

Практическая работа 1: Определение границ контролируемой зоны и демаскирующих признаков

Тема: Определение границ контролируемой зоны и выявление демаскирующих признаков для выбранного здания.

Цель: Составить описание контролируемой зоны и выявить демаскирующие признаки для выбранного здания.

Описание: В рамках этой практики студенты будут изучать выбранное здание и проводить анализ его структуры и особенностей для определения контролируемой зоны и выявления демаскирующих признаков.

Оборудование:

- План и схемы выбранного здания
- Фотоматериал (фотографии здания)
- Онлайн-карты (Яндекс.Карты, Google Maps)
- Графический редактор

Задачи:

1. Изучить план и схемы выбранного здания.
2. Определить границы контролируемой зоны внутри здания.
3. Идентифицировать потенциальные демаскирующие признаки.
4. Предложить рекомендации по маскировке признаков
5. Документировать результаты анализа.

Описание работы

В рамках данной практической работы мы будем изучать понятие контролируемой зоны и демаскирующих признаков в контексте технической защиты информации.

Контролируемая зона представляет собой определенную территорию, на которых исключается неконтролируемое пребывание лиц или транспортных средств без постоянного или разового допуска.

Демаскирующие признаки, в свою очередь, представляют собой внешние признаки, физические поля и элементы деятельности, которые позволяют отличить один объект от другого.

Определение контролируемой зоны и демаскирующих признаков имеет важное значение для обеспечения безопасности и защиты информации. Четкое понимание того, где возможны уязвимости и какие меры защиты могут быть применены, позволяет предотвратить несанкционированный доступ, подслушивание информации, физическое проникновение и другие угрозы, связанные со сферой технической защиты информации.

Ход работы

1. Составьте описание выбранного здания.

Найдите в приложении онлайн-карт (Яндекс.Карты, Google Maps) ваше здание, используя координаты из практики № 0. Ознакомьтесь со схемой здания, спутниковыми фотографиями и панорамами улиц. Кратко опишите ваше здание. Укажите его назначение, размеры, количество этажей и особенности конструкции.

2. Определите границы контролируемой зоны.

Для каждой из четырёх сторон защищённой зоны определите и опишите границу контролируемой зоны. Чтобы составить хорошее описание, ответьте на следующие вопросы:

- Чем представлена граница контролируемой зоны? (*забором, ограждением, стеной здания, и т.д.*)
- Имеет ли граница входы (*калитки, ворота, двери, КПП*)?
- Как нарушитель может преодолеть границу? Может ли он перелезть через забор, перепрыгнуть турникет, разбить окно, пройти незамеченным через КПП?
- Каков пропускной режим входной группы? (*пропуска, карты доступа, охрана*)
- Есть ли видеонаблюдение за границей КЗ?

Используйте схему и фотографии для составления описания границы контролируемой зоны.

Описание одной из сторон может выглядеть следующим образом:

Западная сторона границы защищённой зоны представлена металлическим забором, имеющим два свободных входа, которые открыты днём. В ночное время пересечь забор можно либо сверху (перелезть), либо протиснувшись между прутьями, что довольно затруднительно. Здание с западной стороны имеет несколько входов, а также окна. Проход через двери возможен только при предъявлении пропуска. Окна сплошные и не открываются, поэтому пройти через них можно только разбив их, что привлечёт внимание охраны. Въезд на автомобиле возможен только через юго-западный КПП, ограниченный шлагбаумом.

Также поместите в отчёт схему здания, выделив на ней границу контролируемой зоны — данная схема называется схемой границ защищённого доступа объекта.

3. Подготовьте таблицу для демаскирующих признаков здания.

Создайте в отчёте таблицу, которую будете заполнять в дальнейшем. Шаблон таблицы приведён ниже.

№	Наименование демаскирующего признака	Классификация				Рекомендации по маскировке
		По состоянию	По характеристике	По информативности	По времени проявления	
1.
2.

4. Перечислите демаскирующие признаки.

Посмотрите фотографии здания и перечислите его демаскирующие признаки, запишите их во второй столбец таблицы (Наименование демаскирующего признака).

Признак объекта является демаскирующим, если он позволяет вскрыть принадлежность, состав, деятельность и расположение объектов и их составных частей, выявить назначение, цели и задачи их деятельности.

Например:

- *Люди в униформе* → скорее всего, это предприятие → признак помог выявить назначение объекта → он является демаскирующим.
- *Парковка для автомобилей* → скорее всего, это здание активно используется → признак помогает определить активность объекта → он является демаскирующим.
- *Отблески стекол* → скорее всего, это здание имеет окна или стеклянные элементы → признак помогает определить структуру объекта → он является демаскирующим.

Постарайтесь найти не менее 15 демаскирующих признаков. Вставьте в отчёт фотографии здания, на которых цифрами указаны демаскирующие признаки (цифры должны соответствовать номерам демаскирующих признаков в таблице).

Не забывайте, что вы можете воспользоваться фотографиями и панорамами улиц на картографических сервисах (Яндекс.Карты, Google Maps) для поиска демаскирующих признаков вашего здания.

Вы можете дополнить список признаками, которые нельзя выявить по фотографиям, но которые характерны для вашего вида здания. Например, к ним могут относиться: сеть Wi-Fi университета, характерный запах от заводов, громкие звуки фабрик.

5. Определите вид признака по состоянию.

Для каждого из обнаруженных вами демаскирующих признаков проведите его классификацию по состоянию объекта:

- **Опознавательные признаки** описывают статическое состояние объекта защиты. Эти признаки позволяют идентифицировать объект или указывают на его существование. Примеры опознавательных признаков включают форму здания, размеры, цвет и блеск поверхностей, надписи, эмблемы, символы, логотипы и цветовые коды, тени.
- **Признаки деятельности** характеризуют «следы» функционирования объекта защиты, включая обеспечение процессов его функционирования. Эти признаки указывают на активность объекта и могут включать звуковые и световые сигналы, движущиеся элементы, движение транспортных машин, звуки, огни, вспышки, дым, пыль, вытопанные дорожки, оставленный мусор.

Результаты запишите в третий столбец таблицы (По состоянию).

6. Определите вид признака по характеристике.

Для каждого из обнаруженных вами демаскирующих признаков проведите его классификацию по характеристике объекта:

- **Видовые признаки** относятся к внешнему виду объекта защиты. Они описывают форму, размеры, цвет и другие детали объекта. Видовые признаки могут быть визуально видимыми и помогают идентифицировать или различать объекты по их характеристикам. Например, видеокамеры, парковка, архитектурные особенности здания — все это является примерами видовых признаков.
- **Сигнальные признаки** описываются параметрами физических полей и электрических сигналов, создаваемых объектом защиты. Эти признаки связаны с передачей или приемом сигналов, которые могут привлечь внимание или указывать на активность объекта. Как правило, такие признаки обнаруживаются специальными приборами (радиоволны, тепловые излучения, электромагнитные излучения, звуки).
- **Вещественные признаки** определяют материальный состав, структуру и свойства веществ материального объекта. Эти признаки связаны с физическими или химическими свойствами объекта, которые могут быть обнаружены или идентифицированы. Примеры — радиоактивные вещества или дурно пахнущие испарения от заводов и фабрик.

Результаты запишите в четвертый столбец таблицы (По характеристике).

7. Определите вид признака по информативности.

Для каждого из обнаруженных вами демаскирующих признаков проведите его классификацию по их информативности:

- **Именные признаки** принадлежат только одному конкретному объекту защиты. Такими признаками являются: информационный указатель (название на здании), особый оригинальный узнаваемый элемент дизайна, название Wi-Fi сети.
- **Прямые признаки** принадлежат рассматриваемому объекту, но не являются именными (то есть таким признаком могут обладать и другие здания). Например, установленная на фасаде видеочкамера является демаскирующим признаком этого здания, при этом камеры также установлены и на других зданиях.
- **Косвенные признаки** непосредственно не принадлежат объекту защиты, но могут отражать различные этапы функционирования объекта защиты, являться результатом взаимодействия рассматриваемого объекта с окружающей средой. Например, следы ног или рук человека, автомобиля и других движущихся объектов.

Результаты запишите в пятый столбец таблицы (По информативности).

8. Определите вид признака по времени проявления.

Для каждого из обнаруженных вами демаскирующих признаков проведите его классификацию по времени их проявления:

- **Постоянные признаки** не изменяются в течение жизненного цикла объекта или их изменение происходит в течение длительного времени: форма, структурные особенности, цвет.
- **Периодические признаки** повторяются в течение определенного времени: следы сотрудников, следы автомобиля, накопление мусора.
- **Эпизодические признаки** появляются иногда, при определенных условиях, без определенного периода, например, случайно появившееся на поверхности объекта пятно краски, взрыв.

Результаты запишите в шестой столбец таблицы (По времени проявления).

9. Подготовьте рекомендации по маскировке.

Для каждого из обнаруженных вами демаскирующих признаков подготовьте рекомендации по их маскировке. Маскировка позволяет сделать эти признаки менее заметными или скрыть их совсем, чтобы уменьшить вероятность их обнаружения злоумышленниками.

Примеры рекомендаций по маскировке:

1. Для видового признака, такого как видеокамера, можно рекомендовать его установку в местах, где она будет меньше выделяться на фоне окружающей среды. Например, можно выбрать цвет камеры, который соответствует окружающей стене или окрасить камеру в цвет, который сливается с окружением. Кроме того, можно установить декоративные элементы или растительность, которая будет закрывать особенности поверхности и делать их менее заметными.
2. Для сигнального признака, например, звуковой сирены, можно рекомендовать установку дополнительных звуковых источников в других местах здания, чтобы сирена не привлекала всеобщее внимание. Также можно предложить использование звуковых сигналов, которые не будут вызывать панику или будут менее заметны в окружающей среде.

Результаты запишите в седьмой столбец таблицы (Рекомендации по маскировке).

Если вы считаете, что для некоторых демаскирующих признаков маскировка не нужна, оставьте ячейку таблицы пустой или поставьте прочерк (—).

10. Оформите вывод по проделанной работе.

В выводе укажите, какие рекомендации по защите объекта вы могли бы предложить по результатам анализа границ контролируемой зоны и демаскирующих признаков. Соответствует ли пропускной режим степени секретности объекта? Сильно ли выделяется объект (здание) среди других?

Контрольные вопросы

Основные вопросы.

1. Что такое контролируемая зона?
2. Перечислите, чем могут являться границы контролируемой зоны.
3. Что такое демаскирующий признак?
4. В чём разница между опознавательными признаками и признаками деятельности?
5. Как классифицируются демаскирующие признаки по времени проявления?
6. В чём разница между именными, прямыми и косвенными демаскирующими признаками?
7. Перечислите основные видовые демаскирующие признаки.
8. В чём разница между периодическими и эпизодическими демаскирующими признаками?
9. Перечислите примеры демаскирующих признаков.

Бонусные вопросы.

1. Что такое информативность демаскирующего признака? Как её можно вычислить?
2. Чему должен соответствовать уровень безопасности контролируемой зоны?
3. В чём преимущества и недостатки разбиения пространства на несколько контролируемых зон?
4. Перечислите основные методы обнаружения демаскирующих признаков.
5. Какие стратегии можно использовать для сокрытия демаскирующих признаков?
6. Какие меры могут быть предприняты для предотвращения утечки информации из контролируемой зоны?
7. Какие средства технической защиты могут быть использованы для обеспечения безопасности контролируемой зоны?
8. Есть ли разница между контролируемой зоной и охраняемой территорией предприятия? Может ли одно быть больше другого?
9. В чём разница между обнаружением и распознаванием демаскирующего признака?
10. Каким образом демаскирующий признак может выступать в качестве канала утечки информации?