

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Локтионова Оксана Геннадьевна

Должность: проректор по учебной работе

Дата подписания: 27.03.2023 15:34:10

Уникальный идентификатор документа: 0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d088

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра информационной безопасности



УТВЕРЖДАЮ

Проректор по учебной работе

О.Г. Локтионова

2022 г.

### Критерии оценки и выбора CASE-Средств

Методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03

Курск 2022

УДК 004.056.55

Составители: О.А. Демченко

Рецензент

Кандидат технических наук, доцент *А.Л. Марухленко*

**Критерии оценки и выбора CASE-Средств:** методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03 / Юго-Зап. гос. ун-т; сост. О.А. Демченко Курск, 2022. - 11 с.

Содержат сведения по вопросам информационной безопасности. Указывается порядок выполнения лабораторной работы, пример выполнения работы, правила оформления, содержание отчета, варианты заданий.

Методические указания разработаны для изучения дисциплин, связанными с безопасностью эксплуатации телекоммуникационных систем.

Текст печатается в авторской редакции

Подписано в печать Формат 60x84 1/16.

Усл.печ. л. \_\_\_\_\_ . Уч.-изд.л \_\_\_\_\_ . Тираж 30 экз. Заказ \_\_\_\_\_.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

## СОДЕРЖАНИЕ

Цель работы	4
Задание	4
Содержание отчета	4
Теоретическая часть	4
Пример выполнения работы	9
Контрольные вопросы	10
Список использованных источников и литературы	10

## **ЦЕЛЬ РАБОТЫ**

Целью лабораторной работы является описание и анализ информационной системы

## **ЗАДАНИЕ**

Необходимо:

1. Составить подробное описание информационной системы.
2. Провести анализ осуществимости.
3. Создать заключение о возможности реализации проекта.
4. Распределить роли в группе.
5. Выяснить проблемы, перспективы организации при вводе или не вводе в эксплуатацию системы .

## **СОДЕРЖАНИЕ ОТЧЕТА**

1. Титульный лист.
2. Краткая теория.
3. Описание выполнения практической работы с изображениями.
4. Полный отчет.
5. Вывод

## **ТЕОРЕТИЧЕСКАЯ ЧАСТЬ**

Критерии формируют базис для процессов оценки и выбора и могут принимать различные формы, включая:

– числовые меры в широком диапазоне значений, например, объем требуемой памяти;

– числовые меры в ограниченном диапазоне значений, например, простота освоения, выраженная в баллах от 1 до 5;

– двоичные меры (истина/ложь, да/нет), например, способность генерации документации в формате Postscript;

– меры, которые могут принимать одно или более из конечных множеств значений, например, платформы, для которых поддерживается CASE-средство.

Типичный процесс оценки и/или выбора может использовать набор критериев различных типов.

Структура набора критериев приведена на рисунке 1. Каждый критерий должен быть выбран и адаптирован экспертом с учетом особенностей конкретного процесса. В большинстве случаев только некоторые из множества описанных ниже критериев оказываются приемлемыми для использования, при этом также добавляются дополнительные критерии. Выбор и уточнение набора используемых критериев является критическим шагом в процессе оценки и/или выбора.

#### *Функциональные характеристики*

Критерии первого класса предназначены для определения функциональных характеристик CASE-средства. Они в свою очередь подразделяются на ряд групп и подгрупп.

##### 1. Среда функционирования:

###### а. Проектная среда:

- *поддержка процессов жизненного цикла.* Определяет набор процессов ЖЦ, которые поддерживает CASE-средство. Примерами таких процессов являются анализ требований, проектирование, реализация, тестирование и оценка, сопровождение, обеспечение качества, управление конфигурацией и управление проектом, причем

они зависят от принятой пользователем модели ЖЦ.

- *область применения.* Примерами являются системы обработки транзакций, системы реального времени, информационные системы и т.д.

- *размер поддерживаемых приложений.* Определяет ограничения на такие величины, как количество строк кода, уровней вложенности, размер базы данных, количество элементов данных, количество объектов конфигурационного управления.

в. ПО/технические средства:

- *требуемые технические средства.* Оборудование, необходимое для функционирования CASE-средства, включая тип процессора, объем оперативной и дисковой памяти.

- *поддерживаемые технические средства.* Элементы оборудования, которые могут использоваться CASE-средством, например, устройства ввода/вывода.

- *требуемое ПО.* ПО, необходимое для функционирования CASE-средства, включая операционные системы и графические оболочки.

- *поддерживаемое ПО.* Программные продукты, которые могут использоваться CASE-средством.

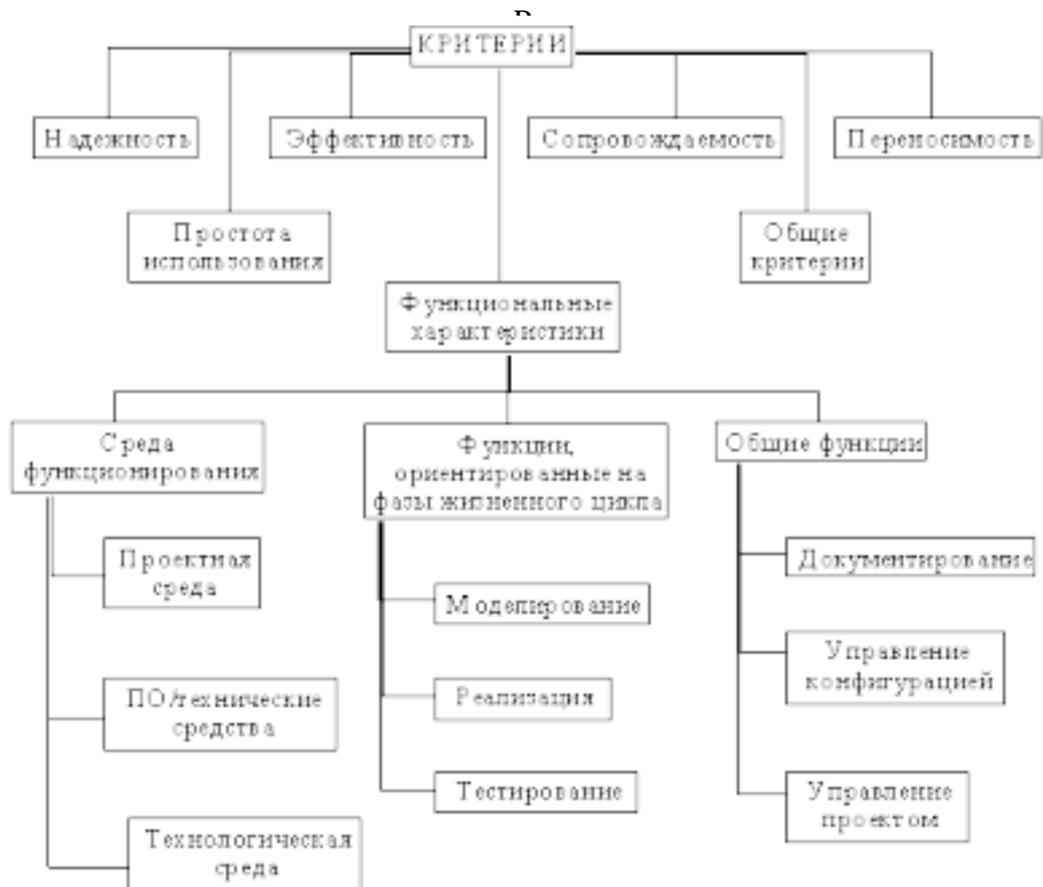


Рис. 1 - Структура набора критериев

Разработка требований — это процесс, включающий мероприятия, необходимые для создания и утверждения документа, содержащего спецификацию системных требований. Для новых программных систем процесс разработки требований должен начинаться с анализа осуществимости. Началом такого анализа является общее описание системы и ее назначения, а результатом анализа — отчет, в котором должна быть четкая рекомендация, продолжать или нет процесс разработки требований проектируемой системы. Другими словами, анализ осуществимости должен осветить следующие вопросы.

1. Отвечает ли система общим и бизнес-целям организации заказчика и организации-разработчика?
2. Можно ли реализовать систему, используя существующие на данный момент технологии и не выходя за пределы заданной стоимости?
3. Можно ли объединить систему с другими системами, которые

уже эксплуатируются?

Критическим является вопрос, будет ли система соответствовать целям организации. Если система не соответствует этим целям, она не представляет никакой ценности для организации. В то же время многие организации разрабатывают системы, не соответствующие их целям, либо не совсем ясно понимая эти цели, либо под влиянием политических или общественных факторов.

Выполнение анализа осуществимости включает сбор и анализ информации о будущей системе и написание соответствующего отчета. Сначала следует определить, какая именно информация необходима, чтобы ответить на поставленные выше вопросы. Например, эту информацию можно получить, ответив на следующее:

1. Что произойдет с организацией, если система не будет введена в эксплуатацию?
2. Какие текущие проблемы существуют в организации и как новая система поможет их решить?
3. Каким образом система будет способствовать целям бизнеса?
4. Требуется ли разработка системы технологии, которая до этого не использовалась в организации?

Далее необходимо определить источники информации. Это могут быть менеджеры отделов, где система будет использоваться, разработчики программного обеспечения, знакомые с типом будущей системы, технологи, конечные пользователи и т.д.

После обработки собранной информации готовится отчет по анализу осуществимости создания системы. В нем должны быть даны рекомендации относительно продолжения разработки системы. Могут быть предложены изменения бюджета и графика работ по созданию системы или предъявлены более высокие требования к системе.

## ПРИМЕР ВЫПОЛНЕНИЯ РАБОТЫ

Необходимо разработать информационную систему для салона видеопроката с целью улучшенного управления деятельностью магазина, занимающихся прокатом видеодисков. ИС позволит регулировать представленную в ходе работы магазина информацию и вести детализированные отчеты.

Требования к системе:

- 1) Хранение каталога всех доступных фильмов с описанием
- 2) Возможность добавления и удаления
- 3) Выдача записей о недоступных на данный момент фильмах
- 4) Хранение данных о выдаче и возврате
- 5) Уведомление о просрочке
- 6) Пользовательский бюджет

Бюджет 150 тыс. Время 3 месяца. Проект может быть реализован в указанные сроки силами небольшой команды разработчиков в рамках заданного бюджета.

Система состоит из двух блоков: сервер базы данных и клиентское приложение для доступа к нему.

Серверная часть может быть реализована средствами современных реляционных СУБД для серверной.

Клиентская часть реализуется средствами современных языков программирования с графическим интерфейсом под ОС Windows.

Организация заказчик нуждается в информационной системе учета арендуемых фильтров.

Система реализуема при помощи современных технологий в рамках заданной стоимости и соответствует потребностям компании-заказчика. Позволяет ускорить взаимодействие с клиентом и улучшить возможности учета, ускорить и упростить процесс менеджмента записей, выдачи и возвращения, хранения записей о клиенте, бронирования.

Проект может осуществлен в течении двух месяцев с дополнительным

месяцем на тестирование.

Следующие сотрудники: руководитель, дизайнер, разработчик БД, разработчик, тестировщик.

Серверная часть проекта реализуется на MySQL, может быть размещена как на локальном, так и на удаленном сервере под управлением различных операционных систем.

Клиентская часть и графический интерфейс реализуется на языке программирования C++ с использованием WinAPI в среде VisualStudio и будут размещены на локальных машинах салона.

### **КОНТРОЛЬНЫЕ ВОПРОСЫ**

1. Какие вопросы включает методика описания проектируемой ИС?
2. На каких уровнях проводится обследование аспектов деятельности предприятия?
3. Какие существуют универсальные методы, пригодные для обследования всех функциональных звеньев предприятия??
4. Какие существуют документы для описания ИС?

### **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ**

1. Петраков В. П., Величко В.В., Субботин Е. А., Ярославцев А.Ф. Телекоммуникационные системы и сети. Том 3. Мультисервисные сети (2005).
2. Петраков А.В. Основы практической защиты информации. 2-е издание Учебное пособие. – М. Радио и связь. 2000. – 368с.
3. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: Учебник для ВУЗов. - СПб.: БХВ-Петербург, 2010. - 400 с.
4. Башарин Г.П. Лекции по математической теории

телетрафика: Учеб. пособие. Изд. 3-е, испр. и доп. - М.: РУДН, 2009. - 342 с.

5. Буч Г. Объектно-ориентированный анализ и проектирование. – М.: Вильямс, 2008.

6. Леоненков А.В. Самоучитель языка UML. – СПб.: БХВ Петербург, 2004.

7. Розенберг Д., Скотт К. Применение объектного моделирования с использованием UML и анализ прецедентов. – М.: ДМК Пресс, 2002.

8. А.В. Росляков. Виртуальные частные сети. Основы построения и применения. - М.: Эко-Трендз, 2006. - 242 с.

# МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра информационной безопасности



## **Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение**

Методические указания по выполнению лабораторной работы

Курск 2017

УДК 621.(076.1)

Составители: В.В. Карасовский, О.А. Демченко

Рецензент

Кандидат технических наук, доцент кафедры  
информационной безопасности *А.Г. Сневаков*

**Оценка показателей качества функционирования комплексной системы защиты информации на предприятии, физическое проникновение:** методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: В.В. Карасовский, О.А. Демченко Курск, 2017.- 16 с.: ил.11, табл. 1 ,Библиогр.: с. 16.

Содержат сведения об администрирование и управление программно-аппаратными средствами контроля и фильтрации сетевых пакетов способами, а так же защиты от несанкционированного доступа к ресурсам персонального компьютера. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Предназначены для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.  
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ . Бесплатно.  
Юго-Западный государственный университет.  
305040, г. Курск, ул. 50 лет Октября, 94.

## СОДЕРЖАНИЕ

Содержание .....	3
1. Цель работы.....	4
2. Оценка вероятности несанкционированного доступа на охраняемый объект .....	4
3. План помещения .....	4
4. Топологическая модель помещения .....	5
5. Расчет вероятностей доступа .....	13
6. Задание на лабораторную работу.....	15
7. Требования к отчету .....	15
8. Контрольные вопросы .....	16
9. Список использованных источников и литературы .....	16

## 1. ЦЕЛЬ РАБОТЫ

Целью данной лабораторной работы является оценка показателей качества функционирования комплексной системы защиты информации на предприятии, расчет защищенности объекта от физического проникновения.

## 2. ОЦЕНКА ВЕРОЯТНОСТИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА ОХРАНЯЕМЫЙ ОБЪЕКТ

Все нарушения единого информационного процесса на предприятии связаны с хищением материальных ценностей: бумажных и электронных носителей информации, компьютеров и периферийного оборудования. Ущерб предприятию может нанести не только потеря материального объекта или информации (предприятие несет убыток в размере рыночной стоимости объекта), но также и модификация или уничтожение объекта информации (предприятие несет убыток в размере упущенной выгоды). Поэтому защиту объекта следует начинать с защиты от самого распространенного способа хищения информации и материальных ценностей- защиты от физического проникновения на охраняемый объект.

## 3. ПЛАН ПОМЕЩЕНИЯ

Первое с чего следует начать защиту охраняемого объекта, это ознакомление с планом объекта защиты, если плана помещения нет, то необходимо его составить.

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

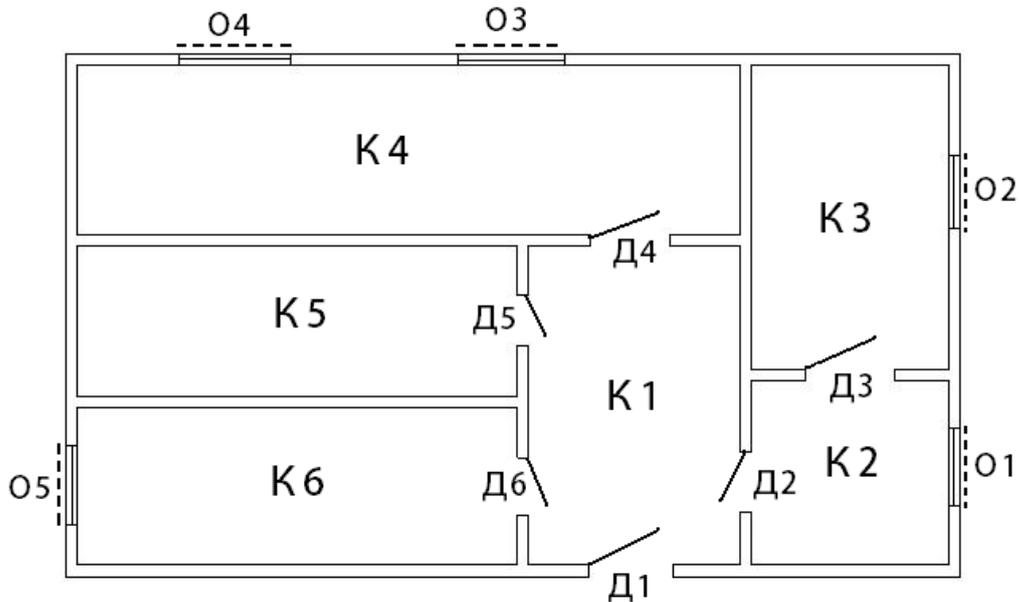


Рис. 1 – План помещений

Как видно из плана, помещение имеет 6 комнат, 6 дверей (1 входная и 5 межкомнатных), 5 окон.

#### 4. ТОПОЛОГИЧЕСКАЯ МОДЕЛЬ ПОМЕЩЕНИЯ

Элементы охраняемого пространства и связи между ними, определяющие возможность перехода из одного элемента в другой или проникновения извне (окон, дверей, переходов и т.д.), выявляются по плану его пространственного размещения. Они могут быть представлены в виде графа представленного на Рисунке 2.

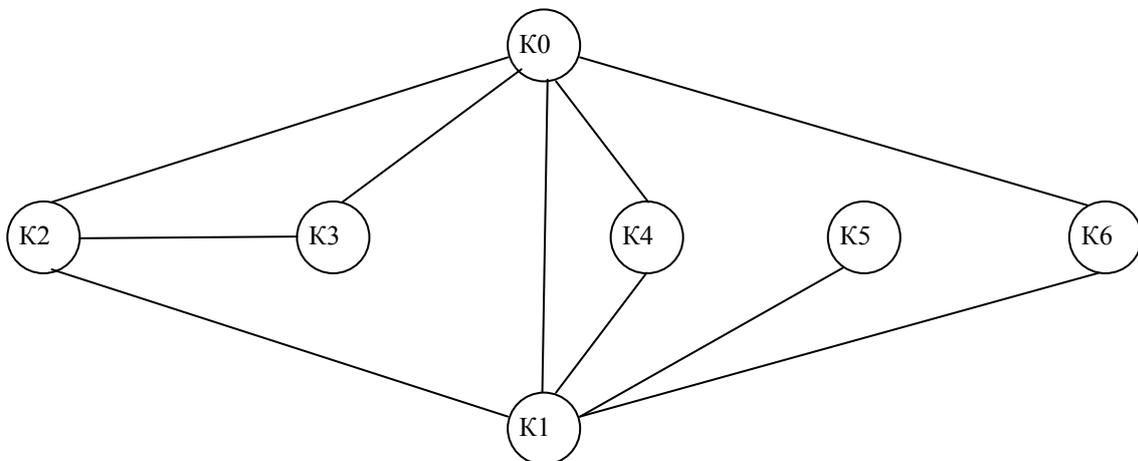


Рис. 2 – Граф путей доступа в помещение

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

Укажем на графе подробно каналы, с помощью которых злоумышленник может проникнуть на объект. Полученный граф изображен на Рис. 3.

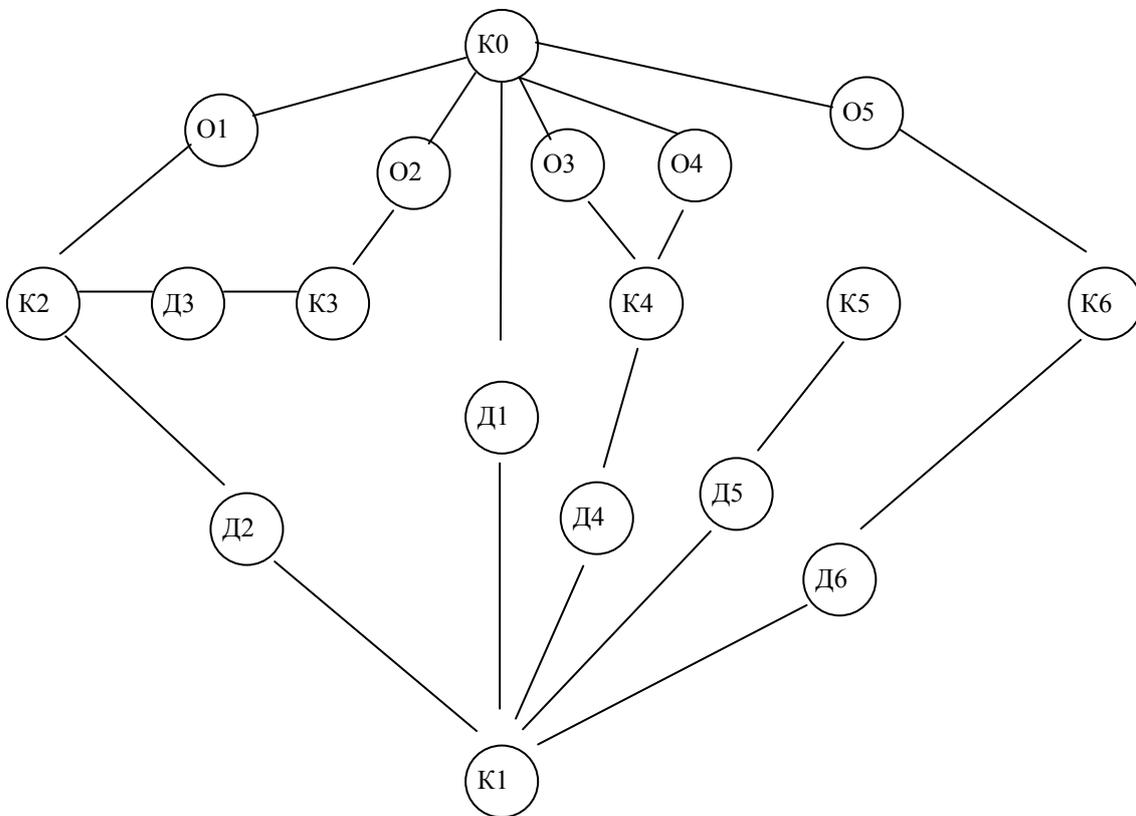


Рис. 3 – Граф путей доступа в помещение через возможные каналы доступа.

При построении графа не учитывались возможные средства защиты от проникновения. При появлении таких средств они будут представлять собой дополнительные вершины. В нашем случае на окнах имеются следующие средства защиты:

- решетки;

- жалюзи;
- датчики разбития стекла.

На входной двери имеется замок и дверь бронирована, а межкомнатные двери оснащены замками. Поэтому появляются барьеры (обозначим их буквой «Б»). В том случае, если на двери нет замка, то соответствующую ей вершину можно удалить из графа, соединив соответствующие комнаты между собой непосредственно. Вершины, соответствующие этим двум комнатам, можно объединить в одну вершину, поскольку доступ в одну из комнат равносителен доступу в другую. Для наглядности примера предположим, что дверь Д2 не имеет замков. Таким образом доступ в помещение К2 равносителен доступу в помещение К1 и наоборот, следовательно вершины К2 и Д2 можно удалить из графа, соединив вершины О1 и К1. С учетом сказанного выше изобразим полученный новый граф на Рис. 4.

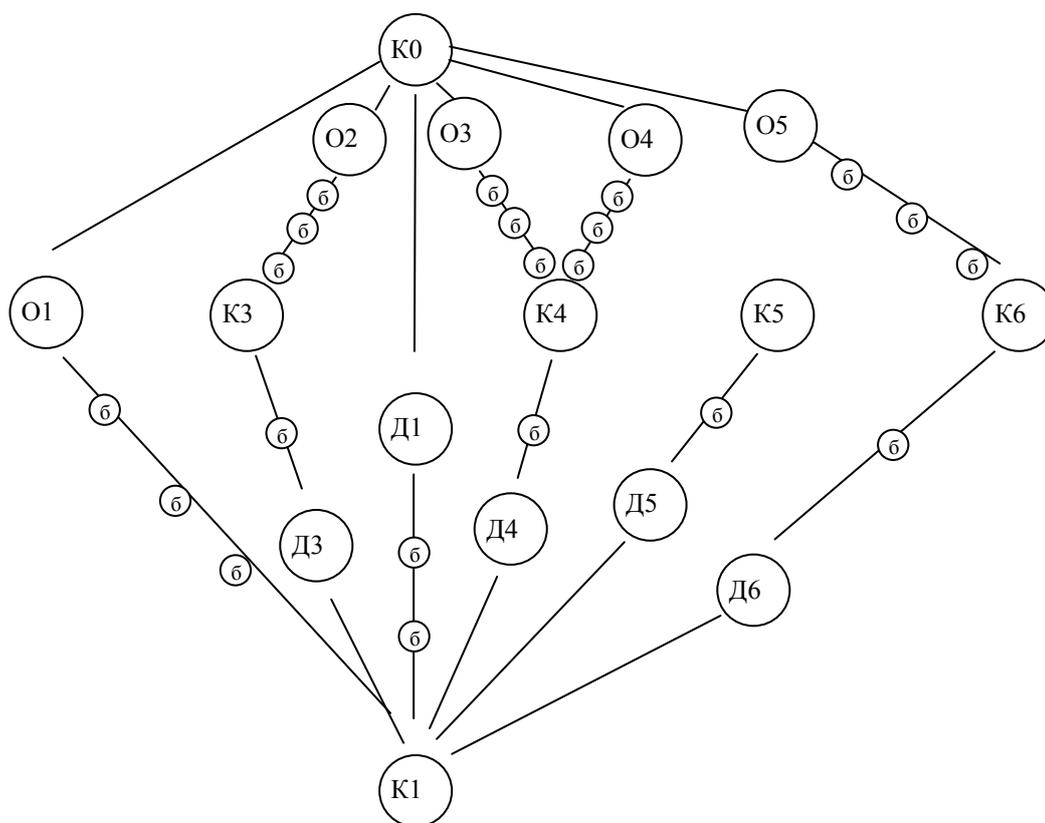


Рис. 4 - Граф путей доступа в помещение через возможные каналы доступа с указанием возможных барьеров.

Преобразуем наш неориентированный граф в ориентированный, каждое ребро при этом распадется на 2 ориентированных ребра направленных к каждой из вершин, соединяемых ими. Это логически понятно, поскольку, если возможен прямой переход из одной вершины в другую, то также возможен и обратный переход. Получим граф, изображенный на рис. 5

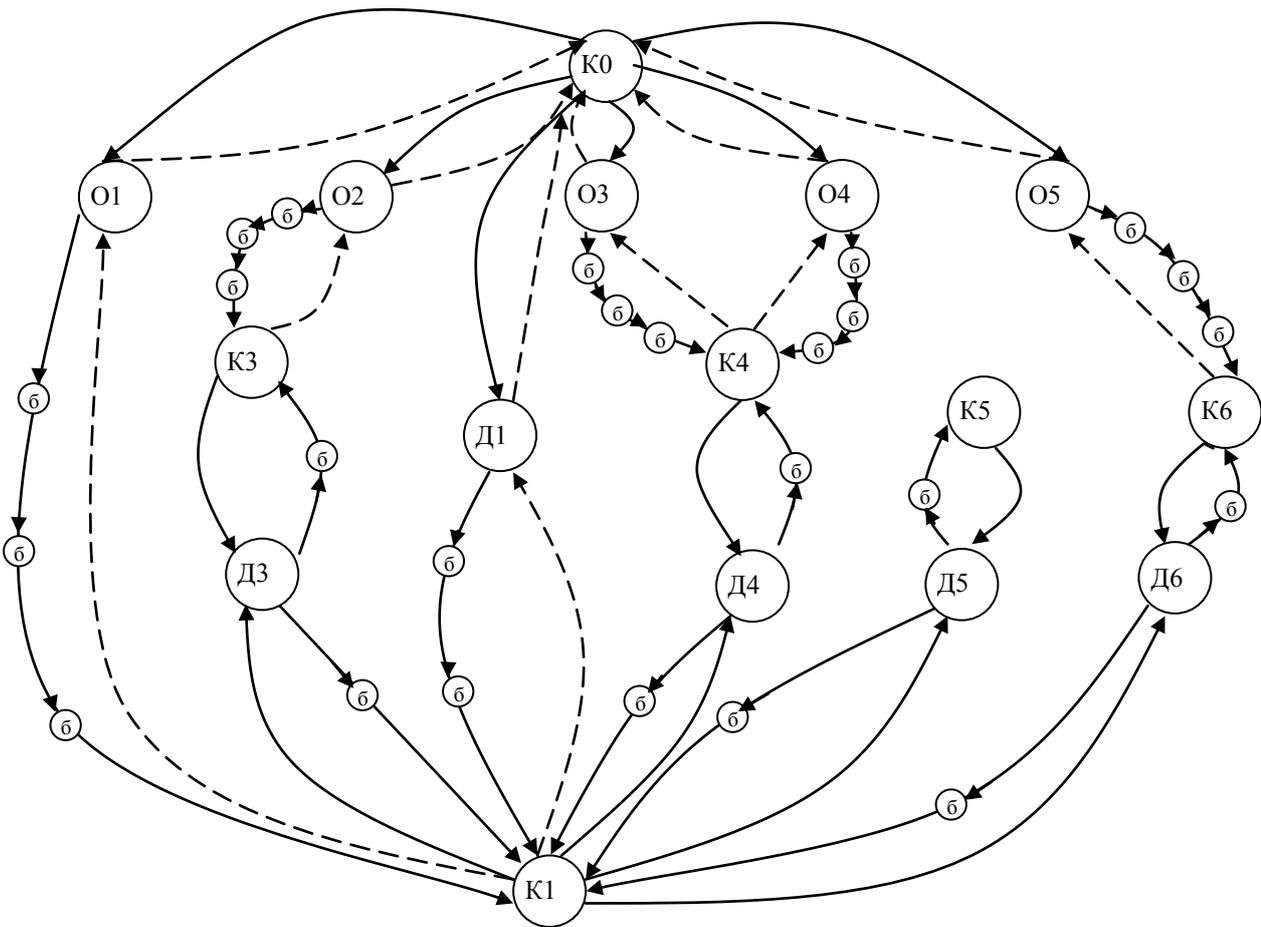


Рис. 5- Орграф путей доступа в помещение.

Следует объяснить, что ребра изображенные пунктирной линией – физически возможные переходы, но они не интересуют нас в данной лабораторной работе, поскольку нас интересует лишь проникновение на объект. Поэтому в дальнейшем мы можем

исключить эти ребра из графа. Также из графа можно исключить вершины, показывающие каналы проникновения. Поскольку мы их использовали для более подробного описания объекта. Необходимо провести следующую замену: «ребро- вершина канала утечки- ребро » преобразовать в одно ребро, при этой замене должны участвовать лишь ребра из кратчайшего расстояния между помещениями, а также одно ребро должно быть направлено в вершину канала утечки, а другое должно исходить из вершины канала утечки. Получим следующий граф, изображенный на рис. 6.

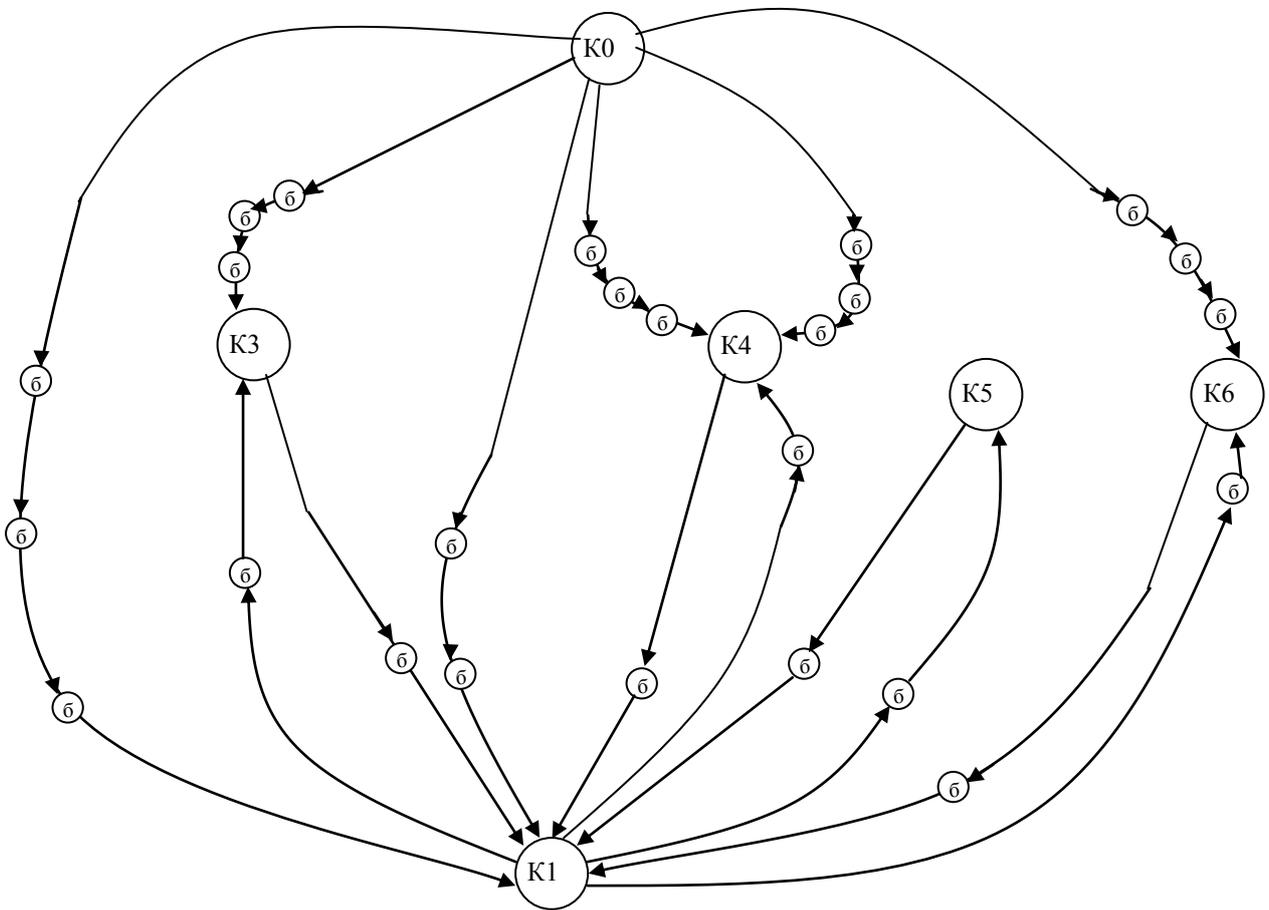


Рис. 6- упрощенный граф путей доступа в помещение

Каждой дуге ставится в соответствие ее вес – вероятность совершения данного перехода. Путь проникновения нарушителя в какое-либо помещение представляет собой путь в графе.

Начальной точкой пути всегда считаем вершину K0. Все переходы, начинающиеся в вершине K0, примем равновероятными, поскольку нам неизвестно, по какому пути пойдет преступник. При этом сумма всех этих вероятностей равна вероятности возникновения соответствующей угрозы, в нашем случае – физического проникновения. В нынешних условиях вероятность попытки проникновения можно принять равной 1. Таким образом, вес дуг, начинающихся в K0 равен 0,167. Для упрощения расчетов в лабораторной работе примем вероятность совершения всех остальных переходов равными 0,1. Следует заметить, что вес дуг, направленных к барьеру между помещениями примем равным  $1/n$ , где n- число выходящих из вершины ребер. Укажем веса дуг на графе (Рис. 7)

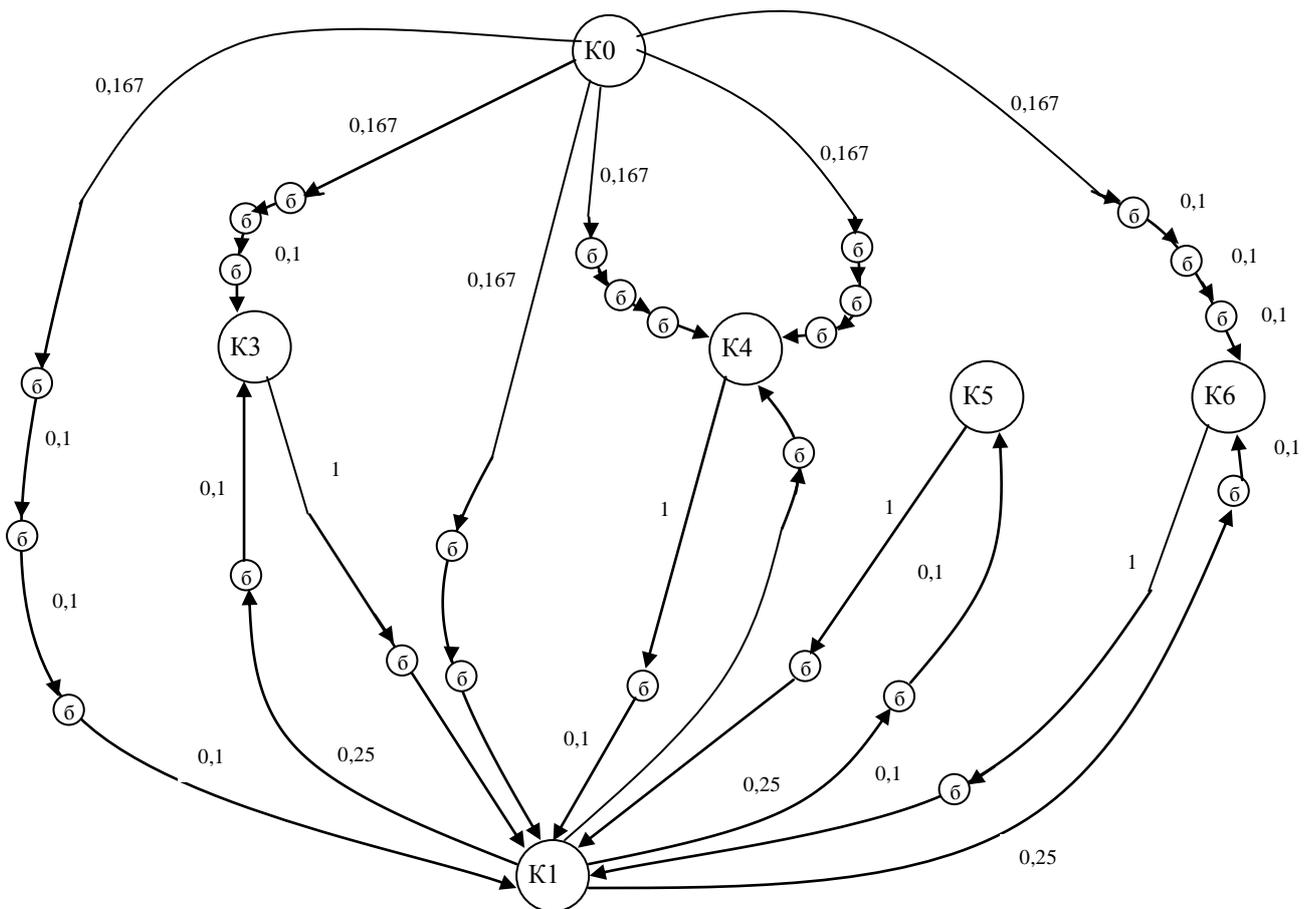


Рис. 7- Граф путей доступа с указанием веса дуг.

Каждой вершине можем приписать вероятность попадания в данную вершину. Эту вероятность можем рассчитать по формуле:

$$p_i = \sum_{j=1}^n v_j \cdot p_j, \quad (1)$$

где  $v_j$  – вес  $j$ -й дуги;

$p_j$  – вероятность нахождения преступника в соседнем состоянии (соседней вершине)  $j$ ,

$n$  – число соседних состояний (вершин).

Если в графе присутствует вершина, переход в которую возможен только из одной вершины и из которой выходит только одна дуга, то такую вершину можно исключить, заменив ее дугой с весом, равным произведению весов входящей и исходящей дуги. Исключив, таким образом, все такие вершины, получим новый граф (рис. 8).

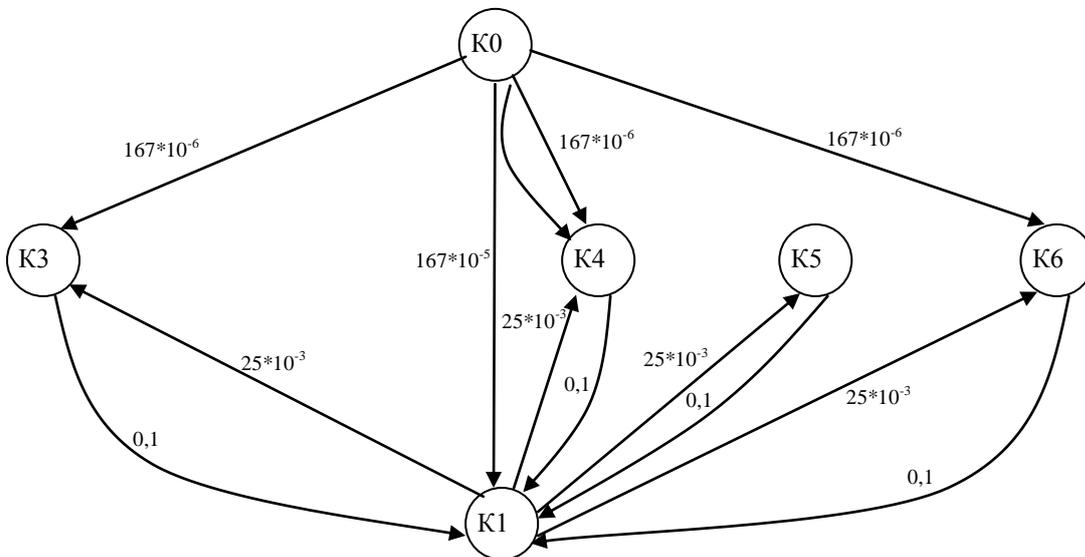


Рис. 8 – Упрощенный граф путей доступа

Если из одной вершины в другую ведут более одной дуги, все эти дуги можно заменить одной с весом, равным сумме весов этих дуг. Составим систему уравнений Колмогорова-Чепмена для определения вероятностей доступа в помещения. Для этого

добавим в граф дуги, ведущие из каждой вершины в саму себя, с весом, равным:

$$v_i = 1 - \sum_{j=1}^n v_j, \quad (2)$$

где  $v_j$  – вес  $j$ -й дуги, выходящей из данной вершины;

$n$  – количество дуг, выходящих из вершины  $i$ .

В результате получим следующий граф (Рис. 9):

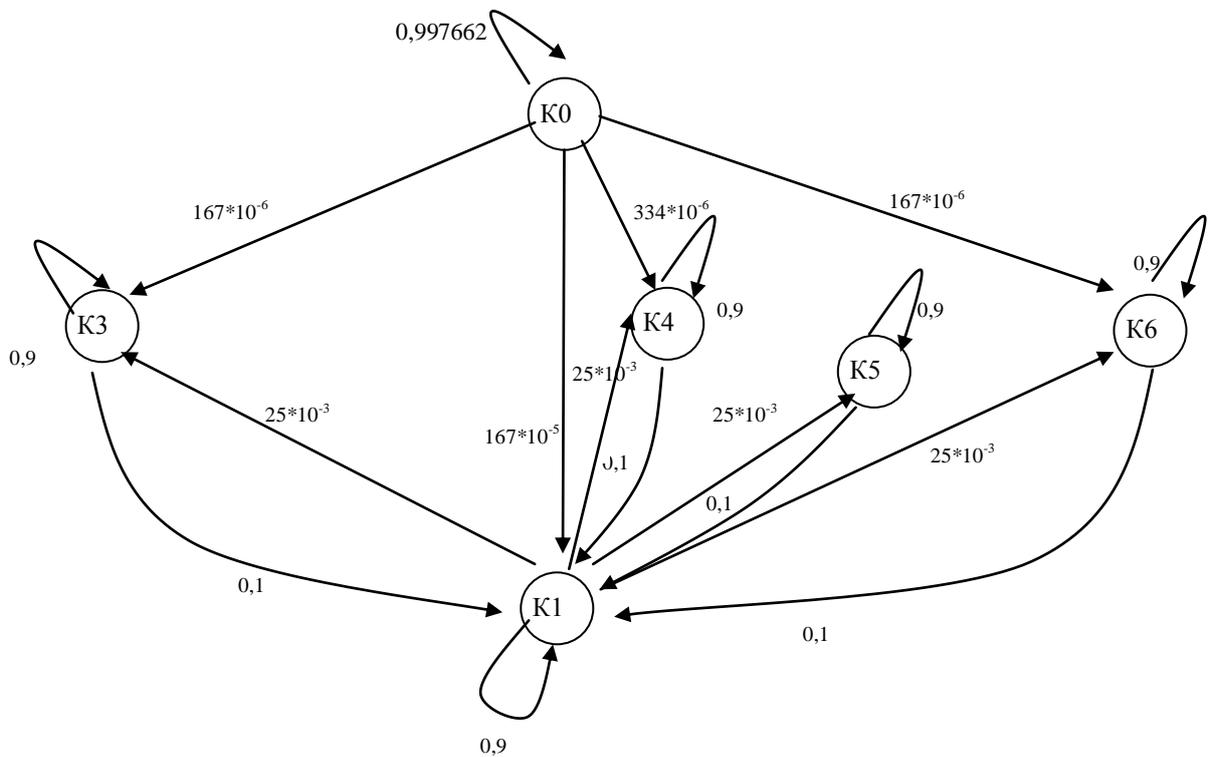


Рис. 9- Конечный граф путей доступа в помещение

Для данного графа матрица переходных вероятностей будет иметь следующий вид:

	K0	K1	K3	K4	K5	K6
Из K0	0,997 662	167* $10^{-5}$	167* $10^{-6}$	334* $10^{-6}$	0	167* $10^{-6}$
Из K1	0	0,9	25*1 $0^{-3}$	25*1 $0^{-3}$	25*1 $0^{-3}$	25*1 $0^{-3}$
Из K3	0	0,1	0,9	0	0	0
Из K4	0	0,1	0	0,9	0	0
Из K5	0	0,1	0	0	0,9	0
Из K6	0	0,1	0	0	0	0,9

## 5. РАСЧЕТ ВЕРОЯТНОСТЕЙ ДОСТУПА

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

$$P_j(k) = M_b \cdot P^k \cdot D_j, \quad (3)$$

где  $M_b = [P_1(0) \ P_2(0) \ \dots \ P_N(0)]_{1 \times N}$  – вектор-строка начального состояния системы;  $P = [p_{ij}]_{N \times N}$  – квадратная матрица переходных вероятностей;  $D_j = [0 \ 0 \ \dots \ 1 \ \dots \ 0]_{N \times 1}^T$  – вектор-столбец анализируемого состояния, который имеет все нулевые элементы и одну единицу, которая стоит в позиции, соответствующей порядковому номеру анализируемого состояния.

Рассчитаем вероятности доступа в помещения. В нашем случае

$M_0 = (1 \ 0 \ 0 \ 0 \ 0 \ 0)$ ,  $k=1..126$  шагов, тогда при построении графика наглядно можно увидеть изменение вероятности проникновения в помещение.

Шаг- временной интервал, который требуется злоумышленнику для перехода из одного помещения в другое.

Решаем следующую систему, записанную в матричной форме:

$$(1 \ 0 \ 0 \ 0 \ 0 \ 0) \cdot \begin{pmatrix} 0.997662 & 0.00167 & 0.000167 & 0.000334 & 0 & 0.000167 \\ 0 & 0.9 & 0.025 & 0.025 & 0.025 & 0.025 \\ 0 & 0.1 & 0.9 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0.9 & 0 & 0 \\ 0 & 0.1 & 0 & 0 & 0.9 & 0 \\ 0 & 0.1 & 0 & 0 & 0 & 0.9 \end{pmatrix}^k \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Получаем 126 различных вероятностей для одного помещения, строим график зависимости вероятности от времени (количества шагов).

для первого помещения получаем следующий график (Рис. 11).

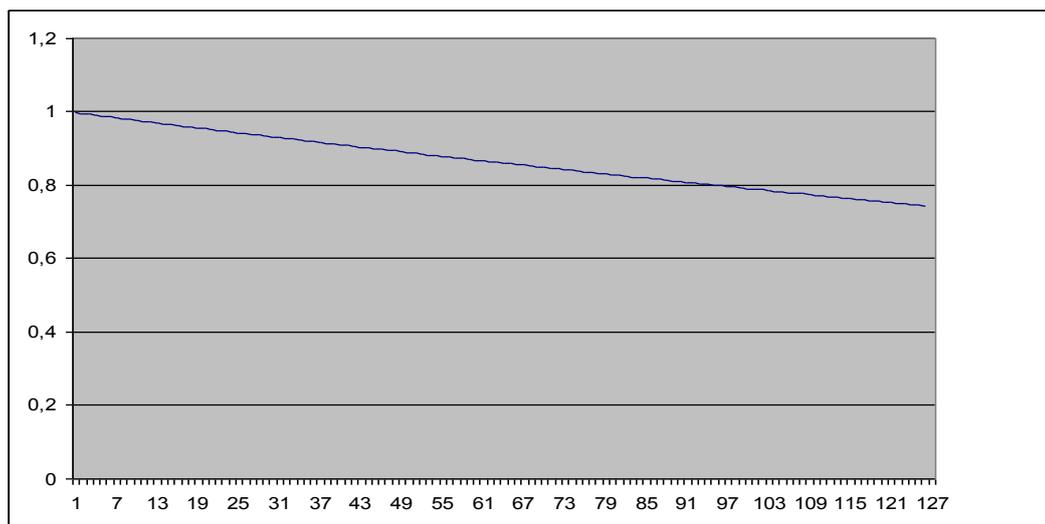


Рис. 11- График вероятности доступа в помещение 1

Для второго помещения график зависимости вероятности доступа в помещения объекта от времени, начиная от момента начала атаки, приведены на Рис. 12

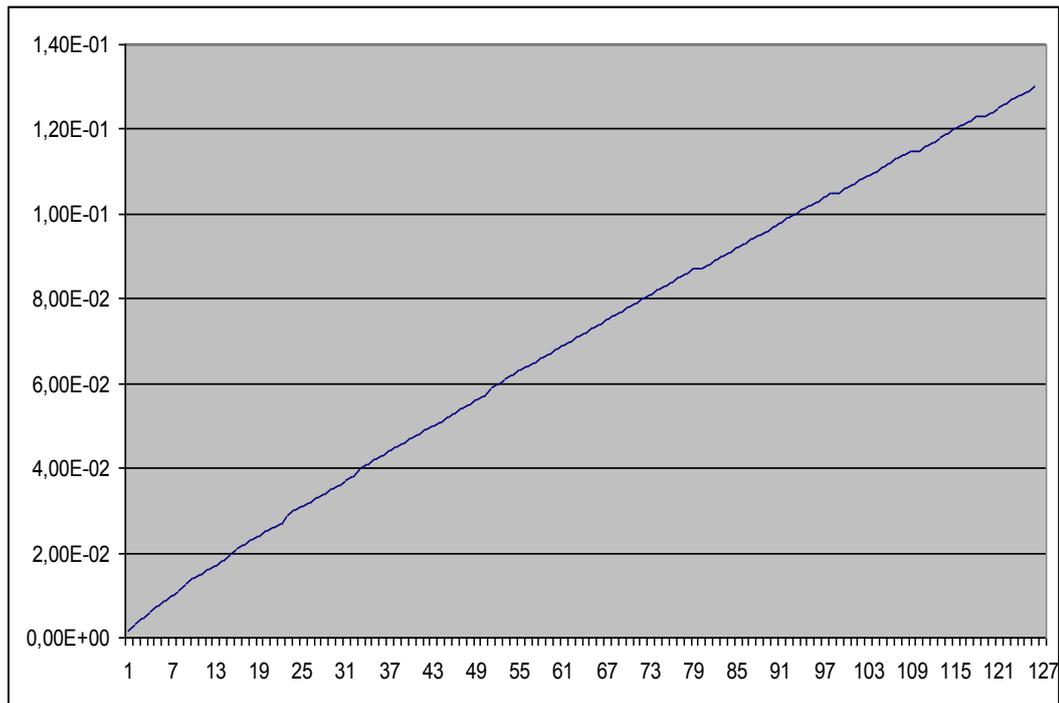


Рис. 12- График вероятности доступа в помещение 2.

## 6. ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

Рассчитать защищённость от физического проникновения для собственной организации (минимальные требования: 4 функциональных помещения, 5 человек персонала). В отчете должен быть представлена план-схема помещений. По полученным графикам сделать выводы о качестве функционирования комплексной системы защиты информации на рассматриваемом предприятии.

## 7. ТРЕБОВАНИЯ К ОТЧЕТУ

Отчет должен содержать:

1. титульный лист;
2. цель работы;
3. краткий теоретический материал (при необходимости);
4. план-схема помещений;
5. ход работы, где будут приведены расчеты и графики с пояснениями и выводами;
6. выводы по проделанной работе.

## 8. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. вероятности несанкционированного доступа на охраняемый объект
2. показатели качества функционирования комплексной системы защиты информации на предприятии
3. расчет защищенности объекта от физического проникновения

## 9. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Смирнов Н.В., Дунин-Барковский Н.В. Курс теории вероятности и математической статистики (для технических приложений). – М.: Наука, 1969. – 230 с.
2. Попов Л.И., Зубарев А.В. Основные принципы повышения эффективности реализации мероприятий по комплексной защите информации
3. «Теория выбора и принятия решений»: учебное пособие. И.М. Макаров, Т.М. Виноградская, А.А. Рубчинский, В.Б. Соколов. Москва, изд. «Наука», 1982.
4. «Теория вероятностей» Е.С. Вентцель. Москва, изд. «Наука», 1969.

# МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра информационной безопасности



## Определение показателей защищенности информации при несанкционированном доступе

Методические указания по выполнению лабораторной работы

Курск 2017

УДК 621.(076.1)

Составители: В.В. Карасовский, О.А. Демченко

Рецензент

Кандидат технических наук, доцент кафедры  
информационной безопасности *А.Г. Сневаков*

**Определение показателей защищенности информации при несанкционированном доступе:** методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: В.В. Карасовский, О.А. Демченко Курск, 2017.- 7 с.: ил.1,Табл. 1 ,Библиогр.: с. 7.

Содержат сведения об администрирование и управление программно-аппаратными средствами контроля и фильтрации сетевых пакетов способах, а так же защиты от несанкционированного доступа к ресурсам персонального компьютера. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Предназначены для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать .

Формат 60x84 1/16.

Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ . Бесплатно.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

## СОДЕРЖАНИЕ

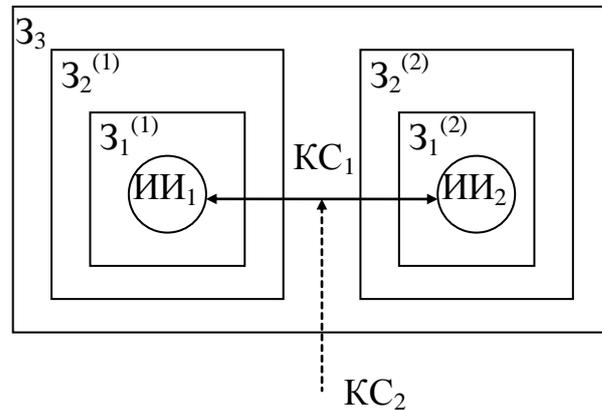
Содержание .....	3
1. Цель работы.....	4
2. Теоретический материал .....	4
3. Постановка задачи .....	5
4. Задание на лабораторную работу.....	6
5. Требования к отчету .....	6
6. Список контрольных вопросов .....	7
7. Библиографический список.....	7

## 1. ЦЕЛЬ РАБОТЫ

Определить показатели защищенности (уязвимости) информации при несанкционированном доступе. Провести анализ зависимости показателя уязвимости информации от параметров системы ЗИ.

## 2. ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

Один из основных принципов построения КСЗИ - необходимость выстраивания вокруг объекта защиты постоянно действующих замкнутых контуров.



**Рис. 1**

Пусть  $P_{угр}$  – вероятность возникновения угрозы.

Вероятность того, что все зоны защиты правильно функционируют, равна:

$$P_{защ} = \prod_{i=1}^n P_{zi}. \quad P_{уязв} = 1 - P_{защ}.$$

Вероятность того, что произошел НСД, равна:

$$P_{НСД} = P_{угр} \prod_{i=1}^n (1 - P_{zi}).$$

Точность расчета зависит от точности исходных данных.

Для получения вероятностей появления отдельных угроз необходимо иметь статистику (закон распределения соответствующих событий). Наиболее распространенный – экспоненциальный закон распределения.

Выраженная по этому закону вероятность появления угрозы  $u_i$ , равна:  $P_{yi}(t) = 1 - e^{-\lambda_i t}$ , где  $\lambda$  - интенсивность НСД (относительное число НСД в единицу времени).

Если  $\lambda_i \ll 1$ , то  $P_{yi}(t) \approx \lambda_i t$ .

### 3. ПОСТАНОВКА ЗАДАЧИ

1) элементарные случайные события:

$A^{(1)}$  - нарушитель разрушил защиту в  $Z_1^{(1)}$ ,

$A^{(2)}$  - нарушитель разрушил защиту в  $Z_1^{(2)}$ ,

$B^{(1)}$  - нарушитель разрушил защиту в  $Z_2^{(1)}$ ,

$B^{(2)}$  - нарушитель разрушил защиту в  $Z_2^{(2)}$ ,

$C$  - нарушитель разрушил защиту в  $Z_3$ ,

$D^{(1)}$  - нарушитель получил НСД к ИИ<sub>1</sub> через  $KC_1$ ,

$D^{(2)}$  - нарушитель получил НСД к ИИ<sub>2</sub> через  $KC_1$ ,

$E$  - нарушитель получил НСД к ИИ<sub>1</sub> и ИИ<sub>2</sub> через  $KC_2$ .

2) интенсивности наступления перечисленных выше событий

$\lambda$  (см. варианты):

Вариант	$\lambda\{A^{(1)}\}$	$\lambda\{A^{(2)}\}$	$\lambda\{B^{(1)}\}$	$\lambda\{B^{(2)}\}$	$\lambda\{C\}$	$\lambda\{D^{(1)}\}$	$\lambda\{D^{(2)}\}$	$\lambda\{E\}$
	1	2	3	4	5	6	7	8
1	0,000 7	0,000 7	0,002 5	0,000 1	0,0029 5	0,000 5	0,0038 5	0,0032 5
2	0,000 6	0,000 4	0,004 5	0,000 2	0,0028 5	0,000 7	0,0045 5	0,0025 5
3	0,000 8	0,000 5	0,001 5	0,000 4	0,0032 5	0,000 8	0,0055 6	0,0022 5
4	0,012 5	0,000 2	0,002 5	0,000 1	0,0035 5	0,000 5	0,0042 5	0,0022 5
5	0,000 5	0,000 5	0,001 5	0,000 1	0,0002 5	0,000 5	0,0022 5	0,0045 6

#### 4. ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

1. Подсчитать вероятности событий 1-8 при  $T=500$  часов.

2. Найти вероятности сложных событий:

$$P\{D^{(1)} + E\} = P\{D^{(1)}\} + P\{E\} - P\{D^{(1)}\} \cdot P\{E\},$$

$$P\{D^{(2)} + E\} = P\{D^{(2)}\} + P\{E\} - P\{D^{(2)}\} \cdot P\{E\},$$

$$P\{CB^{(1)} A^{(1)}\} = P\{C\} \cdot P\{B^{(1)}\} \cdot P\{A^{(1)}\},$$

$$P\{CB^{(2)} A^{(2)}\} = P\{C\} \cdot P\{B^{(2)}\} \cdot P\{A^{(2)}\},$$

$$P\{CB^{(1)} A^{(1)} + CB^{(2)} A^{(2)}\} = 1 - (1 - P\{CB^{(1)} A^{(1)}\})(1 - P\{CB^{(2)} A^{(2)}\}),$$

$$P\{E + CB^{(1)} A^{(1)} + CB^{(2)} A^{(2)}\} = 1 - (1 - P\{E\})(1 - P\{CB^{(1)} A^{(1)}\})(1 - P\{CB^{(2)} A^{(2)}\}).$$

3. Построить график изменения вероятности  $P\{E + CB^{(1)} A^{(1)} + CB^{(2)} A^{(2)}\}$  от времени при  $T=(0 \div 1000)$  часов.

4. Уменьшить наибольшую интенсивность в 4 раза и посмотреть, как это повлияло на изменение вероятности  $P\{E + CB^{(1)} A^{(1)} + CB^{(2)} A^{(2)}\}$  от времени (построить график).

5. Определить, во сколько раз требуется уменьшить все интенсивности, чтобы вероятность  $P\{E + CB^{(1)} A^{(1)} + CB^{(2)} A^{(2)}\}$  уменьшилась в 2 раза при неизменном значении времени.

6. Представить в отчете вычисления и графики.

7. Проанализировать полученные результаты.

#### 5. ТРЕБОВАНИЯ К ОТЧЕТУ

Отчет должен содержать:

1. титульный лист;
2. цель работы;
3. краткий теоретический материал (при необходимости);
4. Расчеты вероятностей в соответствии с вариантом;
5. Графики с пояснениями и выводами;
6. Выводы по проделанной работе.

## 6. СПИСОК КОНТРОЛЬНЫХ ВОПРОСОВ

1. Перечислить показатели защищенности информации при несанкционированном доступе
2. зависимость показателя уязвимости информации от параметров системы ЗИ

## 7. БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Н. В. Гришина. Организация Комплексной Системы Защиты Информации. [Электронный ресурс] : статья / - Электрон. дан. - Режим доступа: <http://coollib.com/b/166590/read>
2. Этапы построения Комплексной системы защиты информации. [Электронный ресурс] : статья / - Электрон. дан. - Режим доступа: [http://www.rusnauka.com/36\\_PWMN\\_2010/Informatica/77026.doc.htm](http://www.rusnauka.com/36_PWMN_2010/Informatica/77026.doc.htm)

## МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра информационной безопасности



**Составление обзорного документа по сертифицированным  
продуктам в заданной области информационной безопасности**

Методические указания по выполнению практической работы

УДК 621.(076.1)

Составители: Е.С.Волокитина, М.О. Таныгин.

Рецензент

Кандидат технических наук, доцент кафедры  
информационной безопасности *А.Г. Сневаков*

**Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности: методические указания по выполнению практической работы / Юго-Зап. гос. ун-т; сост.: Е.С.Волокитина, М.О. Таныгин. Курск, 2017.- 7 с.: табл. 2, Библиогр.: с. 7.**

Содержат сведения об администрировании и управлении программно-аппаратными средствами контроля и фильтрации сетевых пакетов способами, а так же защиты от несанкционированного доступа к ресурсам персонального компьютера. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Предназначены для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.  
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ . Бесплатно.  
Юго-Западный государственный университет.  
305040, г. Курск, ул. 50 лет Октября, 94.

## СОДЕРЖАНИЕ

Содержание .....	3
1.Цель работы.....	4
2. Требования к выполнению задания .....	4
3. Задание на практическую работу .....	5
4. Требования к отчету .....	6
5. Список контрольных вопросов .....	7
6. Список дополнительной литературы.....	7

## 1. ЦЕЛЬ РАБОТЫ

Целью данной лабораторной работы является обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.

## 2. ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ ЗАДАНИЯ

В ходе выполнения задания необходимо провести анализ сертифицированных продуктов в заданной области информационной безопасности. После этого следует определить, какие средства защиты являются наиболее приемлемыми для использования в системах защиты. По результатам анализа оформить отчет.

При поиске средств защиты в заданной области, искать сертификацию на соответствие требованиям:

№	Вид СЗИ	Предназначение средства (область применения)
1.	Средства защиты от несанкционированного доступа	соответствует документу «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа»
2.	Межсетевые экраны	соответствует документу «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатель защищенности от несанкционированного доступа к информации»
3.	Антивирусные средства	соответствует документу «Требования к средствам антивирусной защиты»

№	Вид СЗИ	Предназначение средства (область применения)
		соответствует документу «Профиль защиты средств антивирусной защиты»
4.	Средства криптографической защиты	«может использоваться для криптографической защиты»
5.	Средства обнаружения вторжений	соответствует документу «Требования к системам обнаружения вторжений»
		соответствует документу «Профиль защиты систем обнаружения вторжений уровня узла»
6.	Средства контроля защищенности (автоматизированного анализа защищенности и обнаружения уязвимостей автоматизированных систем)	«является средством анализа защищенности и обнаружения уязвимостей»
7.	Средства резервного копирования	«предназначен для создания автоматизации процессов резервного копирования»

### 3. ЗАДАНИЕ НА ПРАКТИЧЕСКУЮ РАБОТУ

1. Определить, кто из регуляторов проводит сертификацию в заданной области средств защиты информации

2. Пользуясь сайтами регуляторов в области защиты информации Федеральной службы безопасности (<http://clsz.fsb.ru/>) и Федеральной службы по техническому и экспортному контролю (<http://fstec.ru/>) выбрать средства защиты по направлению (номер в списке группы по порядку):

- 2.1. Средства защиты от несанкционированного доступа;
- 2.2. Межсетевые экраны;

- 2.3. Антивирусные средства;
  - 2.4. Средства криптографической защиты;
  - 2.5. Средства обнаружения вторжений;
  - 2.6. Средства контроля защищенности;
  - 2.7. Средства резервного копирования;
  - 2.8. Свой вариант (по согласованию).
3. Сделать сравнительный анализ всех средств защиты в форме таблицы.

№	Название	Срок действия	Выполняемые функции	Изготовитель
---	----------	---------------	---------------------	--------------

4. Из полученного списка и определить наиболее привлекательные средства защиты. Объяснить почему.

5. Найти сертификаты для выбранных средств защиты информации (на сайтах производителей).

6. Сопоставить данные из сертификата выбранного средства защиты и требования руководящего документа Гостехкомиссии или другого соответствующего документа (найти ссылку в сертификате).

#### 4. ТРЕБОВАНИЯ К ОТЧЕТУ

Отчет должен содержать:

1. титульный лист;
2. цель работы;
3. заданную область информационной безопасности;
4. сравнительный анализ средств защиты;
5. выбранное оптимальное средство защиты, обоснование почему и сертификат на него (скачать на сайте производителя СЗИ);
6. Перечень документов, на соответствие которым сертифицирован продукт;
7. выводы по проделанной работе.

## 5. СПИСОК КОНТРОЛЬНЫХ ВОПРОСОВ

1. Как проводится сертификация средств защиты информации?
2. Что показывают характеристики данного средства защиты?
3. Какой регулятор контролирует данную область информационной безопасности?
4. Какая основная информация содержится в сертификате?

## 6. СПИСОК ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

1. Справочно-поисковая система «Консультант Плюс» [Электронный ресурс]: - Электрон. дан. - Режим доступа: <http://www.consultant.ru/>
2. Справочно-поисковая система «Гарант» [Электронный ресурс]: - Электрон. дан. - Режим доступа: <http://www.garant.ru/>
3. Информационный ресурс «Центр по лицензированию, сертификации и защите государственной тайны ФСБ России» [Электронный ресурс]: - Электрон. дан. - Режим доступа: <http://clsz.fsb.ru/>
4. Информационный ресурс «ФСТЭК России» [Электронный ресурс]: - Электрон. дан. - Режим доступа: <http://fstec.ru/>

# МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное  
Учреждение высшего образования

«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра информационной безопасности



## ИССЛЕДОВАНИЕ ПРОТИВОДЕЙСТВИЯ НЕСАНКЦИОНИРОВАННОЙ РАБОТЕ ПОРТАТИВНЫХ ЗВУКОЗАПИСЫВАЮЩИХ УСТРОЙСТВ

Методические указания по выполнению практических работ по  
дисциплине «Технология обеспечения информационной безопасности  
объекта» для студентов специальности 10.04.01

Курск2017

УДК 004.725.7

Составители: А.Л. Марухленко

Рецензент

Кандидат технических наук, доцент *А.Г. Сневаков*

**Исследование противодействия несанкционированной работе портативных звукозаписывающих устройств:** методические указания к выполнению практических работ /Юго-Зап.гос.ун-т; сост. А.Л. Марухленко Курск,2017. -9с. Библиогр.:с.9.

Содержат сведения по вопросам исследования противодействия несанкционированной работы портативных звукозаписывающих устройств. Указывается порядок выполнения практической работы, правила оформления, содержание отчета, контрольные вопросы

Методические указания по выполнению практических работ соответствуют требованиям программы, утвержденной учебно-методическим объединением, предназначены для студентов направления подготовки 10.04.01 для изучения дисциплины «Технология обеспечения информационной безопасности объекта».

Текст печатается в авторской редакции

Подписано в печать 01.11.2017. Формат 60x84 1/16.

Усл.печ. л. 0,5. Уч.-изд.л. 0,5. Тираж 30 экз. Заказ \_\_\_\_\_. Бесплатно.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

**СОДЕРЖАНИЕ**

1. Цель работы .....	4
2. Приборы и материалы .....	4
3. Подготовка к работе .....	4
4. Выполнение работы .....	5
5. Содержание отчета .....	7
6. Контрольные вопросы .....	7
Библиографический список .....	9

## 1. ЦЕЛЬ РАБОТЫ

- Исследовать эффективность активного противодействия утечки речевой информации по акустическому каналу.
- Изучить правила работы с линейным генератором шума типа ЛГШ-104 «РаМЗес» (далее ЛГШ-104).
- Определить зону эффективного подавления ЛГШ-104 в текущих условиях.

## 2. ПРИБОРЫ И МАТЕРИАЛЫ

Цифровой диктофон Olympus VN-240PC.

Аналоговый диктофон Olympus J500.

Подавитель диктофонов ЛГШ-104 «РаМЗес».

## 3. ПОДГОТОВКА К РАБОТЕ

1. Ознакомиться с техническими характеристиками и правилами работы с прибором ЛГШ-104. Особое внимание уделить мерам предосторожности.
2. Изучить инструкции по предоставленным диктофонам.
3. Получить у преподавателя допуск к работе.

### Описание измерительной установки

Схема лабораторного стенда представлена на рис. 2.1.

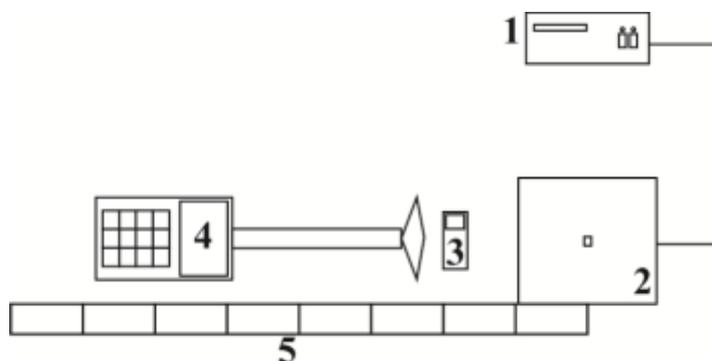


Рис. 1. Лабораторный стенд.

1. Основной блок ЛГШ-104.

2. Антенна ЛГШ-104.
3. Диктофон (для ускорения работы можно размещать сразу два диктофона в одной точке).
4. Измерительный прибор ПЗ-31.
5. Измерительная линейка.

Для проведения лабораторной работы необходимы: прибор ПЗ-31 с измерительной антенной АИ-1; ЛГШ-104; диктофоны (аналоговый и цифровой) и измерительная линейка.

Генератор шума ЛГШ-104 предназначен для предотвращения несанкционированной записи конфиденциальных переговоров аппаратами магнитной звукозаписи (диктофонами и магнитофонами разного типа). В результате воздействия электромагнитного излучения (ЭМИ) ЛГШ-104 на скрытый аппарат звукозаписи, на магнитный носитель записывается шумовой сигнал вместо разговора, содержащего КИ.

В лабораторной работе рассматриваются способы активной защиты КИ от съема с помощью портативных звукозаписывающих устройств (аналоговых и цифровых диктофонов) при ведении переговоров, заседаний, совещаний и т.п.

Для имитации процесса ведения переговоров необходимо зачитывать и записывать на аналоговый и цифровой диктофоны речевой тест (в виде заранее подготовленного текста), постепенно перемещая их в заданном направлении от антенны ЛГШ-104. Расстояние, на котором возможно будет различить речь на записи, соответствует границе зоны эффективного подавления речевой КИ для каждого вида звукозаписывающих устройств. В рамках лабораторной работы следует также с помощью прибора ПЗ-31 определить уровень напряженности поля  $E_{cp}$  сигнала ЛГШ-104, соответствующий границе зоны эффективного подавления.

#### **4. ВЫПОЛНЕНИЕ РАБОТЫ**

Расположить антенну ЛГШ-104 на столе.

Включить питание и прогреть прибор ПЗ-31 (контроль по дисплею прибора).

Включить диктофоны на запись.

Установить диктофоны на расстоянии 15 см от красного маркера на антенне ЛГШ-104. Диктофоны установить так, чтобы их микрофоны находились как можно ближе к точке измерения.

Включить ЛГШ-104 и провести измерение среднего значения напряженности поля  $E$ , В/м прибором ПЗ-31 в точке пространства, расположенной непосредственно над диктофонами. Для этого нажать кнопку « $E(H)/доп$ », затем кнопку «сред макс тек» – пока на экране над числовым значением не появится индикация «avg». Полученное показание прибора занести в таблицу 2.1.

Надиктовать тестовую информацию (с обязательным указанием номера точки, в которой производится измерение, и расстояния до нее от центра антенны ЛГШ-104).

Переместить диктофоны на 15 см в заданную сторону от центра антенны ЛГШ-104. Повторить действия п.п. 6.3-6.5 в этой точке.

Повторить измерения во всех 7 контрольных точках (с учетом того, что в 2 из них измерения уже проведены согласно п.п. 6.1-6.7). Результаты занести в таблицу 2.1.

Поместить антенну прибора ЛГШ-104 на подставку, находящуюся под столом. Перемещение диктофонов производить по-прежнему на поверхности стола.

Повторить измерения согласно п.п. 6.3-6.7 для точек, при антенне, находящейся ниже уровня стола. Полученные результаты занести в таблицу 2.1 с указанием расстояния от антенны ЛГШ-104 до поверхности стола.

Таблица 2.1. Результаты определения напряженности поля  $E_i$ , [В/м]

Контрольные точки	1	2	...	6	7
-------------------	---	---	-----	---	---

$E_{ci}$ , [В/м]; ЛГШ-104 на уровне стола					
$E_{ni}$ , [В/м]; ЛГШ-104 нижестолана см					

Построить графики зависимостей  $E_c(r)$  и  $E_n(r)$ .

Определить, начиная с какого расстояния  $r_{зр}$  становится возможным разобрать речь на записи диктофонов.

Сделать вывод о размерах зоны эффективного подавления речевой КИ – для каждого типа диктофонов и каждого варианта расположения антенны ЛГШ-104, с указанием на графиках  $E_c(r)$  и  $E_n(r)$  величины граничного значения  $E_{зр}$  и соответствующего этой величине расстояния  $r_{зр}$  от центра антенны ЛГШ-104.

## 5. Содержание отчета

Итогом работы является определение зоны эффективного подавления речевой КИ для каждого вида диктофонов и каждого варианта расположения антенны ЛГШ-104. В соответствии с этим в отчете необходимо привести:

- формулировку цели и задания на выполнениеработы;
- схему лабораторнойустановки;
- список приборов иоборудования;
- таблицу со значениями всех измеренных величин и графики зависимостей  $E_c(r)$  и  $E_n(r)$ ;
- уровни напряженности поля  $E_{зр}$  и соответствующие им расстояния  $r_{зр}$  для разных диктофонов при разных вариантах расположения антенны ЛГШ-104;
- выводы по результатам выполненныхисследований.

## 6. Контрольныевопросы

1. Принцип действия ЛГШ-104 как средства активной защиты КИ.
2. От каких факторов зависит эффективность работы (площадь эффективной зоны подавления КИ) ЛГШ?
3. Какие технические характеристики ЛГШ влияют на эффективность защиты речевой КИ?
4. Особенности воздействия ЛГШ разных типов на диктофоны в сотовых телефонах.
5. Каковы правила размещения и эксплуатации ЛГШ-104?
6. Основные типы подавителей диктофонов и особенности их функционирования.
7. По каким критериям выбираются подавители диктофонов?
8. Как можно исключить применение диктофонов, размещенных в мобильных телефонах, для перехвата речевой КИ?
9. В каких случаях целесообразно камуфлировать средства подавления диктофонов и как это можно сделать на практике?
10. Объясните физические явления, на основании которых работает подаватель диктофонов.

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

- 1) Торокин А.А. Инженерно-техническая защита информации. Учебное пособие для студентов, обучающихся по специальностям в области информационной безопасности. [Текст] / М.: Гелиос АРВ, 2005.
- 2) Хорев А.А. Техническая защита информации. Учебное пособие для студентов вузов. Том 1. Технические каналы утечки информации. [Текст] / М.: НПЦ «Аналитика», 2008.
- 3) Лепешкин, О. М. Комплексные средства безопасности и технические средства охранно-пожарной сигнализации : учеб. пособие [Текст] / О. М. Лепешкин. – М. : Гелиос АРВ, 2009.
- 4) Магауенов, Р. Г. Системы охранной сигнализации: основы теории и принципы построения [Текст] / Р. Г. Магауенов. – М. : Горячая линия – Телеком, 2008.

# МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное  
Учреждение высшего образования

«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра информационной безопасности



## ИССЛЕДОВАНИЕ АКУСТИЧЕСКОГО И ВИБРОАКУСТИЧЕСКОГО КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Методические указания по выполнению практических работ по  
дисциплине «Технология обеспечения информационной безопасности  
объекта» для студентов специальности 10.04.01

Курск2017

УДК004.725.7

Составители: А.Л.Марухленко

Рецензент

Кандидат технических наук, доцент *А.Г. Сневаков*

**Исследование акустического и виброакустического каналов утечки информации:** методические указания к выполнению практических работ / Юго-Зап.гос.ун-т; сост. А.Л. Марухленко Курск, 2017.- 12с. Библиогр.:с.12.

Содержат сведения по вопросам исследования акустического и виброакустического каналов утечки информации. Указывается порядок выполнения практической работы, правила оформления, содержание отчета, контрольные вопросы

Методические указания по выполнению практических работ соответствуют требованиям программы, утвержденной учебно-методическим объединением, предназначены для студентов направления подготовки 10.04.01 для изучения дисциплины «Технология обеспечения информационной безопасности объекта».

Текст печатается в авторской редакции

Подписано в печать 01.11.2017. Формат 60x84 1/16.

Усл.печ. л. 0,7. Уч.-изд.л. 0,6. Тираж 30 экз. Заказ \_\_\_\_\_. Бесплатно.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

**СОДЕРЖАНИЕ**

1. Цель работы .....	4
2. Приборы и материалы .....	4
3. Подготовка к работе .....	4
4. Теоретическая часть .....	4
5. Выполнение работы .....	6
6. Содержание отчета .....	10
7. Контрольные вопросы .....	10
Библиографический список .....	12

## **1. ЦЕЛЬ РАБОТЫ**

Исследовать эффективность пассивного и активного противодействия утечке речевой информации по акустическому и виброакустическому каналу.

Изучение способов работы с многофункциональным поисковым прибором (МПП) ST-031 «Пиранья» в области акустических и виброакустических измерений.

Знакомство с системой виброакустической защиты (СВАЗ) путем постановки маскирующей помехи «Соната» и пассивным экранированием акустического и виброакустического каналов утечки конфиденциальной информации (КИ).

## **2. ПРИБОРЫ И МАТЕРИАЛЫ**

Звукоизолированная камера. Генератор звуковых частот. Акустический излучатель.

Перегородки из различных материалов.

МПП ST-031 «Пиранья» (далее МПП ST-031). Направленный микрофон (из комплекта МПП ST-031). Виброакустический датчик (из комплекта МПП ST-031). СВАЗ «Соната» с набором излучателей.

## **3. ПОДГОТОВКА К РАБОТЕ**

- Изучить правила работы с МПП ST-031 «Пиранья» в акустическом и виброакустическом режимах.
- Изучить инструкцию по прибору СВАЗ «Соната».
- Получить у преподавателя допуск к работе.

## **4. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ**

Схема лабораторной установки (стенда) представлена на рис. 1.1.

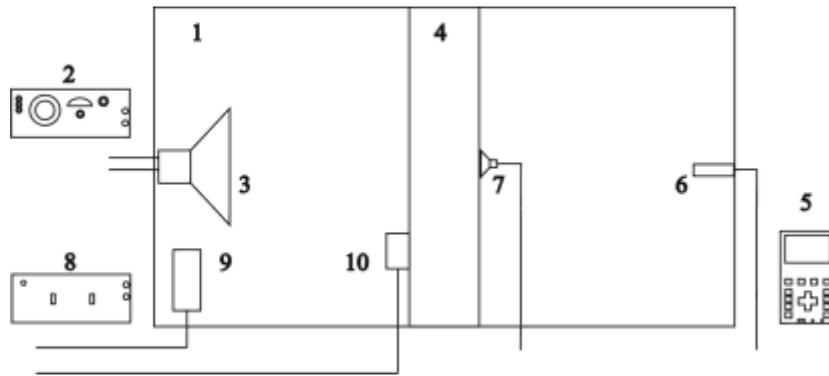


Рис. 1.1. Лабораторный стенд.

- 1 – Звукоизолированная камера.
- 2 – Генератор звуковых частот.
- 3 – Акустический излучатель.
- 4 – Перегородки из разных материалов.
- 5 – Прибор МПП ST-031.
- 6 – Направленный микрофон (из комплекта МПП ST-031).
- 7 – Виброакустический датчик (из комплекта МПП ST-031).
- 8 – Прибор СВАЗ «Соната».
- 9 – Акустический излучатель СВАЗ «Соната».
- 10 – Виброизлучатель СВАЗ «Соната» (плоский, для стекла).

Для выполнения лабораторной работы необходимы: МПП ST-031 с направленным микрофоном и виброакустическим датчиком; генератор звуковых частот с подключенным динамиком; СВАЗ «Соната»; звукоизолированный стенд с макетами ограждающих перегородок.

В лабораторной работе рассматриваются способы пассивной и активной защиты от утечки КИ по акустическому и виброакустическому каналам.

**Пассивная защита.** Исследуются виброакустические свойства перегородок, выполненных из следующих материалов:

- стекло (для имитации канала утечки через окно);
- гипсокартонная плита (для имитации канала утечки через стены);
- плита из минеральных волокон (для имитации канала утечки через навесной потолок).

**Активная защита.** Рассматривается вариант использования для постановки шумовых акустических и виброакустических помех СВАЗ «Соната».

## 5 ВЫПОЛНЕНИЕ РАБОТЫ

1. Включить питание генератора звуковых частот и МПП ST-031.
2. Проверить работоспособность МПП ST-031 в акустическом и виброакустическом режимах.
3. Подключить выносной микрофон к разъему «PROBES».
4. Разместить микрофон МПП ST-031 в отверстии правой стенки звукоизолированной камеры таким образом, чтобы микрофон не выходил за внутреннюю границу звукоизолирующего слоя. Заполнить уплотнителем зазор в отверстии. Микрофон и акустический излучатель должны находиться на расстоянии порядка 1,0 м друг от друга (см. рис. 1.2).
5. Закрыть камеру и включить источник тестового сигнала на октавной частоте 1 кГц при значении напряжения  $-0,5$  В, что соответствует уровню громкой речи  $-74$  дБ. Установить зависимость между значениями МПП ST-031 и заданным уровнем.

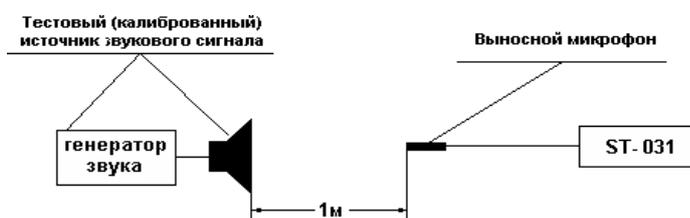


Рис. 1.2. Схема размещения источника звукового сигнала и МПП ST-031

6. Перейти в режим спектроанализатора – кнопка «SA».

Нажать «SET» и установите

«Lineaverage ON/OFF» в положение «ON» (кнопка «3» и «ENTER»).

Включается функция линейного усреднения гармоник спектра.

Полученную спектрограмму занесите в отчет.

7. Нажать кнопки «RUN/STOP». Спектрограмма «замирает», и на экран МПП ST-031 выводится вертикальный маркер, перемещение которого вдоль горизонтальной оси осуществляется кнопками «□» и «□». Измеренные значения частоты и амплитуды, составляющих спектра, соответствующие положению маркера, отображаются в средней части нижней и верхней строк экрана, соответственно. Амплитуда сигнала на заданной частоте будет указываться в вольтах. Для перевода измерения в [дБ] относительно 0,1 мВ в режиме «SA» нажать «SET», «8» затем «Enter».

8. С помощью источника тестовых сигналов необходимо последовательно задавать частоты, соответствующие средним значениям по октавным полосам (см. таблицу 1.1).

Аналогичные измерения уровня тестового сигнала  $L_c$  провести для всех необходимых частот.

9. Измеренные значения занести в таблицу 1.1. По результатам измерений построить АЧХ тестового акустического сигнала.

Таблица 1.1. Результаты определения уровней тестового акустического сигнала  $L_{c,i}$ , [дБ]

Частота, [Гц]	250	500	1000	2000	4000
$L_{c,i}$ , [дБ]					

**Определение акустических и виброакустических свойств ограждающей поверхности.**

1. На данном этапе работы производится оценка звукопоглощающих свойств ограждающих поверхностей, в качестве которых используются специальные перегородки, устанавливаемые в стенд. Для оценки звукопоглощающих свойств – перегородку расположить напротив отметок внутри стенда. Микрофон и акустический излучатель остаются на тех же местах, что и при первой серии измерений. Закрывать стенд.

2. По спектрограмме МПП ST-031, с помощью маркера, определить уровень сигнала, соответствующий  $L_{огр}$ . Оценить снижение уровня звукового сигнала за счет свойств перегородки по формуле  $a_{огр.i} \square L_{с.i} \square L_{огр.i}$ , дБ.

3. Произвести измерения на всех указанных в задании частотах. Принять решение о необходимости дополнительной защиты звуковой КИ, в том числе активными методами.

4. Открыть камеру и расположить виброакустический датчик МПП ST-031 в геометрическом центре перегородки – в данном случае это наиболее подверженная механическим колебаниям область. Присоединить вибродатчик к МПП ST-031 и произвести измерения уровня виброакустических колебаний  $L_{огр.в.i}$ , по аналогии с 6.5.-6.7, на всех заданных частотах.

Таблица 1.2. Результаты определения звукоизоляции ограждения

Частота, [Гц]	2 50	5 00	1 000	2 000	4 000
$L_{огр.i}$ , [дБ]					
$L_{огр.в.i}$ , [дБ]					
$a_{огр.i}$ , [дБ]					

По значениям  $a_{огр}$  построить АЧХ перегородки в акустическом и виброакустическом режимах.

### Оценка эффективности активной защиты КИ с помощью СВАЗ «Соната»

5. Выключить генератор. Установить на перегородку виброизлучатель (пьезоэлектрический ПИ-45, если используется стеклянная перегородка, а в

остальных случаях – «тяжелый» ВИ-45). Подключить к первому каналу СВАЗ «Соната» виброизлучатель (шлейф проводов первого канала выведен в стенде). Переключить работу канала, в режим виброакустики и установить максимальный (девятый) уровень мощности помехи.

6. Включить питание СВАЗ «Соната». По спектрограмме МПП ST-031, с помощью маркера, определить на каждой из заданных частот уровень составляющей помехи. Записать данные  $L_{ВШi}$  в таблицу 1.3.

7. Отсоединить виброакустический датчик и подключить к МПП ST-031 микрофон. Подключить аудиоизлучатель АИ-45 системы акустической защиты СВАЗ «Соната» к первому каналу (переключить канал в акустический режим) и включить данный прибор. Расположить АИ-45 рядом с включенным источником тестового сигнала и провести измерения уровней шумов, соответствующих номеру «9» на шкале прибора. Измерительный микрофон находится в том же положении, что и в первой серии измерений, но за ограждающей поверхностью. Произвести измерения аналогично п.6.15 для всех указанных частот. Результаты измерений  $L_{Ш1}$

...  $L_{Ш5}$  занесите в таблицу 1.3.

Таблица 1.3. Результаты определения отношений «сигнал/шум» в октавных полосах для заданной контрольной точки

Частота, [Гц]	50	100	200	500	1000
Уровень акустического шума в контрольной точке $L_{Шi}$ , [дБ]					
Уровень виброакустического шума в контрольной точке $L_{ВШi}$ , [дБ]					

Отношение сигнал/шум в контрольной точке $q_{Ai}$ , [дБ]					
Отношение сигнал/шум в контрольной точке $q_{Bi}$ , [дБ]					

8. Рассчитать для каждой октавной полосы отношение «сигнала/шум» в акустическом и виброакустическом режимах по формулам.

## 6. Содержание отчета

В отчете необходимо привести:

- формулировку цели и задания на выполнение работы;
- схему лабораторной установки;
- список приборов и оборудования;
- схемы выполненных измерений;
- таблицы значений измеренных величин и графики АЧХ для каждой серии измерений;
- расчет защищенности акустического сигнала;
- выводы по результатам выполненных исследований.

## 7. Контрольные вопросы

1. Физические основы акустического канала утечки.
2. Способы пассивной защиты акустического ТКУ КИ.
3. Способы активной защиты акустического ТКУКИ.
4. Как выбираются частоты сигнала при оценке защищенности акустического ТКУКИ?
5. Что такое октавная полоса звуковых частот?

6. Как образуется виброакустический ТКУКИ?
7. В чем состоят различия акустического и виброакустического сигналов утечкиКИ?
8. Метод оценки утечки КИ по виброакустическомуТКУ.
9. Основные режимы работы МПП ST-031«Пиранья».
10. Какими датчиками комплектуется МПП ST-031 для контроля акустического и виброакустического ТКУ КИ, их принцип работы и основныехарактеристики?
11. Достоинства и недостатки пассивных средств защиты речевойКИ.
12. Достоинства и недостатки активных средств защиты речевой КИ.
13. Рекомендации по установке излучателей СВАЗ«Соната».

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

- 1) Волхонский, В. В. Системы охранной сигнализации [Текст] / В. В. Волхонский. – СПб. : Экополис и культура, 2005.
- 2) ГОСТ Р 50775-95. Системы тревожной сигнализации. Ч. 1. Общие требования. Разд. 1. Общие положения. – М. : Изд-во стандартов, 1995
- 3) ГОСТ Р 50776-95. Системы тревожной сигнализации. Ч. 1. Общие требования. Разд. 4. Руководство по проектированию, монтажу и техническому обслуживанию. – М. : Изд-во стандартов, 1995.
- 4) Лепешкин, О. М. Комплексные средства безопасности и технические средства охранно-пожарной сигнализации : учеб. пособие [Текст] / О. М. Лепешкин. – М. : Гелиос АРВ, 2009.
- 5) Магауенов, Р. Г. Системы охранной сигнализации: основы теории и принципы построения [Текст] / Р. Г. Магауенов. – М. : Горячая линия – Телеком, 2008.
- 6) Синилов, В. Г. Защита объектов современными средствами безопасности [Текст] / В. Г. Синилов. – 5-е изд., перераб. и доп. – М. : Торговый Дом ТИНКО, 2010.