Практическая работа 7: Многозональность и многорубежность технической защиты

Тема: Многозональность и многорубежность инженерно-технической защиты информации.

Цель: Оптимизировать систему защиты путём разделения единой контролируемой зоны на несколько и введя понятие рубежей защиты.

Описание: Данная практика позволяет закрепить знания о контролируемых зонах и применить навыки предыдущих работ для определения зон и рубежей защиты.

Оборудование:

- Схема границ защищённого доступа объекта
- Математические пакеты анализа графов (например, Excel, Python)

Задачи:

1. Изучить план и схемы выбранного здания.
2. Определить контролируемые зоны объекта
3. Определить рубежи на границах КЗ
4. Составить семантическую цепь
5. Определить уязвимости в системе защиты

Описание работы

Многозональная защита предусматривает разделение территории на отдельные контролируемые зоны, в каждой из которых обеспечивается соответствующий уровень безопасности. Это позволяет экономить средства на защите информации, так как каждая зона имеет свой уровень безопасности, соответствующий ценности хранимой там информации. Зоны могут быть независимыми, пересекающимися и вложенными.

Уровень безопасности информации в каждой зоне зависит от нескольких факторов. Во-первых, это расстояние от источника информации до злоумышленника или его средства для получения информации. Во-вторых, это количество и уровень защиты на пути злоумышленника или распространения информации. Например, речь может идти о физических преградах. В-третьих, это эффективность средств контроля доступа людей и транспорта в зону. И, наконец, это меры по защите информации внутри зоны.

Чем дальше находится источник информации от злоумышленника и чем больше слоев защиты присутствует, тем дольше злоумышленнику потребуется, чтобы достичь источника, и тем больше энергии будет потеряно в виде поля или электрического тока. Чтобы обеспечить безопасность информации, как от внешних угроз (находящихся за пределами организации), так и внутренних угроз (от злоумышленников и сотрудников), выбирается определенное количество и расположение защитных зон и слоев. Если информация очень ценная, то рекомендуется окружить ее источник большим количеством слоев и зон, чтобы затруднить злоумышленнику получить доступ к носителям информации.

Ход работы

1. Составьте описание зон для объекта.

Многозональность защиты предусматривает разделение территории на отдельные контролируемые зоны. Вариант классификации зон приведен в таблице:

Категория зоны	**Наименование зоны**	**Функциональное назначение зоны**	**Условия доступа сотрудников**	**Условия доступа посетителей**
0	Свободная	Места свободного посещения	Свободный	Свободный
I	Наблюдаемая	Комнаты приема посетителей	Свободный	Свободный
II	Регистрационная	Кабинеты сотрудников	Свободный	По удостоверению личности с регистрацией
III	Режимная	Секретариат, компьютерные залы, архивы	По идентификационным картам	По разовым пропускам
IV	Усиленной защиты	Кассовые операционные залы, материальные склады	По спецдокументам	По спецпропускам
V	Высшей защиты	Кабинеты высших руководителей, комнаты для ведения переговоров, специальные хранилища	По спецдокументам	По спецпропускам

На основании этой таблицы разделите ваше здание на шесть зон. К примеру, для здания «школа» деление может быть таким:

Наименование зоны		**Описание**
0	Свободная	Школьный двор, холл, коридоры
I	Наблюдаемая	Административные комнаты, где проходят встречи с родителями
II	Регистрационная	Классные комнаты, кабинеты учителей
III	Режимная	Библиотека, архивы с учебными материалами
IV	Усил. защиты	Бухгалтерия, секретариат
V	Высш. защиты	Кабинет директора, комната для хранения важных документов

2. Определите один объект высшей защиты.

Среди всех объектов зоны V (если их несколько) выберите ровно один объект (комнату, помещение) для дальнейшей работы. Это может быть кабинет руководителя организации или архив документов особой важности.

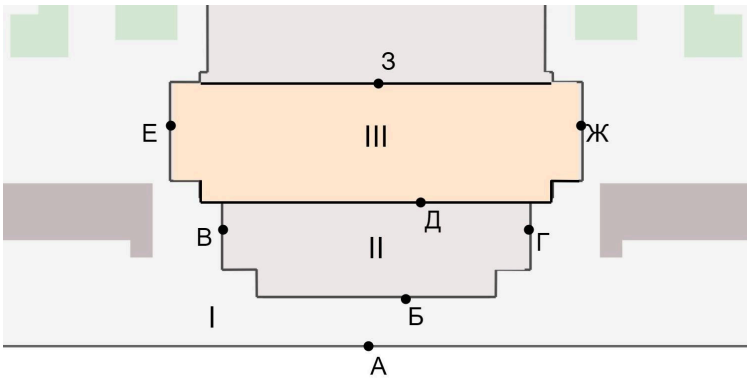
В данном помещении выберите ровно один источник информации (документы, сотрудники, продукция, материалы).

3. Укажите зоны на схеме.

На плане вашего здания выделите зоны и укажите их названия и категории (это можно сделать либо прямо на схеме, либо обозначая зоны на схеме цифрами и указывая описание в легенде под схемой).

4. Определите рубежи защиты на границах зон.

Обозначьте на схеме точками с буквенным обозначением границы контролируемых зон (как одного уровня, так и различных уровней):



Составьте список или таблицу, где укажите, чем является каждый рубеж защиты:

	Рубеж	**Ур. доступа**
А	забор	нет прохода
	калитка	свободный вход
Б	стена	нет прохода
	дверь здания	по карточкам
В	стена, окна здания	нет прохода
Г	…	…
…	…	…

5. Определите рубежи на границах особо опасных направлений.

Добавьте в таблицу из шага 4 дополнительные рубежи, которые не находятся на границах КЗ, но располагаются на возможных направлениях злоумышленника.

Например, такими рубежами могут являться: дверь сейфа (сейф не является отдельной контролируемой зоной, но рубеж в виде двери с замком является препятствием для нарушителя), дверь металлического шкафа, система защиты компьютера. Также, например, рубеж может быть создан, если кабинет руководителя, являющийся одной контролируемой зоной, разделён на две части: приёмная комната и непосредственно комната руководителя.

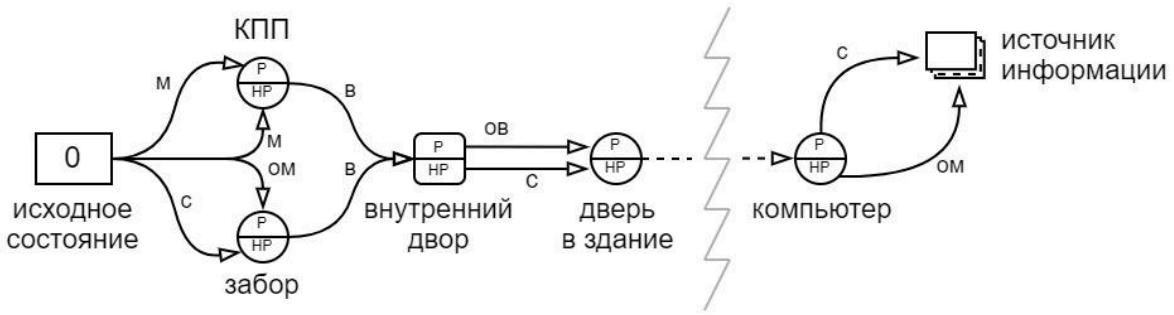
6. Постройте семантическую цепь.

Кабинет содержит информацию, которая может подвергаться угрозам и утечке. Эти потенциальные угрозы всегда существуют, однако они становятся особенно актуальными, когда злоумышленник пытается проникнуть в организацию или вербует сотрудника, возникает пожар или проявляются явные признаки технических каналов для утечки информации.

Постройте семантическую цепь представления вариантов проникновения злоумышленника в объект (помещение) высшей защиты извне контролируемой зоны с градацией вероятностей перехода.

Схема должна начинаться с исходного состояния источника угрозы. Овалами на схеме цепи отмечайте рубежи защиты, четырёхугольниками — зоны, фигуры разделены на две половинки, обозначающие время проникновения (рабочее и нерабочее время организации). Дугами-стрелками показаны участки маршрутов нарушителей, у каждой дуги указаны вероятность её реализации (ом — очень маленькая, м — маленькая, с — средняя, в — высокая, ов — очень высокая).

Пример семантической цепи приведён ниже. Советуем также пронумеровать все объекты на схеме.



Дуга, ведущая от зоны до рубежа, показывает проникновение нарушителя через рубеж. Дуга, ведущая от рубежа до зоны, показывает перемещение нарушителя по зоне до следующего рубежа.

Например, схема ниже показывает, что вероятность проникновения нарушителя из коридора через дверь очень мала (вероятно, дверь железная и на ней находится сложный замок), а вероятность свободного нахождения в служебной секции очень высока (вероятно, там нет камер видеонаблюдения и датчиков охранной сигнализации):

Поместите схему в отчёт и кратко опишите её.

7. Найдите маршрут с минимальной вероятностью обнаружения.

По графу определите, по какому маршруту должен двигаться нарушитель и в какое время он должен совершить проникновение (в рабочее или нерабочее), чтобы иметь минимальные шансы на то, чтобы быть обнаруженным.

Сначала присвойте на своё усмотрение веса вербальным значениям вероятности (к примеру, ом = 0.1, м = 0.3, с = 0.5, в = 0.7, ов = 0.9).

Путём перебора всех маршрутов (отдельно для рабочего и нерабочего времени) вычислите, какой маршрут имеет минимальную итоговую вероятность обнаружения, которая находится как произведение величин дуг, по которым проходит нарушитель. К примеру, в данном фрагменте цепи:

общая вероятность равна 0,1 × 0,7 = 0,07 = 7%

Перебор всех вариантов можно сделать при помощи программы. Ниже приведён пример кода на Python:

```
import numpy as np
import itertools

# Ваша матрица смежности
# Значение -1 означает, что между вершинами нет ребра
adj_matrix = np.array([
    [-1, -1, 0.2, 0.6], # Вершина 1
    [-1, -1, -1, -1],   # Вершина 2
    [-1, 0.8, -1, -1],  # Вершина 3
    [-1, 0.8, -1, -1]   # Вершина 4
```

```
])
for sublist in adj_matrix:
    for i in range(len(sublist)):
        if sublist[i] == -1:
            sublist[i] = float('inf')

start = int(input("Введите номер начальной вершины: ")) - 1
end = int(input("Введите номер конечной вершины: ")) - 1

paths = list()
for i in range(len(adj_matrix)):
    paths.extend(list(itertools.permutations(range(len(adj_matrix)), i + 1)))

paths = [path for path in paths if path[0] == start and path[-1] == end]

def path_product(path, matrix):
    product = 1
    for i in range(len(path) - 1):
        if matrix[path[i]][path[i+1]] == 0:
            return float('inf')
        product *= matrix[path[i]][path[i+1]]
    return product

min_product = float('inf')
min_path = None
for path in paths:
    product = path_product(path, adj_matrix)
    if product < min_product:
        min_product = product
        min_path = path

if min_path is not None:
    print("Минимальный путь: ", [vertex+1 for vertex in min_path])
    print("Произведение весов на этом пути: ", min_product)
else:
    print("Путь не найден")
```

Укажите и опишите в отчёте найденный оптимальный для злоумышленника маршрут и вероятность его осуществления (в процентах) для рабочего и нерабочего времени.

Отличаются ли оптимальные маршруты для рабочего и нерабочего времени? Почему?

8. «Поиграйте» со значениями в матрице.

В обнаруженном вами на предыдущем шаге маршруте найдите ребро с наименьшим весом (то есть самое слабое «звено» в вашей системе защиты здания). В матрице смежности измените вес этого ребра на 1, тем самым сделав его самым сильным «звеном» системы и запустите расчёт снова.

Изменился ли обнаруженный программой маршрут? Сильно ли изменилась вероятность обнаружения нарушителя? Сделайте выводы, отразите это в отчёте.

Сделайте аналогичные действия со схемой для нерабочего времени.

Найдите в матрице ребро с наибольшим весом и измените его вес на 0. Этим действием вы симулируете отказ самого сильного элемента в вашей системе защиты. Изменился ли обнаруженный маршрут и вероятность обнаружения?

Попробуйте дальше изменять значения в матрице. Например, попробуйте добиться защищённости 90% или повысить защищённость в два раза, изменяя веса ребер не более чем на 10 процентных пунктов.

9. Нарисуйте маршрут нарушителя на схеме

На схеме здания с отмеченными границами зон и рубежами защиты обозначьте пунктирной линией оптимальный маршрут нарушителя для рабочего времени, обнаруженный вами на шаге № 5.

10. Разработайте рекомендации по усилению защиты.

На основании выводов из шагов №№ 5 и 6 разработайте рекомендации по защите здания как организационного, так и технического характера. К примеру, можно посоветовать установить железную дверь вместо деревянной, организовать видеонаблюдение, обязать сотрудников блокировать компьютеры при выходе из помещения.

Учтите, что рекомендации должны учитывать специфику здания и не нарушать комфорт сотрудников и посетителей.

11. Оформите вывод по проделанной работе.

В выводе укажите, как многозональная и многорубежная защита способствует повышению защищённости объекта.

Контрольные вопросы

Основные вопросы.

1. Что такое многозональность защиты?
2. Какой уровень безопасности должен обеспечиваться в каждой контролируемой зоне?
3. Как многозональность позволяет уменьшить расходы на инженерно-техническую защиту информации?
4. Перечислите виды контролируемых зон
5. Почему вложенные контролируемые зоны наиболее распространены?
6. Что такое многорубежность инженерно-технической системы защиты?
7. Что такое рубежи защиты? Где они создаются?

Бонусные вопросы.

1. Какие принципы лежат в основе многозональности и многорубежности технической системы защиты?
2. Что представляет собой принцип равнопрочности рубежей?
3. Что представляет собой принцип непрерывности защиты?
4. Какие факторы следует учитывать при определении уровня безопасности в каждой контролируемой зоне?