Государственное образовательное учреждение

«Белорусский государственный технологический университет»

Отчет

*по лабораторной работе №2*

ТЕМА ЗАНЯТИЯ: РЕШЕНИЕ ЗАДАЧИ РАЗРАБОТКИ СРЕДСТВ ЗАЩИТЫ ДЛЯ ОБЕСПЕЧЕНИЯ МАКСИМАЛЬНОЙ ЭФФЕКТИВНОСТИ ОБЪЕКТА В УСЛОВИЯХ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

|  |  |
| --- | --- |
|  | **Исполнитель:**  Студента (-ка) группы 2  Специальность\_\_\_\_ИСиТ\_\_\_  Гулевич Никита Максимович  (Ф.И.О.) |
|  | **Преподаватель**:  Ржеутская Н. В. |

Минск, 2025

**Цель**: научиться решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

Ответы на контрольные вопросы:

1. Что такое технический канал утечки информации?

Технический канал утечки информации – это физический путь сигнала от источника передачи данных к приемному устройству мошенника.

1. Чем отличаются пассивные и активные методы защиты информации от утечки по техническим каналам?

К пассивным техническим средствам защиты относятся экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры и т. д. Цель пассивного способа – максимально ослабить сигнал от источника информативного сигнала, например, за счет отделки стен звукопоглощающими материалами или экранирования технических средств.

Активное техническое средство защиты – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации. Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств.

1. Приведите примеры пассивных методов защиты информации.

* Экранирование.
* Установка сетевых помехоподавляющих фильтров.
* Использование фильтра-генератора для **защиты** цепей питания и заземления.
* Применение устройств зашумливания.

1. Перечислите примеры активных методов защиты информации.

* пространственного электромагнитное зашумление ЗУ и ПЭМИН ТСПИ;
* акустическое и вибрационное зашумление строительных конструкций;
* СВЧ - воздействие на микрофонные цепи (подавления диктофонов устройствами направленного высокочастотного радиоизлучения);
* зашумление каналов передачи данных;
* зашумления силовой сети и цепей заземления;
* разрушающее воздействие на средства съема сигналами большой мощности (тепловое разрушение электронных устройств)
* установка систем гарантированного уничтожения информации;
* шифрование информации, передаваемой по каналам связи.

1. По характеру проводимых действий как разделяются все методы защиты информации?

Все методы защиты информации по характеру проводимых действий можно разделить на следующие:

* законодательные (правовые);
* организационные;
* технические;
* комплексные.

**ВАРИАНТ 7**

**Относительная эффективность при наличии средств защиты:**

**Относительная эффективность при несанкционированном доступе:**

Эффективность функционирования при наличии средств защиты:

Эффективность функционирования без учета воздействия несанкционированного доступа:

Эффективность функционирования с учетом воздействия несанкционированного доступа:

Эффективность функционирования при наличии средств защиты:

Относительная эффективность при несанкционированном доступе:

Относительная эффективность при наличии средств защиты:

Так как относительная эффективность при наличии средств защиты больше чем относительная эффективность при несанкционированном доступе, система защиты является эффективной.

**Список использованных источников**

1. Концепция национальной безопасности РБ, Указ №575
2. [Национальный исследовательский университет «МЭИ»](https://studfile.net/mei/) [Методы и Средства Защиты Информации](https://studfile.net/mei/miszi/folder:44331/#5868802): Подготовительный практикум.

https://studfile.net/preview/5868802/

1. Ржеутская Н. В., Нистюк О. А., Уласевич Н. И. Основы защиты информации: лабораторный практикум. Минск: Учреждение образования «Белорусский государственный технологический университет», 2024.