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
_____ 2017 г.

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. Спеваков*

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 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 60х84 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

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.

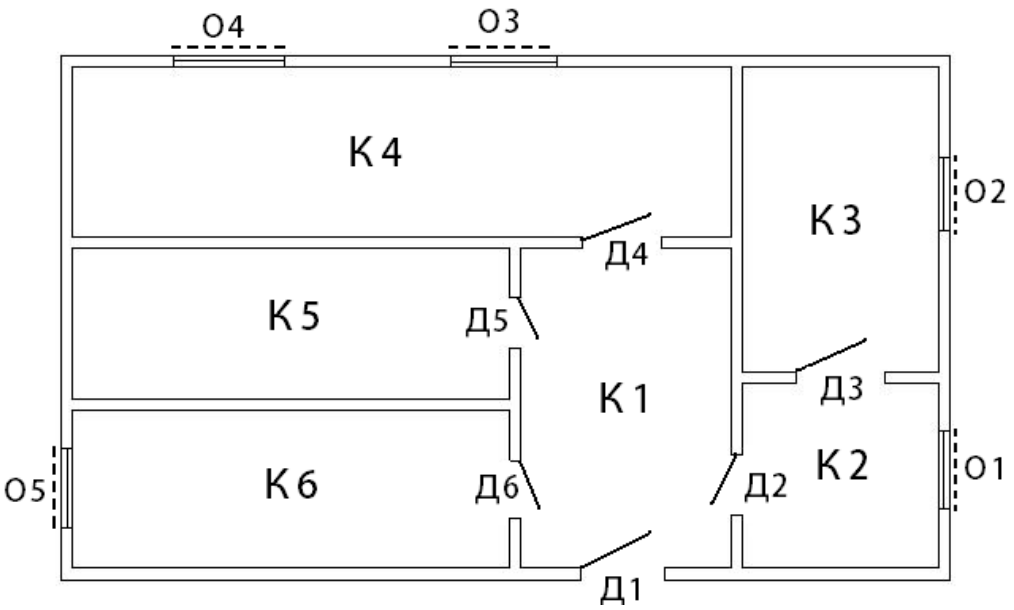

Рис. 1 – План помещений

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.

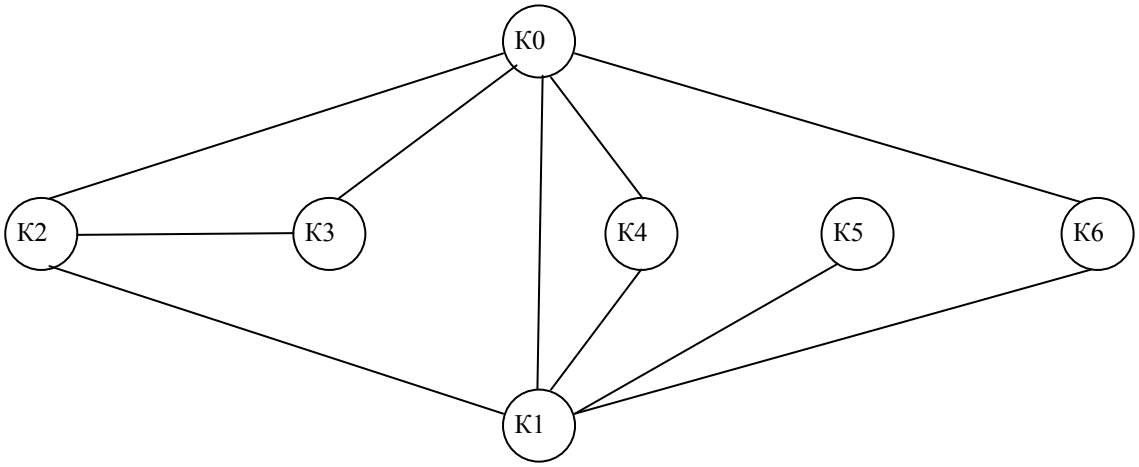

Рис. 2 – Граф путей доступа в помещение

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.

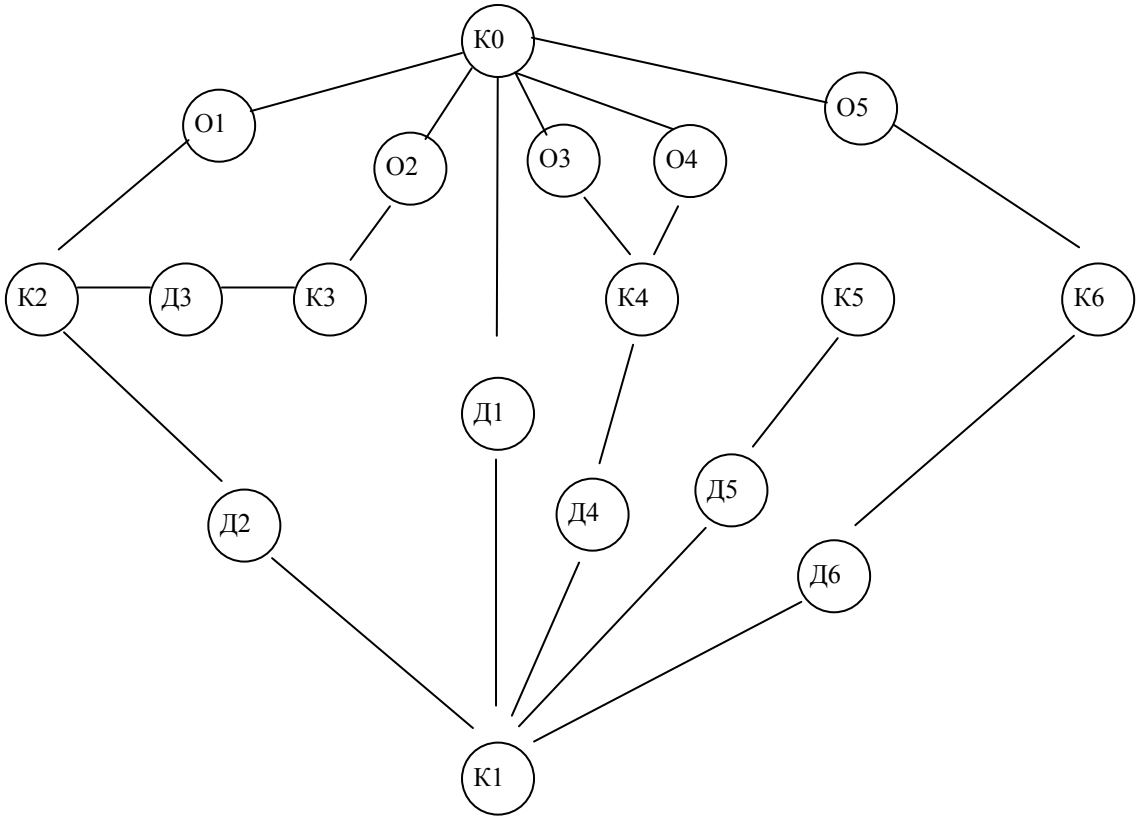

Рис. 3 – Граф путей доступа в помещение через возможные каналы доступа.

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 равносилен доступу в другую. Для наглядности примера предположим, что дверь Д2 не имеет замков. Таким образом доступ в помещение К2 равносилен 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.

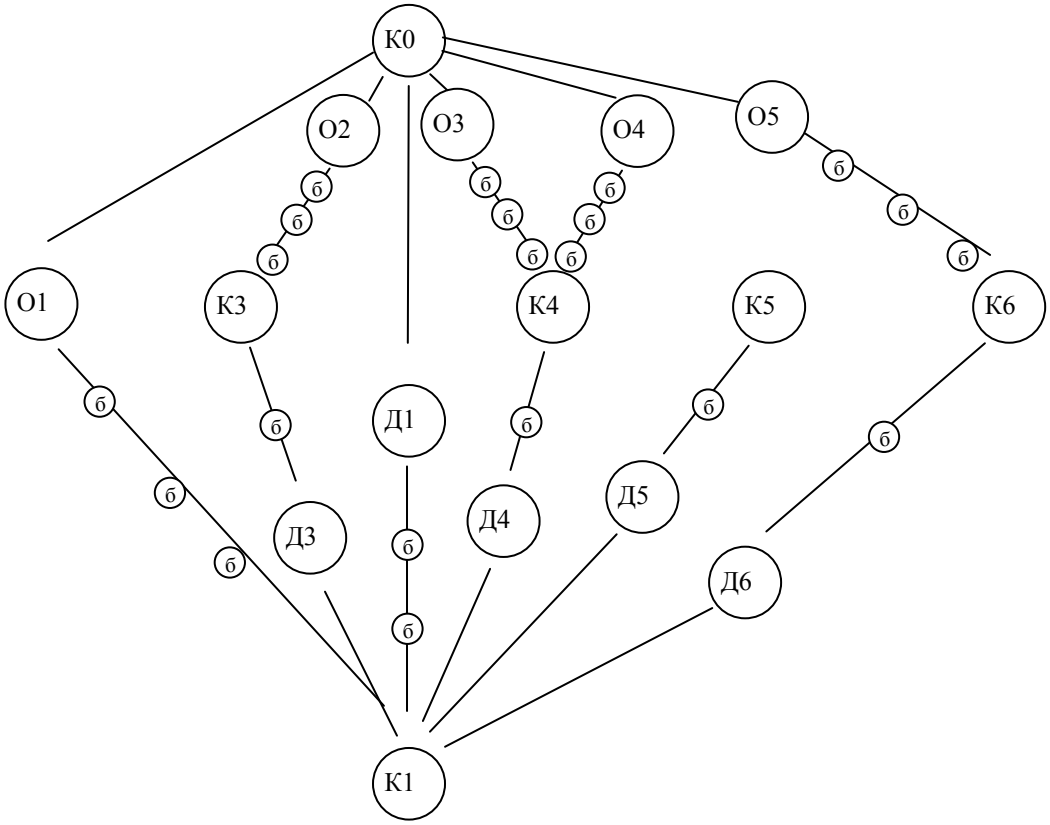

Рис. 4 - Граф путей доступа в помещение через возможные каналы доступа с указанием возможных барьеров.

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

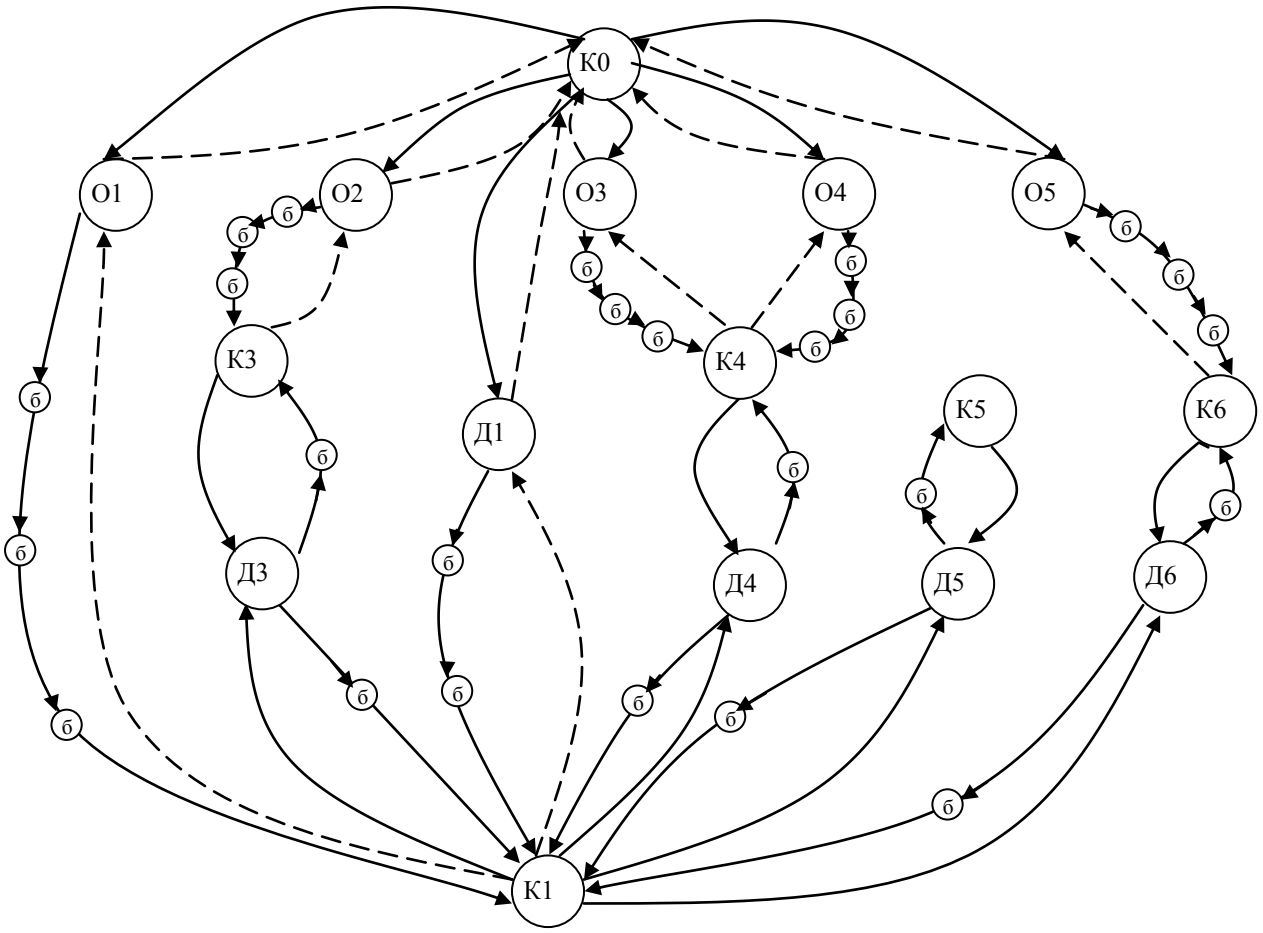

Рис. 5- Орграф путей доступа в помещение.

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.

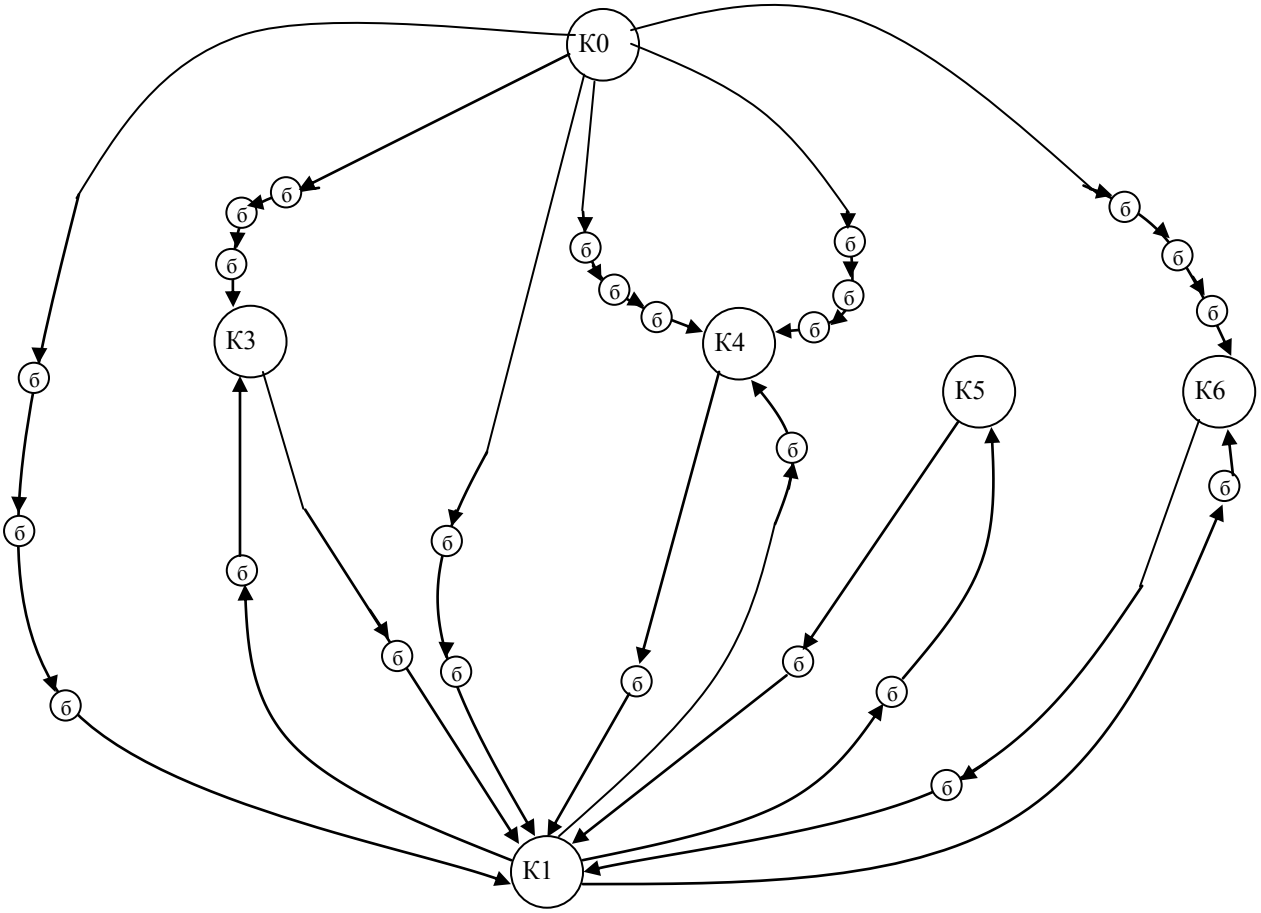

Рис. 6- упрощенный граф путей доступа в помещение

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 К0. Все переходы, начинающиеся в вершине К0, 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 К0 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)

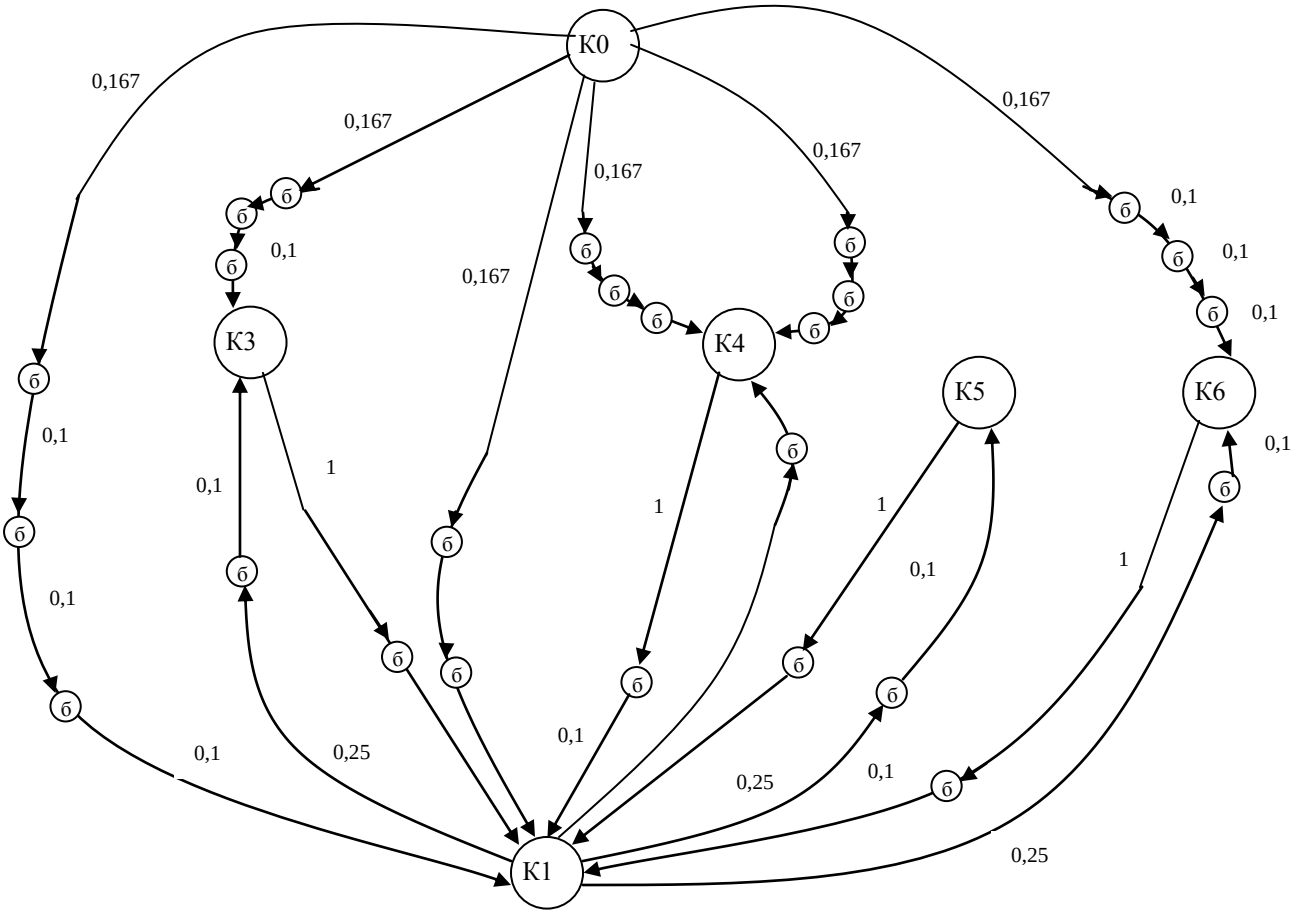

Рис. 7- Граф путей доступа с указанием веса дуг.

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

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

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).

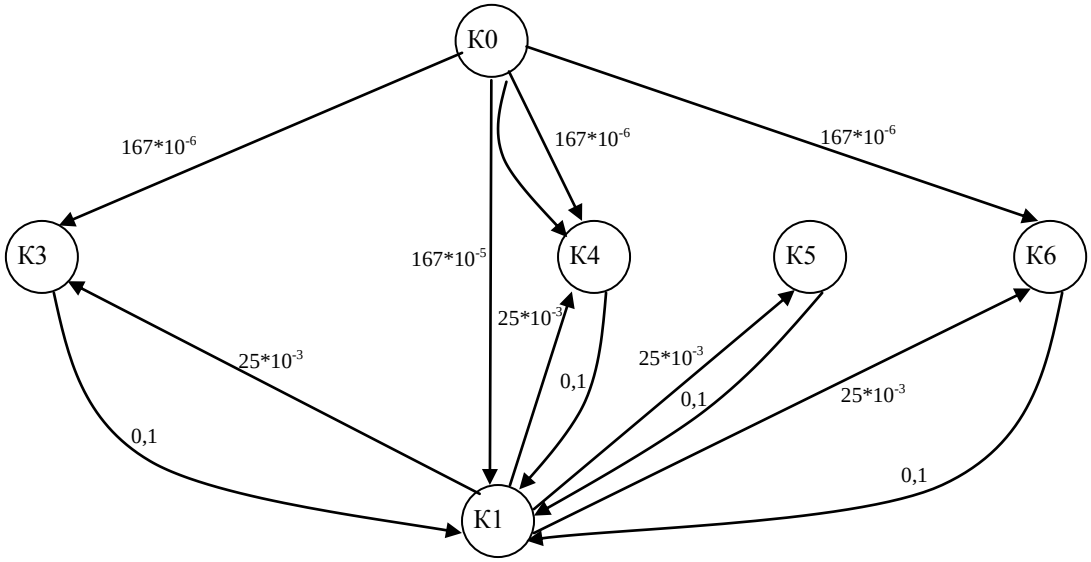

Рис. 8 – Упрощенный граф путей доступа

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:

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

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):

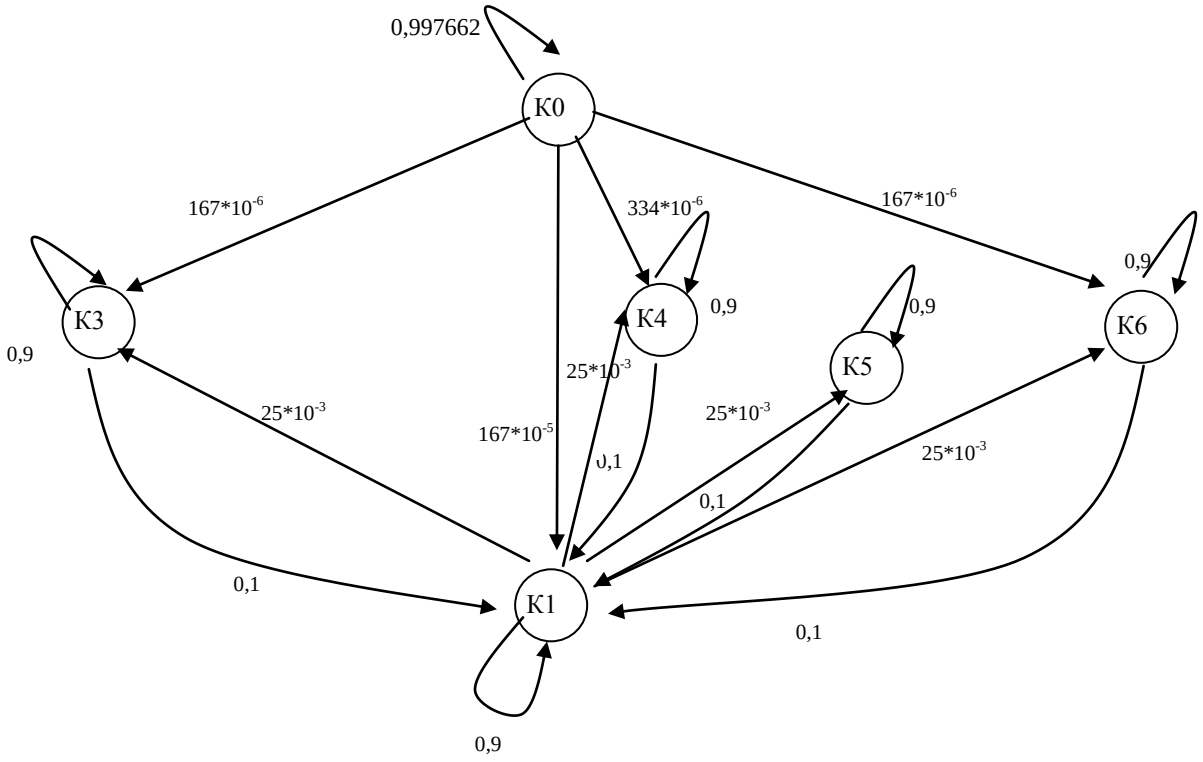

Рис. 9- Конечный граф путей доступа в помещение

Для данного графа матрица переходных вероятностей будет иметь следующий вид:

	К0	К1	К3	К4	К5	К6
Из К0	0,997662	$167*10^{-5}$	$167*10^{-6}$	$334*10^{-6}$	0	$167*10^{-6}$
Из К1	0	0,9	$25*10^{-3}$	$25*10^{-3}$	$25*10^{-3}$	$25*10^{-3}$
Из К3	0	0,1	0,9	0	0	0
Из К4	0	0,1	0	0,9	0	0
Из К5	0	0,1	0	0	0,9	0
Из К6	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:

$$P_j(k) = M_0 \cdot P^k \cdot D_j \text{ , (3)}$$

где $M_0 = [P_1(0) \;\; P_2(0) \;\; \ldots \;\; P_N(0)]_{1\times N}$ – вектор-строка начального состояния системы; $P = |p_{ij}|_{N\times N}$ – квадратная матрица переходных вероятностей; $D_j = [0 \;\; 0 \;\; \ldots \;\; 1 \;\; \ldots \;\; 0]^T_{N\times 1}$ – 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).

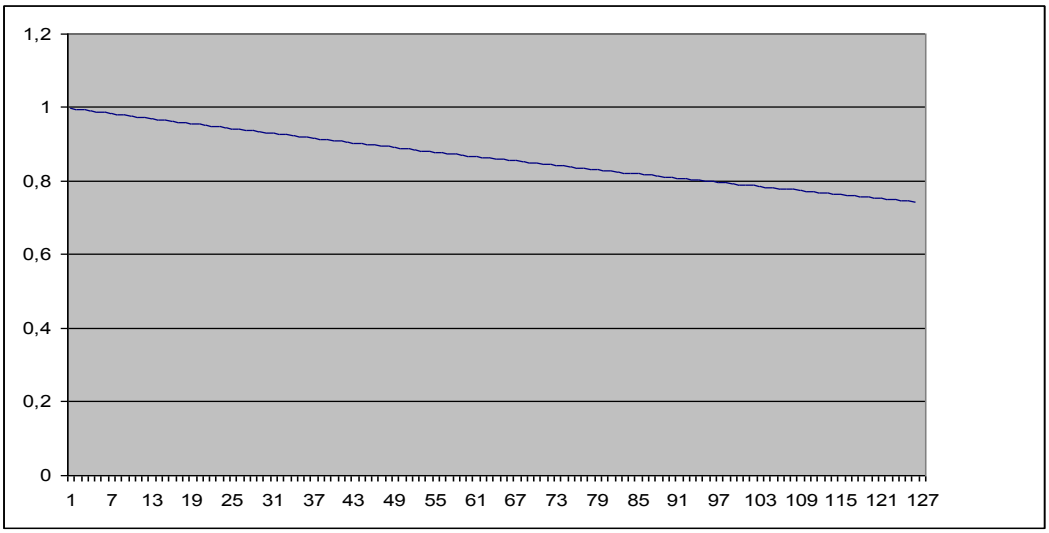

Рис. 11- График вероятности доступа в помещение 1

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

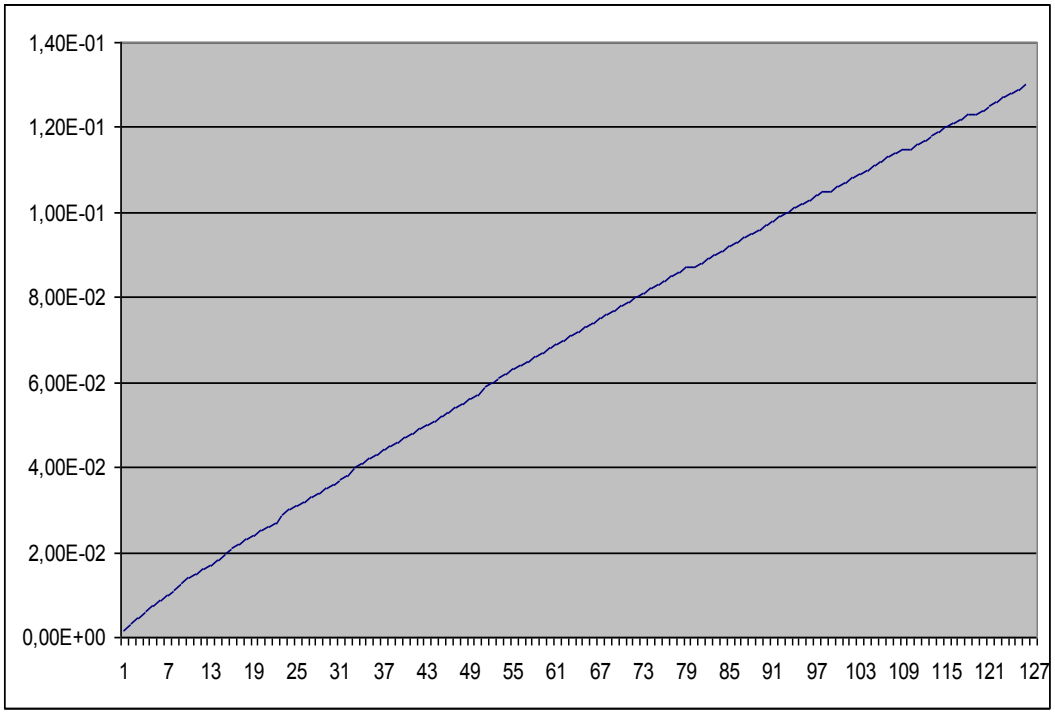

Рис. 12- График вероятности доступа в помещение 2.

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.