментальную часть лабораторной работы

1. Ознакомиться со схемой объекта (здания).

2. Осмыслить возможные пути несанкционированного проникновения в помещения здания с учётом указанных допущений, принимаемых при анализе функционирования ЭСБ.

3. Уточнить подсистемы, на которые разбивается ЭСБ, и устройства, входящие в состав подсистем. По схеме здания ознакомиться с местами расположения устройств в различных помещениях здания:

- датчиков в тамбурах и комнатах здания;
- видеокамер в коридорах (рассматриваются как разновидности датчиков);
- устройств МП, ВР и ПУ в помещении охраны.

Каналы передачи информации от датчиков и видеокамер к устройствам МП, ВР с точки зрения работоспособности и вероятностей правильной передачи сигналов о проникновении условно включены в состав соответствующих датчиков и видеокамер.

Ознакомиться с выделяемыми подсистемами «Тамбур» (4 единицы), «Дверь – комната» (24 единицы), «Окно – комната» (22 единицы) и «Два окна – комната» (2 единицы).

4. Выполнить анализ подсистемы «Тамбур», для чего:

4.1. Выделить для анализа подсистему «Тамбур», нажав соответствующую кнопку на панели управления главной страницы программы для ЭВМ. Ознакомиться с составными частями подсистемы «Тамбур».

4.2. Ознакомиться с расположением датчиков М на дверях тамбура. Рекомендуется также ознакомиться с принципом работы и конструкциями датчиков, используя кнопки справки на панели управления программы для ЭВМ.

4.3. Ознакомиться с расположением видеокамер в коридорах. Рекомендуется также ознакомиться с принципом работы и конструкциями видеокамер, используя соответствующие кнопки справки.

4.4. С помощью кнопок на панели управления для подсистемы «Гамбург» получить возможные её состояния с указанием символических обозначений состояний подсистемы и состояний работоспособности её составных частей (см. табл. 4.3).

4.5. Уточнить состояние подсистемы, для которого необходимо путём расчёта по формулам (см. табл. 4.3) получить вероятность состояния  $h_i$  и соответствующий этому состоянию коэффициент эффективности  $\Phi_i$ . Рассчитать необходимые характеристики с погрешностью до четвертого знака после запятой и ввести их в ЭВМ, пользуясь справочной информацией (прил. 3). Если характеристики определены правильно, то значения характеристик для остальных состояний подсистемы будут подсчитаны автоматически по алгоритму работы программы для ЭВМ.

4.6. Нажатием нужной кнопки на панели управления получить значение показателя эффективности функционирования подсистемы «Гамбург». Осмыслить значение этого показателя.

**5.** Выполнить анализ подсистемы «Дверь – комната», для чего:

5.1. Выделить для анализа подсистему «Дверь – комната», нажав соответствующую кнопку на панели управления главной страницы программы для ЭВМ. Ознакомиться с составными частями подсистемы «Дверь – комната».

5.2. Ознакомиться с расположением датчиков М и ИК на двери и стене. Рекомендуется также ознакомиться с принципом работы и конструкциями датчиков, используя кнопки справки на панели управления программы для ЭВМ.

5.3. С помощью кнопок на панели управления для подсистемы «Дверь – комната» получить возможные её состояния с указанием символических обозначений состояний подсистемы и состояний работоспособности её составных частей (см. табл. 4.4).

5.4. Уточнить состояние подсистемы, для которого необходимо путём расчёта получить вероятность состояния  $h_i$  и соответствующий этому состоянию коэффициент эффективности  $\Phi_i$ . Для расчёта следует воспользоваться формулами табл. 4.4, а далее следовать указаниям программы для ЭВМ.

5.5. Нажатием нужной кнопки на панели управления получить значение показателя эффективности функционирования подсистемы «Дверь – комната». Осмыслить значение этого показателя.

**6.** Выполнить анализ подсистемы «Окно – комната», для чего:

6.1. Выделить для анализа подсистему «Окно – комната», нажав соответствующую кнопку на панели управления главной страницы программы для ЭВМ. Ознакомиться с составными частями подсистемы «Окно – комната».

6.2. Ознакомиться с расположением датчиков У и ИК на окне и стене. Рекомендуется также ознакомиться с принципом работы и конструкциями датчиков, используя кнопки справки на панели управления программы для ЭВМ.

6.3. С помощью кнопок на панели управления для подсистемы «Окно – комната» получить возможные состояния подсистемы с указанием символических обозначений состояний подсистемы и состояний работоспособности её составных частей (см. табл. 4.5).

6.4. Уточнить состояние подсистемы, для которого необходимо путём расчёта получить вероятность состояния  $h_i$  и соответствующий этому состоянию коэффициент эффективности  $\Phi_i$ . Для расчёта следует воспользоваться формулами табл. 4.5, а далее следовать указаниям программы для ЭВМ.

6.5. Нажатием нужной кнопки на панели управления получить значение показателя эффективности функционирования подсистемы «Окно – комната». Осмыслить значение этого показателя.

7. Выполнить анализ подсистемы «Два окна – комната», для чего:

7.1. Выделить для анализа подсистему «Два окна – комната», нажав соответствующую кнопку на панели управления главной страницы программы для ЭВМ. Ознакомиться с составными частями этой подсистемы.

7.2. Ознакомиться с расположением датчиков У и ИК на окнах и стене. Рекомендуется также ознакомиться с принципом работы и конструкциями датчиков, используя кнопки справки на панели управления программы для ЭВМ.

7.3. С помощью кнопок на панели управления для подсистемы «Два окна – комната» получить возможные её состояния с указанием символических обозначений состояний подсистемы и состояний работоспособности её составных частей (см. табл. 4.6).

7.4. Уточнить состояние подсистемы, для которого необходимо путём расчёта получить вероятность состояния  $h_i$  и соответствующий этому состоянию коэффициент эффективности  $\Phi_i$ . Для расчёта следует воспользоваться формулами табл. 4.6, а далее следовать указаниям программы для ЭВМ.

7.5. Нажатием нужной кнопки на панели управления получить значение показателя эффективности функционирования подсистемы «Два окна – комната». Осмыслить значение этого показателя.

8. Определить показатель эффективности функционирования ЭСБ в целом, для чего:

8.1. Находятся вероятности защиты объекта (вероятности события  $A$ ) при условии, что нарушитель попытается проникнуть в здание через  $l$ -ю сторону,  $l \rightarrow$  запад, север, двор, восток, юг (этап 5 на главном окне учебной программы для ЭВМ). Для определения этих вероятностей используются формулы (4.14)–(4.18). Конкретная сторона, для которой выполняется расчёт студентом, указывается программой для ЭВМ.

8.2. Рассматривая студентов бригады в качестве экспертов, определить прогнозные значения привлекательности для нарушителя в процентах той или иной стороны здания и ввести их в ЭВМ (этап 6 на главном окне учебной программы для ЭВМ). Вероятности  $p_l$  того, что нарушитель попытается проникнуть в здание через  $l$ -ю сторону,  $l \rightarrow$  юг (фасадная часть), запад, север, двор, восток далее рассчитываются автоматически программой для ЭВМ с учётом обеспечения условия

$$p_{\text{зап}} + p_{\text{сев}} + p_{\text{двор}} + p_{\text{вост}} + p_{\text{юг}} = 1.$$

8.3. Определить показатель эффективности функционирования ЭСБ в целом ( $E$ ) и осмыслить его суть. Для расчёта используется формула (4.12)

$$E = P(A) = p_{\text{зап}}p(A/\text{зап}) + p_{\text{сев}}p(A/\text{сев}) + p_{\text{двор}}p(A/\text{двор}) + p_{\text{вост}}p(A/\text{вост}) + p_{\text{юг}}p(A/\text{юг}).$$

**9.** Выяснить, как изменится показатель эффективности функционирования ЭСБ, если в подсистемах «Дверь – комната» отказаться от использования датчиков  $M$  на дверях комнат. Для ответа на вопрос необходимо:

– при оценке вероятностей возможных состояний  $h_i$  учесть, что в состав подсистемы «Дверь – комната» входит на одно меньшее количество устройств, в данном случае два: ИК и МП;

– при определении коэффициентов эффективности технических состояний  $\Phi_i$  формулу (4.4), используемую для расчёта вероятности обнаружения нарушителя ( $p_{\text{дк}}$ ) при попытке проникновения в комнату через дверь, преобразовать с учётом  $p_M = 0$ .

**10.** Сделать выводы о возможности отказа от использования магнитоконтактных датчиков  $M$  в подсистемах «Дверь – комната».

*Примечания:*

1. Для выполнения заданий 9 и 10 преподавателем могут быть указаны и другие подсистемы, в которых предполагается отказаться от использования того или иного вида датчика, либо дополнительно установить какой-либо вид датчика и выяснить, как при этом изменится показатель эффективности функционирования ЭСБ в целом.

2. Расчётно-аналитические методы, используемые при выполнении заданий 4...7 для оценки эффективности функционирования подсистем, на которые разбивается исследуемая ЭСБ, могут рассматриваться на практических занятиях с выдачей студентам индивидуальных заданий в соответствии с вариантами, указанными в табл. П.3.1 (прил. 3). При выполнении заданий необходимо принять во внимание результаты тестового расчёта, приведённые в табл. П.3.2 (прил. 3).

#### 4.5. Содержание отчёта

1. Формулировка цели лабораторной работы.

2. Схемы подсистем, на которые разбивалась исследуемая ЭСБ, значения показателя эффективности функционирования каждой подсистемы, вероятностей восприятия (правильной обработки) сигнала и вероятностей работоспособного состояния технических частей ЭСБ. Информацию об указанных вероятностях и показателях эффективности функционирования подсистем свести в таблицу.

3. Формулы для определения вероятностей всех состояний одной из подсистем и коэффициентов эффективности, соответствующих состояниям этой подсистемы. Информацию привести в виде таблицы. Конкретная подсистема уточняется у преподавателя.

4. Прогнозные значения вероятностей  $p_l$  того, что нарушитель попытается проникнуть в здание через  $l$ -ю сторону здания (вероятности гипотез),  $l \rightarrow$  запад, север, двор, восток, юг (фасадная часть).

5. Таблица с указанием вероятностей защиты объекта при условии, что нарушитель попытается проникнуть в здание через  $l$ -ю сторону,  $l \rightarrow$  запад, север, двор, восток, юг.

6. Сравнение показателей эффективности функционирования ЭСБ, полученных аналитическим расчётом и методом моделирования на ЭВМ процесса функционирования ЭСБ.

7. Данные, из которых ясно, как изменится показатель эффективности функционирования ЭСБ в целом, если в подсистеме, указанной преподавателем, отказаться от использования того или иного вида датчика, либо установить дополнительно какой-либо вид датчика.

8. Выводы по работе.

*Примечание.* Вероятности, указанные в пп. 4 и 5, свести в одну таблицу.

#### 4.6. Контрольные вопросы

1. Что понимают под методом декомпозиции сложной ЭСБ?

2. Какие задачи позволяет решить метод декомпозиции сложных систем и в каких случаях его применяют?

3. Как связаны между собой показатели эффективности функционирования подсистем и системы в целом, что влияет на эту связь?

4. Как на практике выполняют декомпозицию ЭСБ, что принимают во внимание? Ответ дать применительно к ЭСБ, рассматриваемой в лабораторной работе.

5. Как выбирают (строят) схему соединения датчиков с точки зрения восприятия факта проникновения нарушителя?

6. Какими дополнительно показателями руководствуются при выборе варианта проектного решения, которое является лучшим для сложной ЭСБ с точки зрения показателя эффективности функционирования?

7. Подтвердить справедливость формулы для определения вероятности того, что защита объекта со стороны «Юг» (фасад здания) будет обеспечена – формула (4.18).

8. Чем объясняется расхождение показателей эффективности ЭСБ, полученных аналитическим расчётом и методом моделирования на ЭВМ процесса функционирования ЭСБ?

9. Объясните характер и причины изменения эффективности функционирования ЭСБ для случая, если в подсистеме, указанной преподавателем, отказаться от использования того или иного вида датчика, либо установить дополнительно какой-либо вид датчика.

## Литература

1. Барсуков, В. С. Современные технологии безопасности / В. С. Барсуков, В. В. Водолазкий. – М. : Нолидж, 2000. – 496 с.
2. Барсуков, В. С. Безопасность: технологии, средства, услуги / В. С. Барсуков. – М. : КУДИЦ – ОБРАЗ, 2001. – 496 с.
3. Ярочкин, В. И. Информационная безопасность : учебник для вузов / В. И. Ярочкин. – 3-е изд. – М. : Академический проект : Трикста, 2005. – 544 с.
4. Боровиков, С. М. Теоретические основы конструирования, технологии и надёжности : учебник для инж.-техн. спец. вузов / С. М. Боровиков. – Минск : Дизайн ПРО, 1998. – 336 с.
5. Надёжность технических систем : справочник / Ю. К. Беляев [и др.] ; под ред. И. А. Ушакова. – М. : Радио и связь, 1985. – 608 с.

Библиотека БГУИР

# ЛАБОРАТОРНАЯ РАБОТА №5

## ВЛИЯНИЕ ВИДА СРЕДСТВ ОБНАРУЖЕНИЯ И МОДЕЛЕЙ НАРУШИТЕЛЕЙ НА ЭФФЕКТИВНОСТЬ ФУНКЦИОНИРОВАНИЯ ЭСБ

### 5.1. Цель работы

На примере ЭСБ, выполняющей функции по защите периметра тепловой электростанции, исследовать влияние заградительных и маскирующих средств обнаружения (СО) на эффективность функционирования ЭСБ с учётом моделей возможных нарушителей.

### 5.2. Краткие теоретические сведения

Для охраны периметра территорий объектов гражданского и специального назначения используют периметровые СО. Они предназначены для сигнализационного блокирования рубежей объектов от несанкционированного вторжения нарушителей. Периметровые СО делят на два вида: заградительные и маскирующие.

Под *заградительным СО* будем понимать средство, устанавливаемое на линии периметра или вблизи неё, явно видимое невооружённым глазом и служащее для выработки сигнала о проникновении нарушителя через периметр охраняемой территории.

Под *маскирующим СО* понимают средство, невидимое для человека за счёт размещения его в грунте или в конструктивных элементах ограды периметра и предназначенное для выработки сигналов о проникновении нарушителей через периметр охраняемой территории.

Основными тактико-техническими характеристиками СО, которые характеризуют его сигнализационную надёжность, являются чувствительность  $V$ , вероятность обнаружения нарушителя  $P_0$  и средняя наработка на ложную тревогу  $T_{л}$ .

Из других тактико-технических характеристик следует отметить следующие:

- длина блокируемого рубежа (протяжённость периметра);
- способность к классификации нарушителей или определению направления их движения;
- энергопотребление;
- погонная стоимость;
- ремонтпригодность.

Основные характеристики СО являются взаимосвязанными. Некоторые из них находятся в противоречивой связи. Например, с повышением чувствительности  $V$  вероятность обнаружения нарушителя  $P_0$  возрастает, а средняя наработка на ложную тревогу  $T_{л}$  уменьшается (т. е. увеличивается количество ложных тревог). Поэтому при разработке или настройке СО обнаружительную способность стараются довести до удовлетворительного уровня ( $P_0 \geq 0,9$ ),

высокого уровня ( $P_0 \geq 0,95$ ), а в некоторых изделиях – до очень высокого уровня ( $P_0 \geq 0,97$ ). При этом большой наработкой на ложную тревогу может считаться величина  $T_n \geq 720$  час [1] или не более одного ложного срабатывания в месяц. Нарботка на ложную тревогу достоверно определяется из долговременных испытаний СО (не менее 3–6 месяцев) в различных природно-промышленных условиях, не выходящих за рамки технических условий. Понятно, например, что ураганный ветер, расшатывающий или даже разрушающий заграждение, наверняка вызовет ложную тревогу установленного на нём вибрационного СО [2].

Информация о физическом принципе работы, месте установки и виде СО, полученная различными путями, может облегчить нарушителю, особенно тренированному, преодолеть зону обнаружения (ЗО) без формирования средством обнаружения сигнала тревоги. Такие случаи будем называть «обходом» СО.

Характеристику СО, описывающую возможность осуществления его «обхода», будем называть «уязвимостью к обходу». «Уязвимость к обходу», несмотря на попытки специалистов её формализации, во многом пока является сравнительной характеристикой «больше/меньше». Любой тип периметровых средств обнаружения в той или иной степени уязвим к «обходу» – меньше ему подвержены маскируемые (невидимые) или малозаметные СО, а также СО пассивного способа обнаружения (не обнаруживаются радиосканерами), обладающие не контактной, а объёмной зоной обнаружения, стелющейся вдоль поверхности без «дыр» или зон пониженной чувствительности. Обычно при описании конкретного СО не упоминаются возможности «обхода», однако в специальной технической литературе обязательно есть ссылки на эти недостатки [3].

Целями нарушителей могут быть случайный или спонтанный интерес, причинение ущерба без мотивации, хищение имущества, нанесение умышленного вреда людям или имуществу, сбор информации об объекте, диверсия и т. д. В соответствии с целями они в различной степени готовятся к преодолению рубежа охраны, чтобы по возможности остаться незамеченными. При этом знание физического принципа работы, места установки или вида СО облегчает нарушителям преодоление зоны обнаружения без выработки тревоги, т. е. осуществление «обхода» СО.

Степень осведомленности нарушителей о системе охраны различна – от незнания или некоторого знакомства до полного знания и тренированности преодоления. Практика показывает, что для анализа ЭСБ, как правило, достаточно выделить четыре типа (модели) нарушителей. Ниже приведено их краткое описание, даны приблизительные оценки и характеристики нарушителей [4, 5].

1. Так называемые «нормальные» или случайные нарушители (обозначим через  $T_1$ ), которые достоверно обнаруживаются в соответствии со сценарием их действий, заложенным в алгоритм обработки информации СО. Только для таких нарушителей обеспечивается вероятность обнаружения, приводимая в тех-

нических условиях на СО. Эти нарушители представляют собой основной, наиболее распространенный тип.

2. Неквалифицированные нарушители ( $T_2$ ), включающие воров, контрабандистов, наркокурьеров. Они имеют представление об установленной охранной сигнализации, что-то читали в технической литературе, поэтому стараются своим поведением снизить, как им кажется, воздействие на СО. Например, уменьшить или увеличить скорость, применить для преодоления попутные средства или материалы (доска, палка). Такие нарушители, не знающие физического принципа работы и типа СО, обнаруживаются, но не столь уверенно, как случайные нарушители.

3. Квалифицированные нарушители ( $T_3$ ), в том числе террористы, бандиты. Они преимущественно хорошо знакомы с системой охраны – информация может быть получена агентурным путем, «зондированием» рубежа. Одиночные нарушители, как правило, имеют специальные технические средства для облегчения преодоления рубежа (стремянка и т. п.) или даже «обхода», например путём подкопа под сигнализационным ограждением. Группа нарушителей может помогать друг другу, например производя «зашумляющие» сигналы. Обнаружение нарушителей такого типа возможно по причине плохой тренированности, неправильной идентификации СО и т. п. Процентный состав таких нарушителей невелик, однако во многих случаях именно с ними отождествляется максимальная реальная угроза объекту.

4. Высококвалифицированные нарушители ( $T_4$ ), включающие разведчиков, диверсантов. Такие нарушители прошли тренировку и полностью осведомлены о СО. Одиночными СО если и обнаруживаются, то крайне неудовлетворительно, по случайным отклонениям от сценария. Устойчивое обнаружение таких нарушителей обеспечивается путём комплексирования рубежа охраны двумя или тремя СО различного физического принципа действия, сконфигурированными в пространстве так, чтобы максимально затруднить «обход». Примером может служить организация охраны периметра военных баз НАТО, стоимость которой превышает 1 000 дол./м:

– первый рубеж охраны – ограждение из колючей проволоки высотой до 4 м с установленным на нём проводно-натяжным СО, дополнительно отсекающее случайных нарушителей и животных, мусор при ветре;

– второй рубеж – радиотехническое двухпозиционное СО, у которого зона обнаружения шириной до 5 м практически примыкает к ограждению с внутренней стороны, либо маскируемое сейсмическое или на основе линии вытекающей волны (ЛВВ), зона обнаружения которых скрыта и распространяется вглубь;

– третий рубеж – сеточное внутреннее ограждение, расположенное в 5–8 м от первого, блокируемое вибрационным либо инфракрасным СО.

Конечно, и эти рубежи периметра теоретически можно преодолеть (глубокий длинный туннель, дельтаплан), но на такие «экзотические» случаи есть противодействие – решение упирается в стоимость единицы длины периметра защиты, которую может себе позволить заказчик.

В табл. 5.1 приводится обобщённая (усреднённая) характеристика различных типов (моделей) нарушителей [5].

Таблица 5.1

Характеристика моделей нарушителей

Обозначение модели нарушителя	Описание нарушителей	Степень осведомленности о системе охраны	Примерный состав нарушителей
$T_1$	Случайные	Не знакомы с системой охраны	Случайные или любопытные люди; хулиганы; люди, находящиеся в алкогольном или наркотическом опьянении; мелкие воры; вандалы; иммигранты
$T_2$	Слабо подготовленные, неквалифицированные	Знакомы по внешним признакам с установленной системой сигнализации	Воры; грабители; контрабандисты; наркокурьеры; нарушители государственной границы
$T_3$	Квалифицированные	Хорошо осведомлены о СО, могут использовать вспомогательные средства	Искусные воры; убийцы; террористы; специалисты, ранее работавшие на объекте
$T_4$	Высококвалифицированные	Полностью осведомлены о СО, прошли тренировку преодоления СО, в том числе с использованием вспомогательных средств	Разведчики; диверсанты; банковские грабители

В табл. 5.2 приводятся типовые значения вероятностей обнаружения нарушителей заградительными и маскирующими СО. В этой же таблице указаны среднестатистические значения вероятностей появления нарушителя на рубеже периметра  $P(T_i)$  при условии, что нарушитель появится обязательно, т. е. при выполнении условия

$$\sum_{i=1}^4 P(T_i) = 1. \quad (5.1)$$

Таблица 5.2

Типичные значения вероятностей обнаружения нарушителей

Тип (модель) нарушителя	Вероятность появления нарушителя на рубеже периметра $P(T_i)$	Вероятность обнаружения нарушителя		Степень потенциального ущерба $k_i$
		заградительные СО	маскирующие СО	
$T_1$	0,6	0,97	0,999	1
$T_2$	0,3	0,6	0,9	30
$T_3$	0,09	0,2	0,5	100
$T_4$	0,01	0,001	0,1	300 и более

Корректная оценка вероятностей  $P(T_i)$  для конкретного объекта очень важна и принимается исходя из специфики объекта, имеющейся статистики зарегистрированных нарушений, окружающей криминальной обстановки, ситуации в регионе и т. д. Например, если 20 лет назад количество вооруженных нарушителей государственной границы России не превышало нескольких процентов, то в настоящее время на южных направлениях их «вклад» увеличился более чем на порядок. Для типичного случая периметровой охраны объекта типа «предприятие», «база», «склад», находящегося в городской черте, можно полагать:  $P(T_1) \approx 0,5-0,8$ ;  $P(T_2) \approx 0,2-0,4$ ;  $P(T_3) \approx 0,05-0,2$ ;  $P(T_4) \approx 0$ .

Коэффициент  $k_i$  характеризует относительный потенциальный ущерб, который могут нанести различные нарушители жизнедеятельности объекта охраны. Ущерб оценивается относительно нарушителя типа  $T_1$ .

Модель нарушителя с точки зрения его проникающей способности и наносимой угрозы, не есть какая-то догма – для разных СО и конкретных объектов она различается, и в ряде случаев весьма существенно. Например, для маскируемого сейсмического СО, блокирующего участок государственной границы на юге России, модель может с наибольшей вероятностью включать вооруженного бандита или контрабандиста, не владеющего достаточными знаниями или техническими средствами для вторжения. Для того же средства, установленного на ядерно-опасном объекте, наиболее вероятной моделью будет разведчик или диверсант, хорошо подготовленный и тренированный для преодоления зоны обнаружения. Во втором случае вероятность обнаружения нарушителя будет существенно меньше, что должно учитываться в общей концепции охраны объекта.

### 5.3. Показатель эффективности функционирования ЭСБ

В качестве объекта защиты рассматривается ЭСБ, выполняющая функции по защите периметра тепловой электростанции. ЭСБ в своём составе в качестве датчиков может содержать заградительные и/или маскирующие СО.

В качестве показателя эффективности функционирования ЭСБ рассматриваются средние потери (затраты), обусловленные стоимостью используемых СО в составе ЭСБ и возникающим ущербом в случае проникновения нарушителя на территорию электростанции. Используется следующее математическое выражение:

$$E = R_{\text{ср}} + C_{\text{ЭСБ}} = p_1 q_1 C_1 + p_2 q_2 C_2 + p_3 q_3 C_3 + p_4 q_4 C_4 + C_{\text{ЭСБ}}, \quad (5.2)$$

где  $E$  – показатель эффективности функционирования ЭСБ;

$R_{\text{ср}}$  – средний риск, обусловленный вероятностями проникновения нарушителя того или иного типа и возможным ущербом, возникающим в случае проникновения нарушителя;

$C_{\text{ЭСБ}}$  – стоимость ЭСБ, включающая только стоимость использованных СО в проекте ЭСБ;

$p_1, p_2, p_3, p_4$  – вероятность появления на рубеже периметра нарушителя соответственно типа  $T_1, T_2, T_3$  и  $T_4$  (вероятности вида  $P(T_i)$  в выражении (5.1));

$q_1, q_2, q_3, q_4$  – вероятность необнаружения всеми СО, входящими в состав ЭСБ (вероятность «обхода» СО), соответственно нарушителя типа  $T_1, T_2, T_3$  и  $T_4$ .

#### 5.4. Описание программы для ЭВМ

Пользователю программы для ЭВМ представлен фотоснимок электростанции сверху. Для просмотра периметра электростанции рекомендуется в п. 1 «Состав СО» первого этапа выбрать «Только заградительные (включая реку и её берега)». Охраняемый периметр включает территорию электростанции и автомобильную стоянку работников. Для охраны стоянки используются только заградительные СО. Для защиты периметра самой электростанции может использоваться один или два рубежа. При использовании двух рубежей защиты периметра снаружи устанавливаются заградительные СО, а внутри территории – маскирующие СО. Периметр территории электростанции с западной стороны проходит вдоль реки. С этой стороны могут использоваться или не использоваться СО.

На первом этапе пользователю предоставлена возможность выбрать состав используемых СО для защиты периметра электростанции: заградительные или маскирующие, либо и те и другие. При этом со стороны реки СО могут использоваться либо не использоваться.

На втором этапе пользователем должны быть указаны привлекательности направления (стороны) для проникновения того или иного типа нарушителя. Причём с восточной стороны выделены два направления «Восток 1» и «Восток 2», которые разделены автостоянкой и подъездной дорогой. Привлекательности указываются в процентах от нуля до ста. Ноль соответствует случаю, когда направление нарушителем данного типа практически не будет выбираться, а значение, равное 100 %, соответствует максимальной привлекательности. Подсчёт вероятностей вида  $P(T_i/H)$  и обеспечение условия (5.1) программа выполняет автоматически. В роли экспертов, прогнозирующих привлекательность направления для нарушителей, выступают студенты бригады, выполняющей лабораторную работу.

Количественное определение показателя эффективности функционирования ЭСБ выполняется путём обработки результатов моделирования процесса функционирования ЭСБ, включающих заданное число реализаций. Реализацией будем считать движение нарушителя с той или иной стороны и соответствующую реакцию на это СО, включённых в состав ЭСБ.

Используемая программа для ЭВМ позволяет пользователю выполнить некоторые вспомогательные действия:

- уточнить характеристику моделей нарушителей;

- просмотреть информацию по выбранным заградительным и/или маскирующим СО;
- ознакомиться с математическим видом показателя эффективности функционирования ЭСБ;
- выйти в режим справки и получить доступ к её следующим разделам: *Ход работы, Каталог заградительных СО, Каталог маскирующих СО, Характеристика видов нарушителей, О программе...*;
- визуально просмотреть анимации попыток проникновения нарушителя на территорию электростанции и реакцию ЭСБ на эти попытки;
- вывести результаты моделирования на печать; таблица результатов включает следующую информацию: номер итерации (реализации, попытки проникновения на территорию), тип нарушителя, направление, сведения об обнаружении или необнаружении нарушителя с помощью используемых СО, нанесённый ущерб в случае проникновения нарушителя на электростанцию;
- сохранить результаты моделирования в Microsoft Excel.

### **5.5. Задания на экспериментальную часть лабораторной работы**

- 1.** Ознакомиться со схемой объекта и его охраняемым периметром. Для просмотра периметра электростанции рекомендуется на первом этапе выбрать «Пункт 1. Состав СО», а в нём в качестве состава СО указать «Только заградительные (включая реку и её берега)».
- 2.** Осмыслить возможные пути несанкционированного проникновения нарушителя на территорию электростанции.
- 3.** Ознакомиться с показателем эффективности функционирования ЭСБ и его математическим видом.
- 4.** Используя студентов бригады в качестве экспертов, указать прогнозные значения привлекательностей каждого направления (пять направлений) с учётом моделей нарушителей.
- 5.** С привлечением полученных выше результатов экспериментально (моделированием на ЭВМ) исследовать влияние на эффективность функционирования ЭСБ различных сочетаний состава заградительных и маскирующих СО из числа, указанных в «Пункт 1. Состав СО». Исследованию подлежат все сочетания СО, к которым имеется доступ в программе.
- 6.** Путём анализа выяснить наиболее эффективный состав СО из числа исследованных.
- 7.** Экспериментально (моделированием на ЭВМ) выяснить, какой тип заградительных СО является наиболее эффективным для рассматриваемой ЭСБ.
- 8.** Моделированием на ЭВМ выяснить, какой тип маскирующих СО является наиболее эффективным для рассматриваемой ЭСБ.

## 5.6. Содержание отчёта

1. Формулировка цели лабораторной работы.
2. Математический вид показателя эффективности функционирования ЭСБ и пояснение его смысла.
3. Таблица с указанием модели нарушителя, вероятностей его появления на рубеже периметра, вероятностей обнаружения заградительными и маскирующими СО, коэффициента  $k_i$ , характеризующего относительный потенциальный ущерб, который могут нанести различные нарушители жизнедеятельности объекта охраны (см. главное окно программы для ЭВМ).
4. Таблица прогнозных значений привлекательностей для нарушителя различных направлений движения к периметру с учётом его модели (в процентах).
5. Таблица, включающая состав СО, используемых в составе ЭСБ, и значения показателя эффективности функционирования системы.
6. Таблица сравнительной эффективности заградительных и маскирующих СО из числа тех, которые включены в учебную программу для ЭВМ.
7. Вывод о составе СО, который целесообразно использовать для охраны периметра электростанции.

## 5.7. Контрольные вопросы

1. Что понимают под заградительным и маскирующим СО?
2. Назовите основные тактико-технические характеристики СО, которые характеризуют его обнаружительную способность (сигнализационную надёжность).
3. Что понимают под зоной обнаружения СО?
4. Какую информацию о СО содержит характеристика, называемая «уязвимость к обходу»?
5. Чем объясняется более высокая обнаружительная способность маскирующих СО в сравнении с заградительными СО?
6. Дайте характеристику используемым на практике моделям нарушителей.
7. В чём состоит смысл показателя эффективности функционирования ЭСБ, используемого в лабораторной работе?
8. Как практически можно оценить значения условных вероятностей появления нарушителя того или иного типа (модели) на рубеже периметра?
9. Поясните смысл численных значений коэффициента  $k_i$ , учитывающего степень потенциального ущерба функционированию электростанции, рассматриваемой в лабораторной работе.
10. Что понимают под итерацией (реализацией) при статистическом моделировании процесса функционирования ЭСБ, предназначенной для защиты периметра электростанции в лабораторной работе?
11. Обоснуйте основные критерии (факторы) выбора состава СО, наиболее эффективного для защиты электростанции, рассматриваемой в лабораторной работе.

## Литература

1. Звежинский, С. С. Проблема выбора периметровых средств обнаружения / С. С. Звежинский // «БДИ». – 2002. – №4 (44). – С. 36–41.
2. Введенский, Б. С. Оборудование для охраны периметров / Б. С. Введенский. – М. : Мир безопасности, 2002. – 112 с.
3. Report TCRP-86-4. Intrusion detection for public transportation facilities handbook. Transit Cooperative Research Program. Washington. 2003, November.
4. Caskey, D. L. Security subsystems application / D. L. Caskey, E. S. Rao // Evaluation guide in general services administration : Carnahan Conference of Security Technology. – IEEE Cat. CH-3031-2/91. – P. 235–245.
5. Звежинский, С. С. О сигнализационной надёжности периметровых средств обнаружения / С. С. Звежинский // «БДИ». – 2004. – №2 (53). – С. 32–38.

Библиотека БГУМР

**ПРОВЕРКА ЗНАЧИМОСТИ КОЭФФИЦИЕНТА КОРРЕЛЯЦИИ**

При нахождении коэффициента корреляции между двумя параметрами число наблюдений пар параметров  $n$  ограничено, поэтому на практике возникает вопрос, насколько правомерно в дальнейшем инженерном анализе можно пользоваться полученной оценкой коэффициента корреляции  $r^*$ .

Для ответа на этот вопрос выполняют проверку статистической значимости (в дальнейшем просто значимости) значения  $r^*$ . Это означает выяснение, за счёт чего оценка  $r^*$  оказалась отличной от нуля: за счёт ограниченности числа наблюдений, т. е. случайных причин, либо за счёт того, что это объективно имеет место.

Проверку значимости коэффициента корреляции выполняют по-разному, в зависимости от числа наблюдений пар параметров. При числе наблюдений  $n > 50$  принимают гипотезу о нормальном распределении оценки  $r^*$ , поскольку доказано, что при  $n > 50$  эта гипотеза, как правило, работает.

Затем строят доверительный интервал, симметричный относительно рассчитанной точечной оценки  $r^*$ . Для коэффициента корреляции его определяют как

$$I_{\gamma}^{(r)} = (r^* - t_{\gamma} \sigma_r; r^* + t_{\gamma} \sigma_r), \quad (\text{П.1.1})$$

где  $t_{\gamma}$  – коэффициент, зависящий от доверительной вероятности  $\gamma$ ;

$\sigma_r$  – среднее квадратическое отклонение коэффициента корреляции, равное

$$\sigma_r \approx \frac{1 - (r^*)^2}{\sqrt{n}}. \quad (\text{П.1.2})$$

Построив доверительный интервал, проверяют, попадает ли в этот интервал точка  $r = 0$ . Если да, то оснований считать значимой оценку коэффициента корреляции нет, т. к. отличной от нуля с вероятностью  $\gamma$  она оказалась за счёт ограниченного числа наблюдений.

Применяя формулу (П.1.1), необходимо помнить, что значения доверительных границ для выборочного коэффициента корреляции по абсолютной величине (модулю) ограничены единицей. Кроме того, следует знать, что примерное равенство (П.1.2) при значениях  $r^*$ , близких к  $\pm 1$ , является весьма грубым.

**Пример П.1.1.** Путём обработки результатов измерений пар параметров  $h_{11Э}$  и  $\beta$  шестидесяти транзисторов типа КТ365А получена точечная оценка коэффициента парной корреляции этих параметров  $r^* = 0,56$ . Требуется дать ответ на вопрос о статистической значимости коэффициента корреляции при значении доверительной вероятности  $\gamma = 0,95$ .

Решение.

1. Для  $\gamma = 0,95$  находим  $t_{\gamma} = 1,96$  [5].

2. По формуле (П.1.2) определяем среднее квадратическое отклонение коэффициента корреляции:

$$\sigma_r = \frac{1 - (r^*)^2}{\sqrt{n}} = \frac{1 - 0,56^2}{\sqrt{60}} \approx 0,09.$$

3. Пользуясь выражением (П.1.1), вычисляем нижнюю  $r_{\text{H}}$  и верхнюю  $r_{\text{B}}$  границы доверительного интервала для коэффициента корреляции:

$$r_{\text{H}} = r^* - t_{\gamma} \sigma_r = 0,56 - 1,96 \cdot 0,09 = 0,38;$$

$$r_{\text{B}} = r^* + t_{\gamma} \sigma_r = 0,56 + 1,96 \cdot 0,09 = 0,74.$$

Тогда доверительный интервал

$$I_{\gamma}^{(r)} = (0,38; 0,74).$$

Так как полученный интервал не содержит точки  $r = 0$ , то с доверительной вероятностью  $\gamma = 0,95$  наличие корреляционной зависимости между исследуемыми параметрами считается доказанным, и значением коэффициента корреляции  $r = 0,56$  можно пользоваться в дальнейшем инженерном анализе.

При  $n < 50$  рассмотренный приём оценки статистической значимости коэффициента корреляции оказывается достаточно грубым. Поэтому при  $n < 50$ , а также в случаях, когда  $|r^*| \rightarrow 1$ , пользуются преобразованием Фишера, определяемым как

$$F = \frac{1}{2} \ln \frac{1 + r^*}{1 - r^*} = \text{arth}(r^*). \quad (\text{П.1.3})$$

Для проверки значимости коэффициента корреляции вначале определяют доверительный интервал для  $F$ :

$$I_{\gamma}^{(F)} = \left( \underbrace{F - t_{\gamma} \sigma_F}_{F_{\text{H}}}; \underbrace{F + t_{\gamma} \sigma_F}_{F_{\text{B}}} \right), \quad (\text{П.1.4})$$

где  $\sigma_F$  – среднее квадратическое отклонение  $F$ .

Фишер показал, что

$$\sigma_F = \frac{1}{\sqrt{n-3}}. \quad (\text{П.1.5})$$

Зная доверительный интервал  $F$ , с помощью обратного преобразования Фишера находят доверительный интервал для коэффициента корреляции:

$$r_{\text{H}} = \text{th}(F_{\text{H}});$$

$$r_{\text{B}} = \text{th}(F_{\text{B}}).$$

При решении практических задач можно пользоваться таблицей значений преобразования Фишера (табл. П.2.1).

**Пример П.1.2.** Исследовалось 12 экземпляров транзисторов типа КТ645А, и была определена точечная оценка коэффициента линейной корреляции между параметрами  $I_{КЭ0}$  (обратный ток коллекторного перехода) и временем до отказа транзистора  $t_0$ . Эта оценка приняла значение  $r^* = -0,66$ . Требуется выяснить, правомерно ли в дальнейшем инженерном анализе пользоваться этой оценкой.

Решение.

1. Так как  $n < 50$ , то воспользуемся преобразованием Фишера. Можно получить

$$F = \text{arth}(r^*) = \text{arth}(-0,66) = -0,79.$$

2. Подсчитываем среднее квадратическое отклонение  $F$ :

$$\sigma_F = \frac{1}{\sqrt{n-3}} = \frac{1}{\sqrt{12-3}} \approx 0,33.$$

3. Выберем  $\gamma = 0,95$ , находим  $t_\gamma = 1,96$  [5].

4. Подсчитываем нижнюю доверительную границу:

$$F_H = F - t_\gamma \sigma_F = -0,79 - 1,96 \cdot 0,33 \approx -1,44.$$

5. Для значения  $F_B$  получим

$$F_B = F + t_\gamma \sigma_F = -0,79 + 1,96 \cdot 0,33 \approx -0,14.$$

6. Определяем нижнюю и верхнюю доверительные границы для коэффициента корреляции:

$$r_H = \text{th}(F_H) = \text{th}(-1,44) \approx -0,89;$$

$$r_B = \text{th}(F_B) = \text{th}(-0,14) \approx -0,14.$$

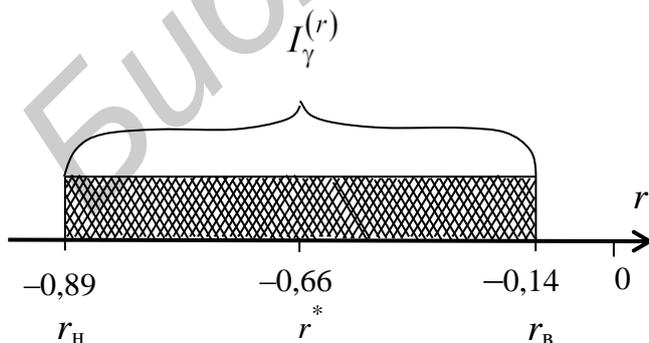


Рис. П.1.1. К определению значимости коэффициента корреляции

7. Проверяем, попадает ли в построенный доверительный интервал для коэффициента корреляции точка со значением  $r = 0$  (рис. П.1.1).

Из рис. П.1.1 видно, что коэффициент корреляции в данном случае значим при доверительной вероятности  $\gamma = 0,95$ . Следовательно, его точечной оценкой  $r^* = -0,66$  можно пользоваться в дальнейшем инженерном анализе.

## ПРИЛОЖЕНИЕ 2

### ПРЕОБРАЗОВАНИЕ ФИШЕРА

Таблица П.2.1

Преобразование Фишера для коэффициента корреляции,  $F = \text{arth}(r)$

$r$	$F$	$r$	$F$	$r$	$F$
0,00	0,000	0,34	0,354	0,68	0,8290
0,01	0,010	0,35	0,365	0,69	0,8480
0,02	0,020	0,36	0,376	0,70	0,8670
0,03	0,030	0,37	0,388	0,71	0,8870
0,04	0,040	0,38	0,400	0,72	0,9070
0,05	0,050	0,39	0,411	0,73	0,9280
0,06	0,060	0,40	0,423	0,74	0,9500
0,07	0,070	0,41	0,435	0,75	0,9730
0,08	0,080	0,42	0,459	0,76	0,9960
0,09	0,100	0,43	0,459	0,77	1,2030
0,10	0,100	0,44	0,472	0,78	1,4540
0,11	0,110	0,45	0,484	0,79	1,7140
0,12	0,120	0,46	0,490	0,80	1,9860
0,13	0,130	0,47	0,510	0,81	1,1270
0,14	0,140	0,48	0,523	0,82	1,1881
0,15	0,151	0,49	0,536	0,83	1,1881
0,16	0,161	0,50	0,549	0,84	1,2212
0,17	0,171	0,51	0,562	0,85	1,2562
0,18	0,182	0,52	0,576	0,86	1,2933
0,19	0,192	0,53	0,590	0,87	1,3331
0,20	0,202	0,54	0,604	0,88	1,3758
0,21	0,213	0,55	0,618	0,89	1,4219
0,22	0,223	0,56	0,632	0,90	1,4722
0,23	0,234	0,57	0,647	0,91	1,5275
0,24	0,244	0,58	0,662	0,92	1,5890
0,25	0,255	0,59	0,667	0,93	1,6584
0,26	0,266	0,60	0,693	0,94	1,7380
0,27	0,276	0,61	0,708	0,95	1,8318
0,28	0,287	0,62	0,725	0,96	1,9433
0,29	0,298	0,63	0,741	0,97	2,0923
0,30	0,309	0,64	0,758	0,98	2,2976
0,31	0,320	0,65	0,775	0,99	2,6467
0,32	0,331	0,66	0,792	0,995	2,9945
0,33	0,342	0,67	0,810	0,999	3,8002

Свойство преобразования:  $\text{arth}(-r) = -F$ .

## ПРИЛОЖЕНИЕ 3

### СПРАВОЧНАЯ ИНФОРМАЦИЯ К ЛАБОРАТОРНОЙ РАБОТЕ №4

Таблица П.3.1

Вероятности восприятия (правильной обработки) сигнала устройствами ЭСБ и вероятности работоспособного состояния (коэффициенты готовности) устройств ЭСБ

Вариант	Устройство подсистемы	М	ВК	ИК	У	МП	ВР
1	Вероятность восприятия сигнала	0,9	0,9	0,9	0,9	1	1
	Вероятность работоспособного состояния	0,9	0,9	0,9	0,9	0,9	0,9
2	Вероятность восприятия сигнала	0,95	0,95	0,95	0,95	1	1
	Вероятность работоспособного состояния	0,95	0,95	0,95	0,95	0,95	0,95
3	Вероятность восприятия сигнала	0,97	0,97	0,97	0,97	1	1
	Вероятность работоспособного состояния	0,97	0,97	0,97	0,97	0,97	0,97
4	Вероятность восприятия сигнала	0,98	0,98	0,98	0,98	1	1
	Вероятность работоспособного состояния	0,98	0,98	0,98	0,98	0,98	0,98
5	Вероятность восприятия сигнала	0,9	0,9	0,9	0,9	1	1
	Вероятность работоспособного состояния	0,9	0,9	0,9	0,9	0,9	0,9
6	Вероятность восприятия сигнала	0,95	0,95	0,95	0,95	1	1
	Вероятность работоспособного состояния	0,95	0,95	0,95	0,95	0,95	0,95
7	Вероятность восприятия сигнала	0,97	0,97	0,97	0,97	1	1
	Вероятность работоспособного состояния	0,97	0,97	0,97	0,97	0,97	0,97
8	Вероятность восприятия сигнала	0,98	0,98	0,98	0,98	1	1
	Вероятность работоспособного состояния	0,98	0,98	0,98	0,98	0,98	0,98
9	Вероятность восприятия сигнала	0,9	0,9	0,9	0,9	1	1
	Вероятность работоспособного состояния	0,9	0,9	0,9	0,9	0,9	0,9
10	Вероятность восприятия сигнала	0,95	0,95	0,95	0,95	1	1
	Вероятность работоспособного состояния	0,95	0,95	0,95	0,95	0,95	0,95
11	Вероятность восприятия сигнала	0,97	0,97	0,97	0,97	1	1
	Вероятность работоспособного состояния	0,97	0,97	0,97	0,97	0,97	0,97
12	Вероятность восприятия сигнала	0,98	0,98	0,98	0,98	1	1
	Вероятность работоспособного состояния	0,98	0,98	0,98	0,98	0,98	0,98
13	Вероятность восприятия сигнала	0,9	0,9	0,9	0,9	1	1
	Вероятность работоспособного состояния	0,9	0,9	0,9	0,9	0,9	0,9
14	Вероятность восприятия сигнала	0,95	0,95	0,95	0,95	1	1
	Вероятность работоспособного состояния	0,95	0,95	0,95	0,95	0,95	0,95
15	Вероятность восприятия сигнала	0,97	0,97	0,97	0,97	1	1
	Вероятность работоспособного состояния	0,97	0,97	0,97	0,97	0,97	0,97
16	Вероятность восприятия сигнала	0,98	0,98	0,98	0,98	1	1
	Вероятность работоспособного состояния	0,98	0,98	0,98	0,98	0,98	0,98
17	Вероятность восприятия сигнала	0,9	0,9	0,9	0,9	1	1
	Вероятность работоспособного состояния	0,9	0,9	0,9	0,9	0,9	0,9
18	Вероятность восприятия сигнала	0,95	0,95	0,95	0,95	1	1
	Вероятность работоспособного состояния	0,95	0,95	0,95	0,95	0,95	0,95
19	Вероятность восприятия сигнала	0,97	0,97	0,97	0,97	1	1
	Вероятность работоспособного состояния	0,97	0,97	0,97	0,97	0,97	0,97

Вариант	Устройство подсистемы	М	ВК	ИК	У	МП	ВР
20	Вероятность восприятия сигнала	0,98	0,98	0,98	0,98	1	1
	Вероятность работоспособного состояния	0,98	0,98	0,98	0,98	0,98	0,98
21	Вероятность восприятия сигнала	0,9	0,9	0,9	0,9	1	1
	Вероятность работоспособного состояния	0,9	0,9	0,9	0,9	0,9	0,9
22	Вероятность восприятия сигнала	0,95	0,95	0,95	0,95	1	1
	Вероятность работоспособного состояния	0,95	0,95	0,95	0,95	0,95	0,95
23	Вероятность восприятия сигнала	0,97	0,97	0,97	0,97	1	1
	Вероятность работоспособного состояния	0,97	0,97	0,97	0,97	0,97	0,97
24	Вероятность восприятия сигнала	0,98	0,98	0,98	0,98	1	1
	Вероятность работоспособного состояния	0,98	0,98	0,98	0,98	0,98	0,98
25	Вероятность восприятия сигнала	0,9	0,9	0,9	0,9	1	1
	Вероятность работоспособного состояния	0,9	0,9	0,9	0,9	0,9	0,9
26	Вероятность восприятия сигнала	0,95	0,95	0,95	0,95	1	1
	Вероятность работоспособного состояния	0,95	0,95	0,95	0,95	0,95	0,95
27	Вероятность восприятия сигнала	0,97	0,97	0,97	0,97	1	1
	Вероятность работоспособного состояния	0,97	0,97	0,97	0,97	0,97	0,97
28	Вероятность восприятия сигнала	0,98	0,98	0,98	0,98	1	1
	Вероятность работоспособного состояния	0,98	0,98	0,98	0,98	0,98	0,98
29	Вероятность восприятия сигнала	0,9	0,9	0,9	0,9	1	1
	Вероятность работоспособного состояния	0,9	0,9	0,9	0,9	0,9	0,9
30	Вероятность восприятия сигнала	0,95	0,95	0,95	0,95	1	1
	Вероятность работоспособного состояния	0,95	0,95	0,95	0,95	0,95	0,95
31	Вероятность восприятия сигнала	0,97	0,97	0,97	0,97	1	1
	Вероятность работоспособного состояния	0,97	0,97	0,97	0,97	0,97	0,97
32	Вероятность восприятия сигнала	0,98	0,98	0,98	0,98	1	1
	Вероятность работоспособного состояния	0,98	0,98	0,98	0,98	0,98	0,98
33	Вероятность восприятия сигнала	0,9	0,9	0,9	0,9	1	1
	Вероятность работоспособного состояния	0,9	0,9	0,9	0,9	0,9	0,9
34	Вероятность восприятия сигнала	0,95	0,95	0,95	0,95	1	1
	Вероятность работоспособного состояния	0,95	0,95	0,95	0,95	0,95	0,95

Таблица П.3.2

Результаты тестового расчёта, все вероятности  $p$  и  $r(j)$  приняты равными 0,9 (кроме вероятностей правильной обработки сигналов устройствами МП и ВР, для которых  $p = 1$ )

Подсистема	«Тамбур»	«Дверь – комната»	«Окно – комната»	«Два окна – комната»
Значение $E$	0,926559	0,86751	0,86751	0,86751

*Учебное издание*

**Боровиков** Сергей Максимович  
**Шнейдеров** Евгений Николаевич  
**Гришель** Рафаил Петрович и др.

**ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОЕКТИРОВАНИЯ  
ЭЛЕКТРОННЫХ СИСТЕМ БЕЗОПАСНОСТИ.  
ЛАБОРАТОРНЫЙ ПРАКТИКУМ**

ПОСОБИЕ

Редактор *Е. С. Чайковская*

Корректор *Е. Н. Батурчик*

Компьютерная правка, оригинал-макет *Е. Г. Бабичева*

Подписано в печать 13.03.2014. Формат 60x84 1/16. Бумага офсетная. Гарнитура «Таймс».  
Отпечатано на ризографе. Усл. печ. л. 4,3. Уч.-изд. л. 4,3. Тираж 100 экз. Заказ 203.

Издатель и полиграфическое исполнение: учреждение образования  
«Белорусский государственный университет информатики и радиоэлектроники».  
Свидетельство о государственной регистрации издателя, изготовителя,  
распространителя печатных изданий №1/238 от 24.03.2014.

ЛП №02330/0494175 от 03.04.2009.

220013, Минск, П. Бровки, 6