

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 08.02.2021 16:51:23
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

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

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.

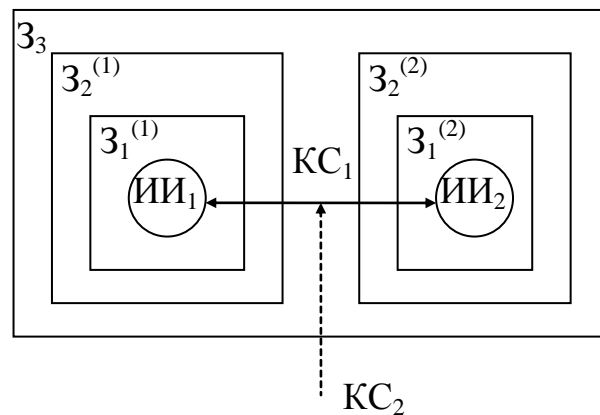


Рис. 1

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 λ - 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 ИИ₁ через KC_1 ,

$D^{(2)}$ - нарушитель получил НСД к ИИ₂ через KC_1 ,

E - нарушитель получил НСД к ИИ₁ и ИИ₂ через KC_2 .

2) интенсивности наступления перечисленных выше событий

λ (см. варианты):

Вариант	$\lambda\{A^{(1)}\}$	$\lambda\{A^{(2)}\}$	$\lambda\{B^{(1)}\}$	$\lambda\{B^{(2)}\}$	$\lambda\{C\}$	$\lambda\{D^{(1)}\}$	$\lambda\{D^{(2)}\}$	$\lambda\{E\}$
	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