**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования**

**«Юго-Западный государственный университет»**

**Кафедра ЗИиСС**

**Практическая работа №4**

**на тему: «Основные методы управления информационной безопасностью в ГИС».**

**Ст. преподаватель к.т.н., Волокитина Е.С.**

**2014 г.**

**Цель работы**

Целью данной лабораторной работы является оценка показателей качества функционирования комплексной системы защиты информации на предприятии, расчет защищенности от физического проникновения и от несанкционированного доступа в локальную сеть.

**Постановка задачи**

1. **План предприятия и назначение помещений:**

1. проходная;
2. помещение охраны;
3. операторская;
4. операторская;
5. бухгалтерия;
6. кабинет директора;
7. приемная;
8. библиотека;
9. комната для переговоров.

В соответствии с описанием помещений составить собственную графическую схему.

1. **Перечень информации, циркулирующей на предприятии**

| Перечень информации | *Возможные потери, руб* |
| --- | --- |
| Плановая документация | 100000 |
| Информационно-справочная и справочно-аналитическая документация | 150000 |
| Отчетная документация | 80000 |
| Документация по обеспечению кадрами | 50000 |
| Финансовая документация | 1000000 |
| Материально-техническое снабжение | 50000 |
| Договорная документация | 200000 |

1. **Параметры локальной сети и список сотрудников**

*Параметры локальной сети:*

Количество компьютеров – 7;

Сеть на витой паре Ethernet 100Мбит;

*Персонал состоит из постоянного и переменного состава*

1) Постоянный:

* генеральный директор;
* зам. директора;
* юрист;
* секретарь;
* администратор сети и безопасности;
* сотрудники – 3 человека;
* программист;
* охранники – 3 человека;
* уборщицы – 2 человека.

2) Переменный состав:

* группа поиска – 3 человека;
* бухгалтер;
* электрик-телефонист;
* заказчики.

1. **Перечень угроз с учетом возможных потерь**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *№* | *Угроза* | *Объект угрозы* | *Опасность угрозы в баллах от 1 до 100* | *Возможные потери* |
| 1 | Утечка за счет структурного звука в стенах и перекрытиях | Переговоры | 20 | 50 тыс. |
| 2 | Съем информации с плохо стертых дискет | Информация на дискетах | 40 | Незначительные |
| 3 | Программно-аппаратные закладки в ПЭВМ | Информация в локальной сети | 50 | 90 тыс. |
| 4 | Радио-закладки в стенах и мебели | Секретные переговоры | 70 | 90 тыс. |
| 5 | Съем информации по системе вентиляции | Разговоры | 40 | Незначительные |
| 6 | Лазерный съем акустической информации с окон | Секретные переговоры | 70 | 90 тыс. |
| 7 | Производственные и технологические отходы | Служебная и профессиональная тайны | 20 | Незначительные |
| 8 | Компьютерные вирусы, логические бомбы и т.п | Информация в локальной сети | 50 | 90 тыс. |
| 9 | Съем информации за счет наводок и навязывания | Секретные переговоры, информация в локальной сети | 80 | 90 тыс. |
| 10 | Дистанционный съем видеоинформации | персонал, клиенты | 40 | 50 тыс. |
| 11 | Съем акустической информации с использованием диктофонов | Разговоры, переговоры | 70 | 50 тыс. |
| 12 | Хищение носителей информации | Документированная информация, информация на НЖМД | 40 | 90 тыс. |
| 13 | Высокочастотный канал утечки в бытовой технике | переговоры | 30 | незначительные |
| 14 | Съем информации направленным микрофоном | Переговоры, разговоры | 30 | 50 тыс. |
| 15 | Внутренний канал утечки (обслуживающий персонал, несанкционированное копирование); | Информация на НЖМД, документированная информация, переговоры | 80 | 90 тыс. |
| 16 | Утечка за счет побочного излучения терминалов | Компьютерная информация, разговоры | 40 | 90 тыс. |
| 17 | Съем информации с телефонного уха | Телефонные переговоры | 50 | незначительные |
| 18 | Визуальный съем с дисплея и принтера | Различная информация | 20 | незначительные |
| 19 | Утечка по линиям связи | переговоры | 80 | 50 тыс. |
| 20 | Утечка по цепям заземления | Различная информация | 20 | незначительные |
| 21 | Утечка по цепи электропитания | Переговоры | 40 | 50 тыс. |

**2. Расчет защищенности от физического проникновения**

2.1. **Для поставленной задачи рассчитать вероятность доступа в помещения предприятия** (для построения графов можно воспользоваться программой *Deadlock*)

*Пример.* Помещение имеет 10 комнат, включая коридор (обозначим буквой «К»), 17 окон (обозначим буквой «О») и 10 дверей (обозначим буквой «Д»). Построенный для данного здания граф имеет следующий вид, при этом помещением 0 считаем внешнюю среду.

Для наглядности вынесем переходы, доступ к которым невозможен из внешней среды отдельно.

Данный граф представляет собой схему переходов между помещениями предприятия. 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.

А на входной двери имеется замок и дверь бронирована.

Поэтому появляются три барьера (обозначим их буквой «Б») от Б1 до Б53. 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. Таким образом, из графа исключаются вершины Д3, Д6, Д8.

Каждой дуге ставится в соответствие ее вес – вероятность совершения данного перехода. При этом двунаправленные дуги распадаются на две. 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 0.056. Для упрощения расчетов в лабораторной работе примем вероятность совершения всех остальных переходов равными 0,1.

С учетом сказанного выше граф примет следующий вид:

0,1

0,1

0,1

0,1

0,056

0,056

0,1

0,1

0,1

0,1

0,1

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

, (1)

где  – вес *j*-й дуги;

 – 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.

56\*10-6

56\*10-7

56\*10-7

0,1

0,1

0,1

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:

, (2)

где  – вес *j*-й дуги, входящей в данную вершину;

*n* – количество дуг, входящих в вершину *i*.

В результате получим следующий граф:

1-1,56\*10-4

0,9

0,8

1,68\*10-5

0,9

0,9

0,9

0,8

0,6

1,12\*10-5

1,12\*10-5

1,68\*10-5

1,68\*10-5

56\*10-7

1,12\*10-5

56\*10-7

56\*10-7

56\*10-6

0,9

0,9

0,8

0,1

0,1

0,1

Для данного графа матрица смежности будет иметь следующий вид:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | К0 | К1 | К2 | К3 | К4 | К5 | К6 | К7 | К8 | К9 | К10 |
| Из К0 | 0,999844 | 56\*10-6 | 56\*10-7 | 1,12\*10-5 | 56\*10-7 | 1,68\*10-5 | 1,68\*10-5 | 1,68\*10-5 | 1,12\*10-5 | 56\*10-7 | 1,12\*10-5 |
| Из К1 | 0 | 0,6 | 0 | 0 | 0,1 | 0,1 | 0 | 0 | 0,1 | 0,1 | 0 |
| Из К2 | 0 | 0 | 0,8 | 0,1 | 0 | 0 | 0 | 0 | 0 | 0 | 0,1 |
| Из К3 | 0 | 0 | 0,1 | 0,9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Из К4 | 0 | 0,1 | 0 | 0 | 0,9 | 0 | 0 | 0 | 0 | 0 | 0 |
| Из К5 | 0 | 0,1 | 0 | 0 | 0 | 0,8 | 0,1 | 0 | 0 | 0 | 0 |
| Из К6 | 0 | 0 | 0 | 0 | 0 | 0,1 | 0,9 | 0 | 0 | 0 | 0 |
| Из К7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,9 | 0,1 | 0 | 0 |
| Из К8 | 0 | 0,1 | 0 | 0 | 0 | 0 | 0 | 0,1 | 0,8 | 0 | 0 |
| Из К9 | 0 | 0,1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,9 | 0 |
| Из К10 | 0 | 0 | 0,1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,9 |

**Расчет вероятности доступа в помещения**











**3. Расчет защищенности от НСД к локальной сети предприятия**

**3.1. Для поставленной задачи рассчитать защищенность от НСД ЛВС.**

*Пример.* Граф будет иметь следующий вид:

0.1

0.1

0.1

0.1

0.17

0.17

Будем считать: К0- внешняя среда, К4..К9 – комнаты, С- компьютеры, Л- локальная сеть предприятия.

0.1

0.1

Граф, преобразованный с учетом исключения вершин с одной входной и одной выходной дугой, имеет вид:

0.1

0.1

0.8

0.9

0.17\*10-5

0.8

0.8

0.8

0.8

0.17\*10-5

0,99898

0.1

0.1

1

0.1

0.1

0.2

Матрица смежности будет иметь следующий вид:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | К0 | К4 | К5 | К6 | К7 | К8 | К9 | Л |
| из К0 | 0.99898 | 0.17\*10-5 | 0.17\*10-5 | 0.17\*10-5 | 0.17\*10-5 | 0.17\*10-5 | 0.17\*10-5 | 0 |
| из К4 | 0 | 0.8 | 0 | 0 | 0 | 0 | 0 | 0.2 |
| из К5 | 0 | 0 | 0.8 | 0.1 | 0 | 0 | 0 | 0.1 |
| из К6 | 0 | 0 | 0.1 | 0.8 | 0 | 0 | 0 | 0.1 |
| из К7 | 0 | 0 | 0 | 0 | 0.8 | 0.1 | 0 | 0.1 |
| из К8 | 0 | 0 | 0 | 0 | 0.1 | 0.8 | 0 | 0.1 |
| из К9 | 0 | 0 | 0 | 0 | 0 | 0 | 0.9 | 0.1 |
| из Л | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

**Расчет вероятности НСД к локальной сети предприятия**











**3.2. По полученным графикам сделать выводы о качестве функционирования комплексной системы защиты информации на рассматриваемом предприятии.**