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.

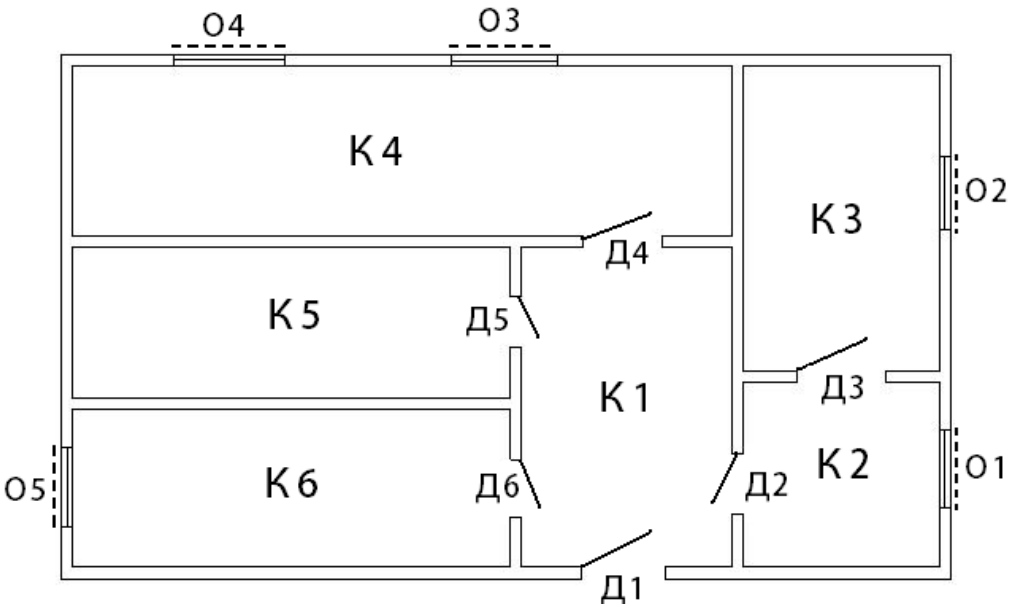


Рис. 1 – План помещений

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.

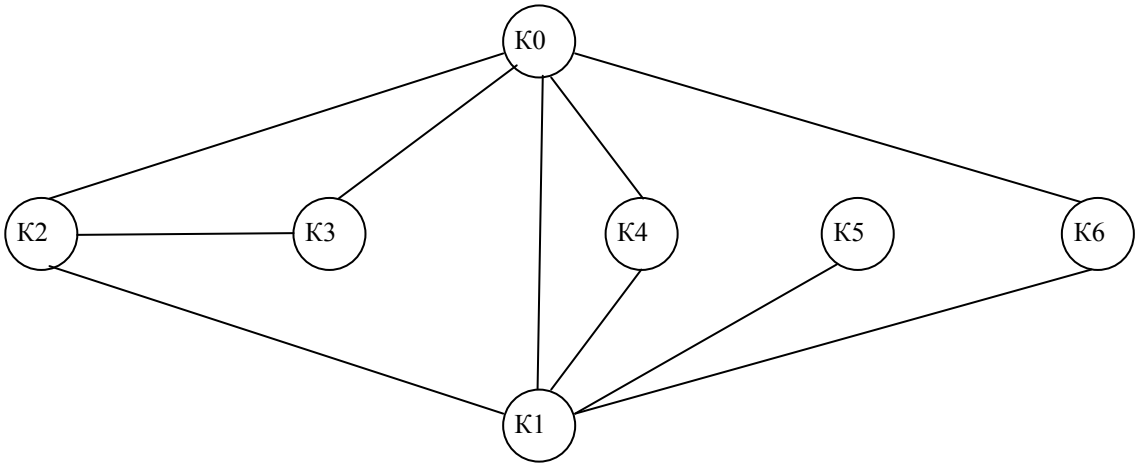


Рис. 2 – Граф путей доступа в помещение

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.

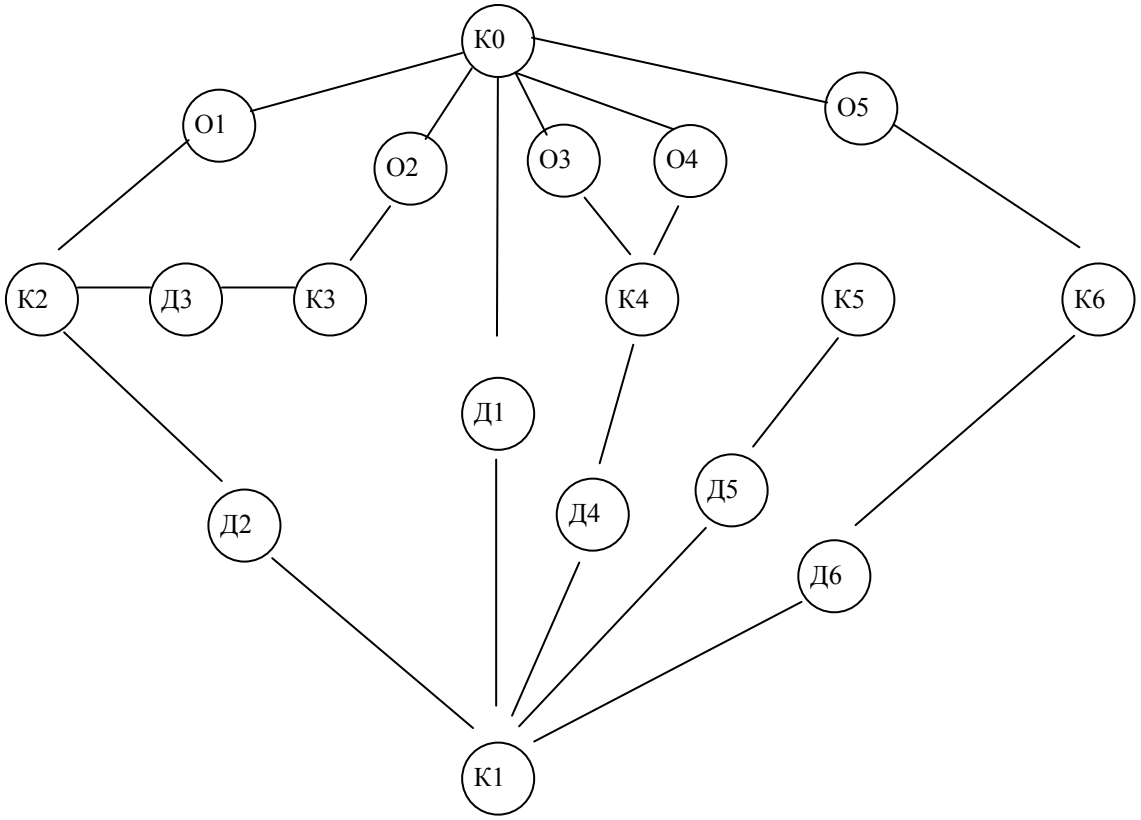


Рис. 3 – Граф путей доступа в помещение через возможные каналы доступа.

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.

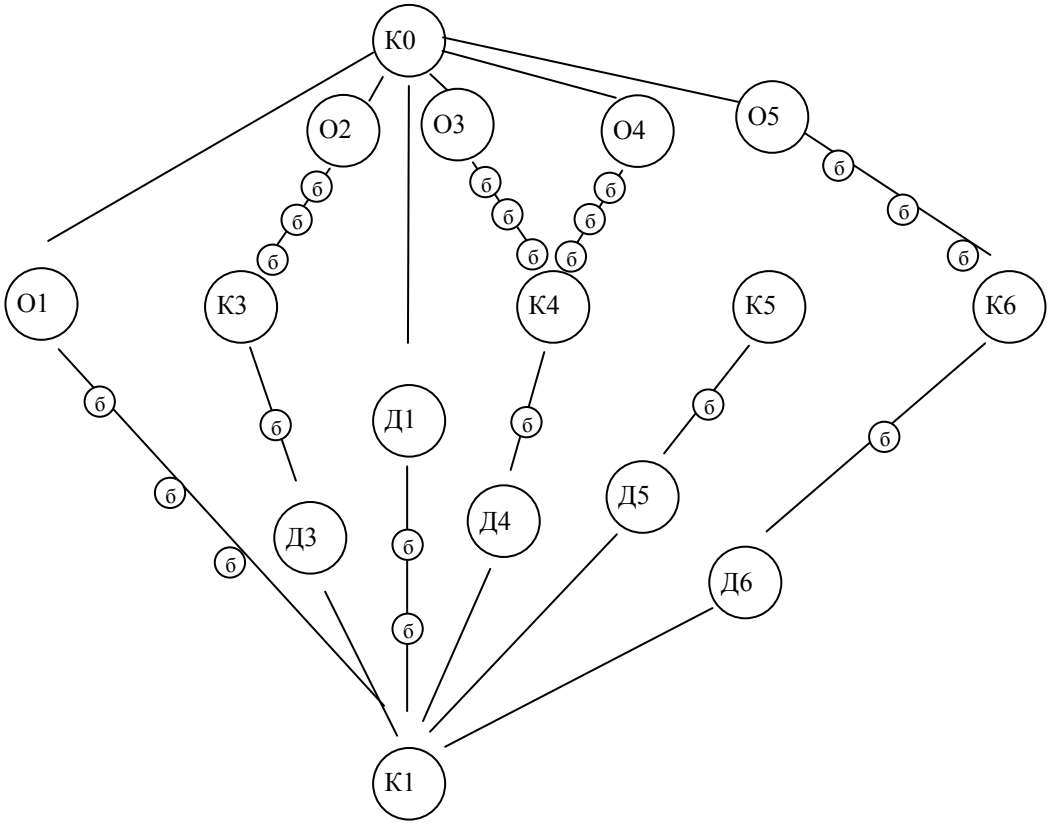


Рис. 4 - Граф путей доступа в помещение через возможные каналы доступа с указанием возможных барьеров.

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

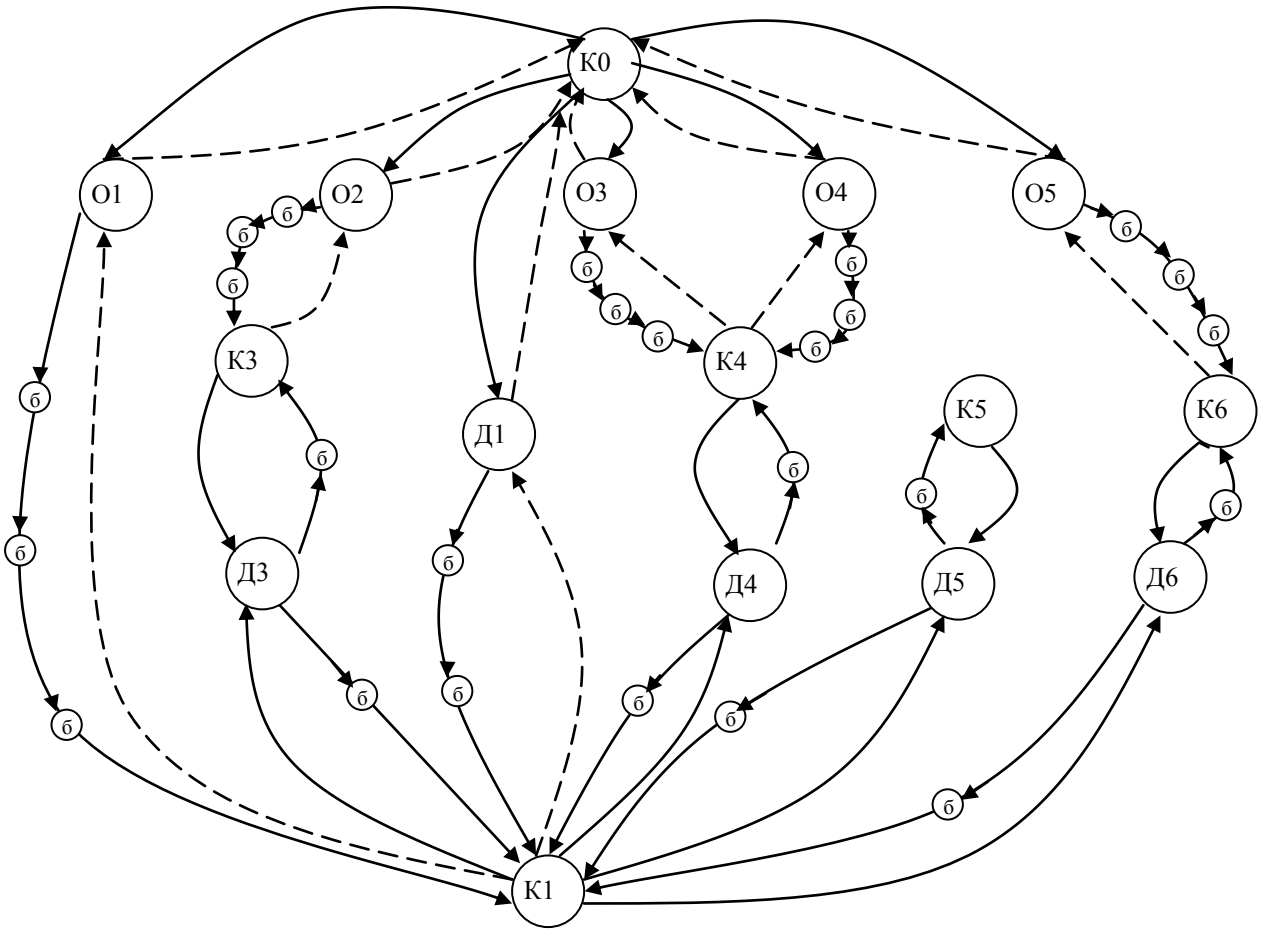


Рис. 5- Орграф путей доступа в помещение.

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.

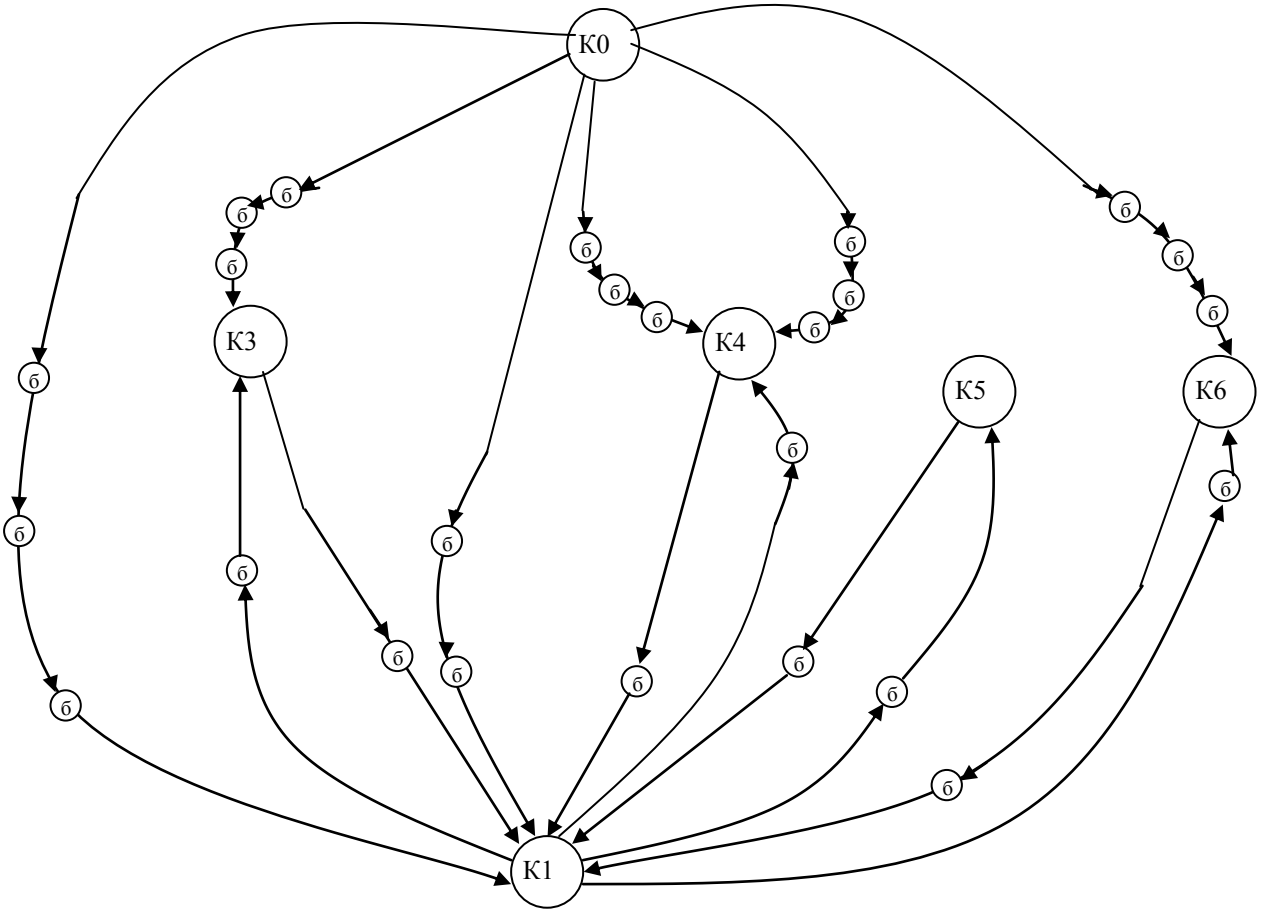


Рис. 6- упрощенный граф путей доступа в помещение

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)

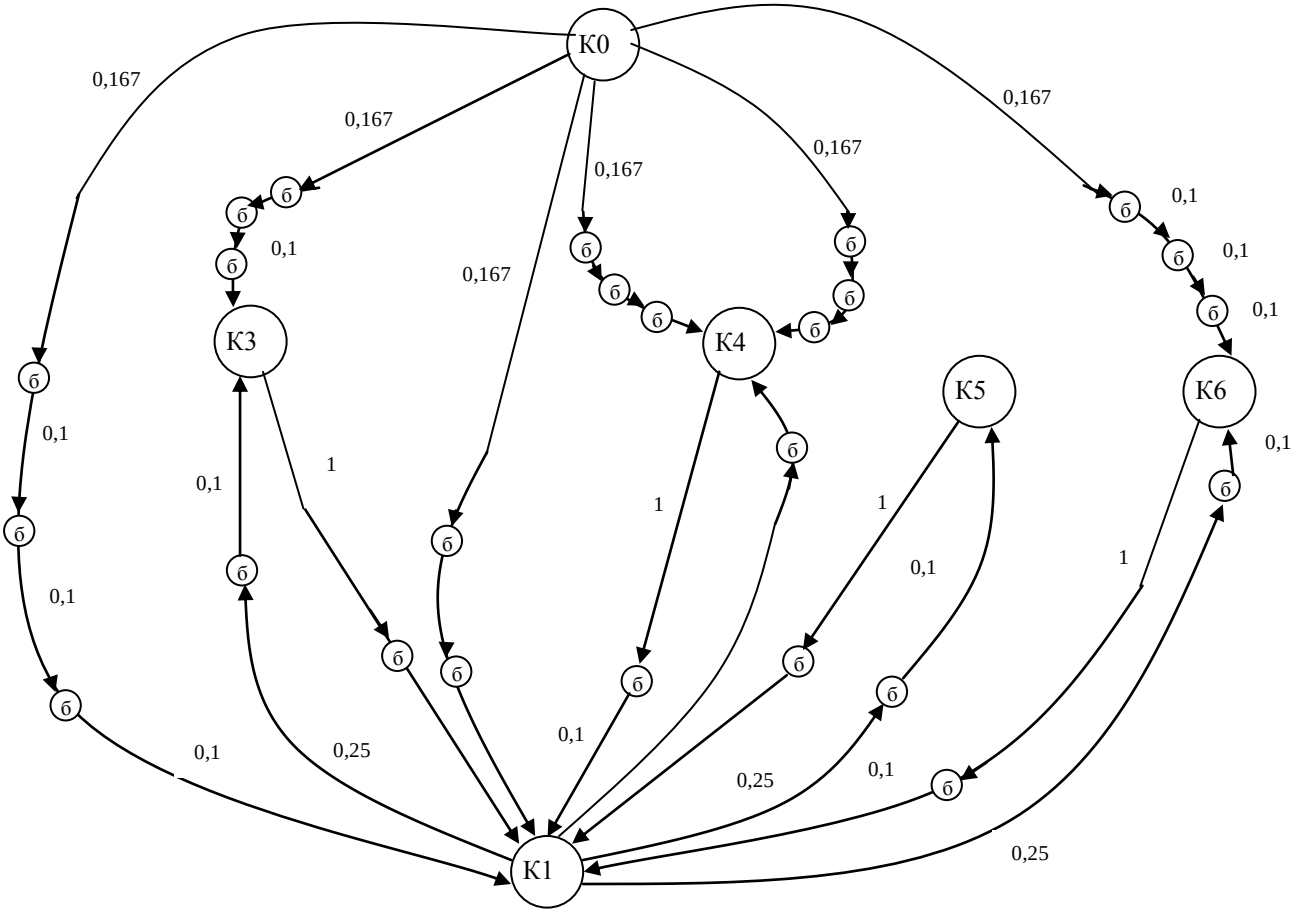


Рис. 7- Граф путей доступа с указанием веса дуг.

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).

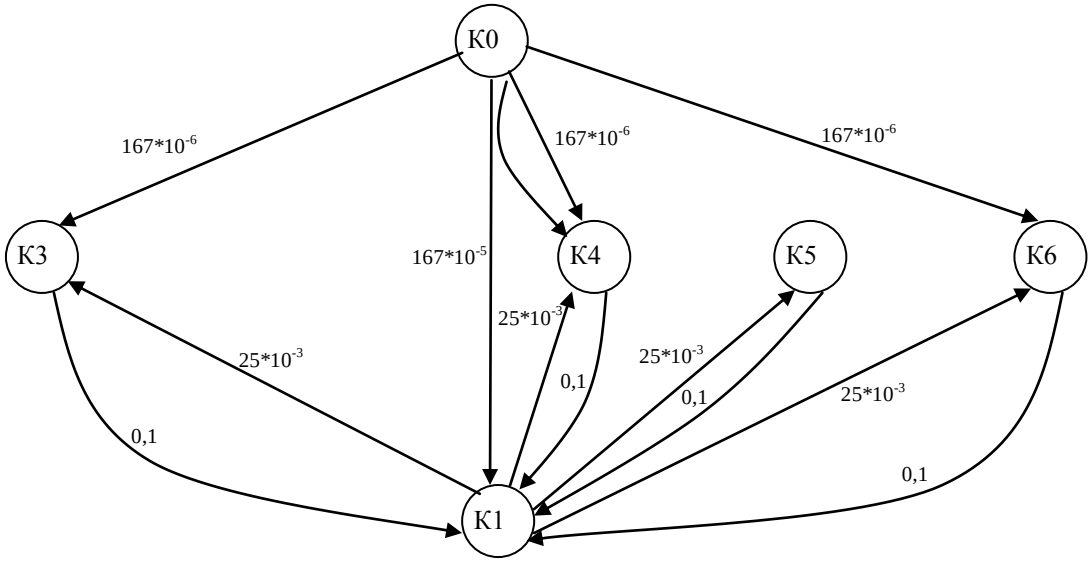


Рис. 8 – Упрощенный граф путей доступа

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):

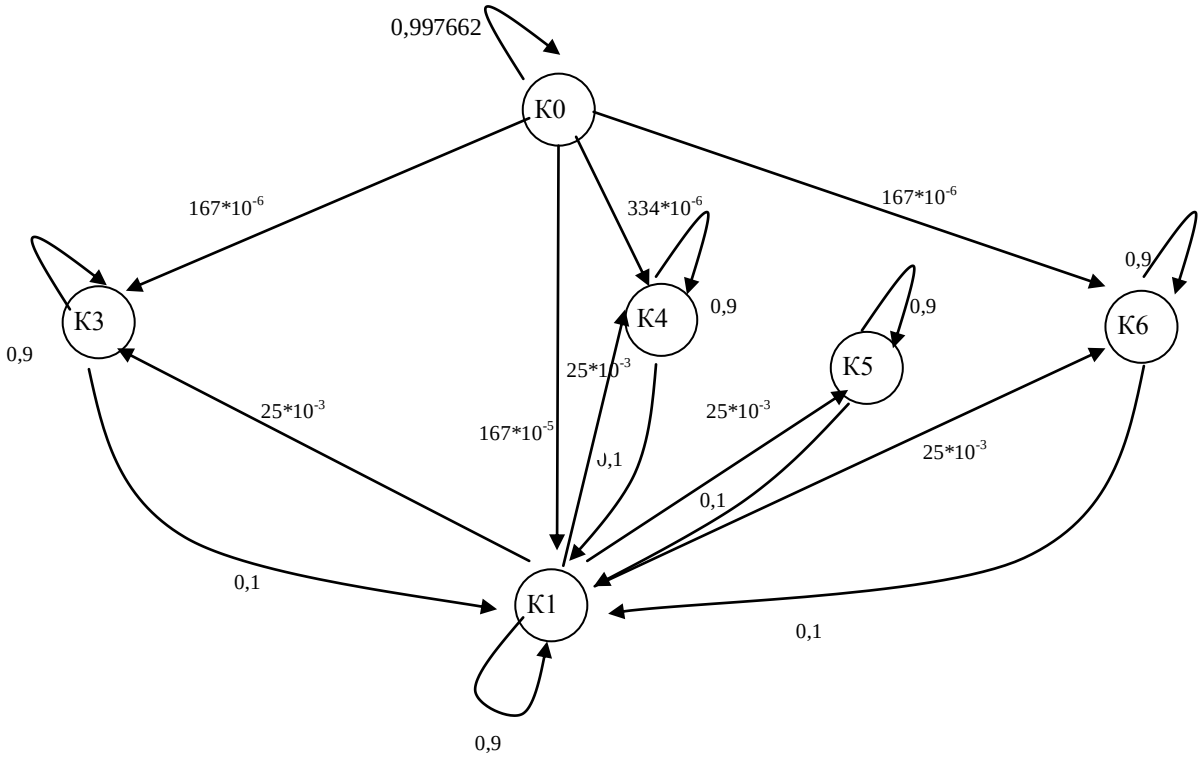


Рис. 9- Конечный граф путей доступа в помещение

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:

$$P_j(k) = M_0 \cdot P^k \cdot D_j, \quad (3)$$

где $M_0 = [P_1(0) \;\; P_2(0) \;\; \ldots \;\; P_N(0)]_{1\times N}$ – вектор-строка начального состояния системы; $P = \lfloor p_{ij} \rfloor_{N\times N}$ – 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).

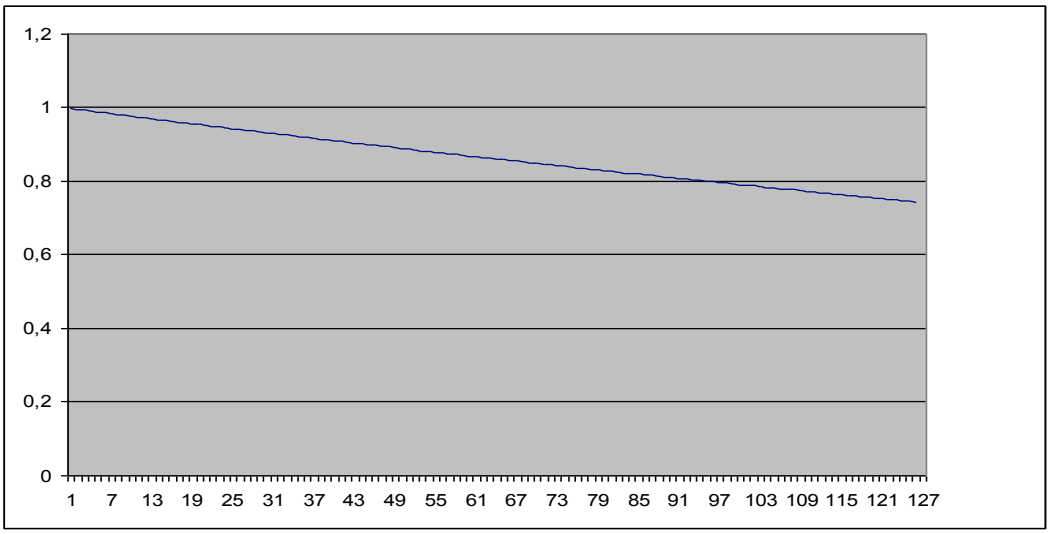


Рис. 11- График вероятности доступа в помещение 1

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

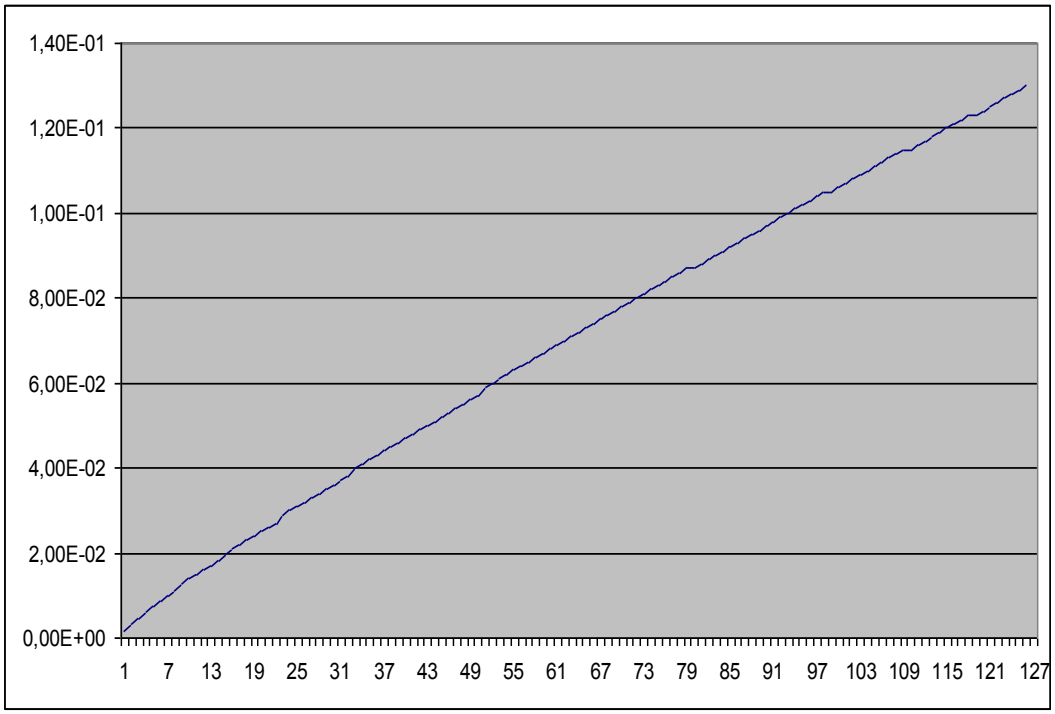


Рис. 12- График вероятности доступа в помещение 2.

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.

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.

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. Спеваков*

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 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

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.

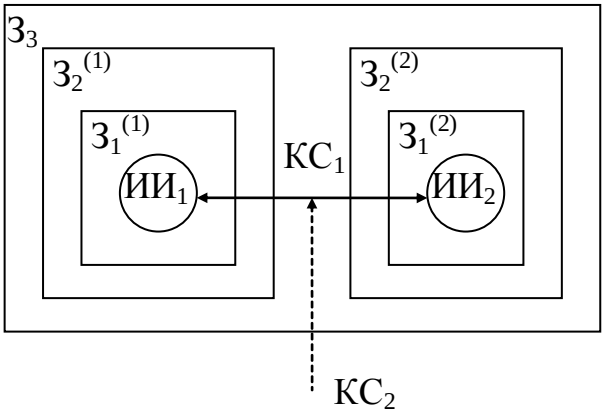


Рис. 1

Пусть $P_{угр}$ – вероятность возникновения угрозы.
Вероятность того, что все зоны защиты правильно функционируют, равна:

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

Вероятность того, что произошел НСД, равна:

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

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 y_i, равна: $P_{yi}(t)=1-e^{-\lambda_i t}$, где λ - интенсивность НСД (относительное число НСД в единицу времени).
Если $\lambda_i << 1$, то $P_{yi}(t)\approx \lambda_i t$.

3. ПОСТАНОВКА ЗАДАЧИ

1) элементарные случайные события:
$A^{(1)}$ - нарушитель разрушил защиту в $З_1^{(1)}$,
$A^{(2)}$ - нарушитель разрушил защиту в $З_1^{(2)}$,
$B^{(1)}$ - нарушитель разрушил защиту в $З_2^{(1)}$,
$B^{(2)}$ - нарушитель разрушил защиту в $З_2^{(2)}$,
C - нарушитель разрушил защиту в $З_3$,
$Д^{(1)}$ - нарушитель получил НСД к $ИИ_1$ через $КС_1$,
$Д^{(2)}$ - нарушитель получил НСД к $ИИ_2$ через $КС_1$,
E - нарушитель получил НСД к $ИИ_1$ и $ИИ_2$ через $КС_2$.

2) интенсивности наступления перечисленных выше событий λ (см.варианты):

Вариант	$\lambda\{A^{(1)}\}$	$\lambda\{A^{(2)}\}$	$\lambda\{B^{(1)}\}$	$\lambda\{B^{(2)}\}$	$\lambda\{C\}$	$\lambda\{Д^{(1)}\}$	$\lambda\{Д^{(2)}\}$	$\lambda\{E\}$
	1	2	3	4	5	6	7	8
1	0,0007	0,0007	0,0025	0,0001	0,00295	0,00005	0,00385	0,00325
2	0,0006	0,0004	0,0045	0,0002	0,00285	0,00007	0,00455	0,00255
3	0,0008	0,0005	0,0015	0,0004	0,00325	0,00008	0,00556	0,00225
4	0,0125	0,0002	0,0025	0,0001	0,00355	0,00005	0,00425	0,00225
5	0,0005	0,0005	0,0015	0,0001	0,00025	0,00005	0,00225	0,00456

4. ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

1. Подсчитать вероятности событий 1-8 при T=500 часов.
2. Найти вероятности сложных событий:

$P\{Д^{(1)} + E\}=P\{Д^{(1)}\} + P\{E\} - P\{Д^{(1)}\}\cdot P\{E\}$,
$P\{Д^{(2)} + E\}=P\{Д^{(2)}\} + P\{E\} - P\{Д^{(2)}\}\cdot P\{E\}$,
$P\{СВ^{(1)}\ А^{(1)}\}=P\{C\}\cdot P\{В^{(1)}\}\cdot P\{А^{(1)}\}$,
$P\{СВ^{(2)}\ А^{(2)}\}=P\{C\}\cdot P\{В^{(2)}\}\cdot P\{А^{(2)}\}$,
$P\{СВ^{(1)}\ А^{(1)} + СВ^{(2)}\ А^{(2)}\}=1 - (1 - P\{СВ^{(1)}\ А^{(1)}\})(1 - P\{СВ^{(2)}\ А^{(2)}\})$,
$P\{E + СВ^{(1)}\ А^{(1)} + СВ^{(2)}\ А^{(2)}\}=1 - (1 - P\{E\})(1 - P\{СВ^{(1)}\ А^{(1)}\})(1 - P\{СВ^{(2)}\ А^{(2)}\})$.

3. Построить график изменения вероятности $P\{E + СВ^{(1)}\ А^{(1)} + СВ^{(2)}А^{(2)}\}$ от времени при T=(0÷1000) часов.
4. Уменьшить наибольшую интенсивность в 4 раза и посмотреть, как это повлияло на изменение вероятности $P\{E + СВ^{(1)}\ А^{(1)} + СВ^{(2)}\ А^{(2)}\}$ от времени (построить график).
5. Определить, во сколько раз требуется уменьшить все интенсивности, чтобы вероятность $P\{E + СВ^{(1)}\ А^{(1)} + СВ^{(2)}\ А^{(2)}\}$ 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

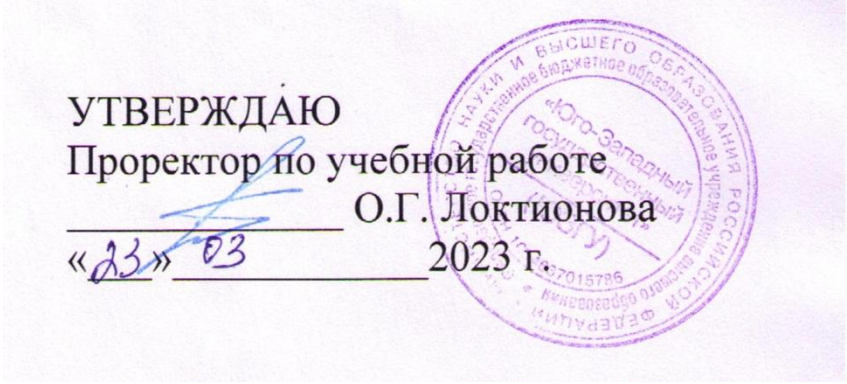
1. Н. В. Гришина. Организация Комплексной Системы Защиты Информации. [Электронный ресурс] : статья / - Электрон. дан. - Режим доступа: http://coollib.com/b/166590/read

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

МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности



КРИТЕРИИ ОЦЕНКИ И ВЫБОРА CASE-СРЕДСТВ

Методические указания по выполнению практических работ для студентов укрупненной группы специальностей и направлений подготовки 10.00.00

Курск 2023

УДК 004.725

Составитель: А.В. Митрофанов

Рецензент

Кандидат технических наук, доцент кафедры «Информационная безопасность» А.Л. Марухленко

Критерии оценки и выбора case-средств: методические указания к выполнению практических работ по дисциплине «Проектирование защищенных телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: А. В. Митрофанов. Курск, 2023. 10 с. Библиогр.: с. 10.

Указывается порядок выполнения практической работы, правила оформления, содержание отчета.

Методические указания по выполнению практических работ по дисциплине «Проектирование защищенных телекоммуникационных систем», предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00

Текст печатается в авторской редакции

Подписано в печать _____. Формат 60×84 1/16.
Усл.печ.л. . Уч.-изд.л. . Тираж 50 экз. Заказ ____. Бесплатно
Юго–Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Описать и проанализировать информационную систему.

2. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

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:

a. 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.

b. 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.

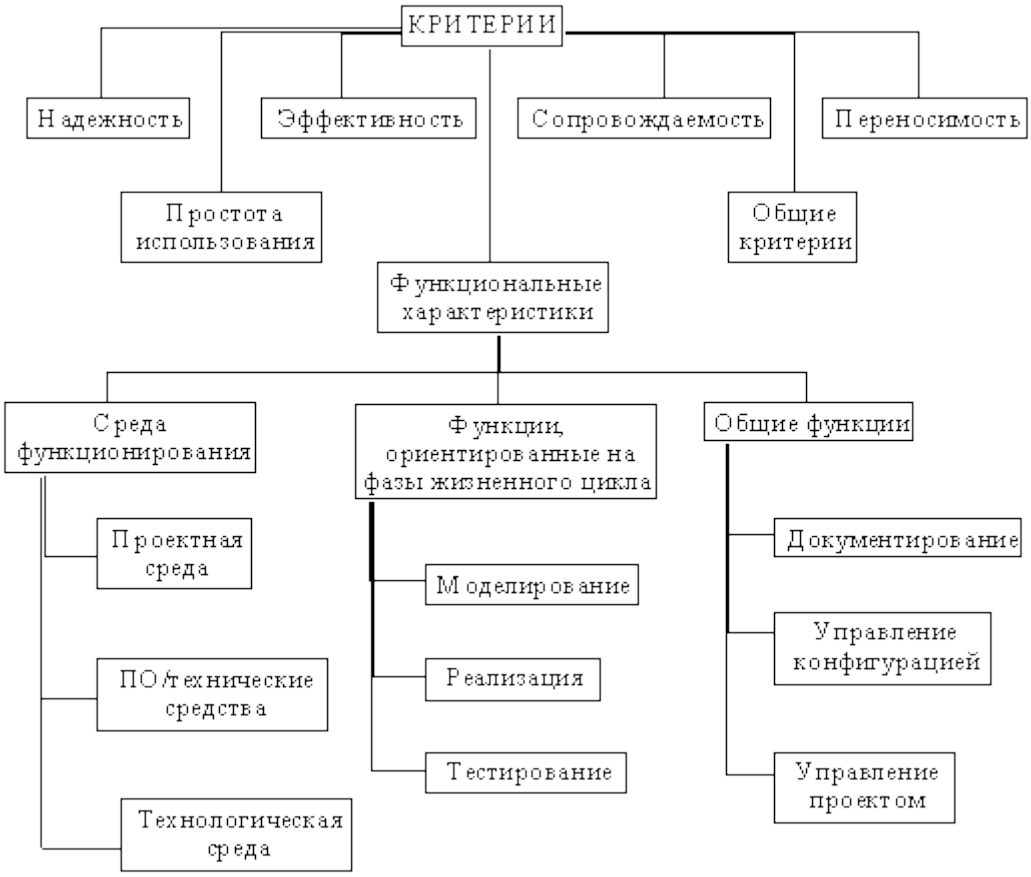


Рис. 1 - Структура набора критериев

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. Требует 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.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить предлагаемый теоретический материал.
2. Составить подробное описание информационной системы.
3. На основании описания системы провести анализ осуществимости. В ходе анализа ответить на вопросы:

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

Результатом анализа должно явиться заключение о возможности реализации проекта.

4. Распределить роли в группе (руководитель проекта-разработчик, системный аналитик-разработчик, тестер-разработчик).
5. Заполнить разделы плана:

- Введение
- Организация выполнения проекта
- Анализ рисков

Разделы должны содержать рекомендации относительно разработки системы, базовые предложения по объёму требуемого бюджета, числу разработчиков, времени и требуемому программному обеспечению.

6. Составить отчет о проделанной работе.

4. СОДЕРЖАНИЕ ОТЧЕТА

В отчете следует указать:

1. Цель работы
2. Введение. Краткое описание целей проекта и проектных ограничений (бюджетных, временных и т.д.), которые важны для управления проектом
3. Описание информационной системы (ПО) - наличие заключения о возможности реализации проекта, содержащего рекомендации относительно разработки системы, базовые предложения по объёму требуемого бюджета, числу разработчиков, времени и требуемому программному обеспечению
4. Анализ осуществимости (согласно требованиям к результатам выполнения лабораторного практикума п.2), указать возможные проблемы и пути их решения.
5. Роли участников группы разработки ПО.
6. Программно-аппаратные средства, используемые при выполнении работы.
7. Заключение (выводы)

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) Шувалов 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 изд. Учебн. пособие. – М.: Радио и связь. 2000. – 368 с.

3) Цифровые и аналоговые системы передачи: Учебник для вузов/ В.И.Иванов, В.Н.Гордиенко, Г.Н.Попов и др.; Под ред. В.И.Иванова. – 2-е изд. – М.: Горячая линия – Телеком, 2003. – 232 с.

4) Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: Учебник для ВУЗов. - СПб.: БХВ-Петербург, 2010. - 400 с.

5) Башарин Г.П. Лекции по математической теории телетрафика: Учеб. пособие. Изд. 3-е, испр. и доп. - М.: РУДН, 2009. - 342 с.

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

7) Леоненков А.В. Самоучитель языка UML. – СПб.: БХВ-Петербург, 2004.

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

9) 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

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
_____ 2017 г.

Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности

Методические указания по выполнению практической работы

Курск 2017

УДК 621.(076.1)
Составители: Е.С.Волокитина,М.О. Таныгин.

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

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 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 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 защитыв 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 Гостехкомисии 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/