ВОЕННАЯ КАФЕДРА
при НАО «КазНИТУ имени К.И. САТПАЕВА»

ЦИКЛ
ИНФОРМАЦИОННОЙ ЗАЩИТЫ

Дисциплина

«Аппаратные и программные средства защиты информации в АСУВ»

Тема №8

«Техническая разведка и системы безопасности»

Занятие №1

«Техническая разведка и противодействие технической разведке»

Учебные вопросы:

1. **Цели и задачи технической разведки.**
2. **Угрозы безопасности информации.**
3. **Виды угроз безопасности информации.**

Цели занятия:

- ✔ **изучить цели и задачи технической разведки;**
- ✔ **обучить выявлять угрозы безопасности информации.**

Учебный вопрос №1.
Цели и задачи технической разведки.

Разведка **- сбор информации о противнике или конкуренте для обеспечения своей безопасности и получения преимуществ в области вооружённых сил, военных действий, политики или экономики.**

Техническая разведка (ТР) **- получение сведений путем сбора и анализа информации техническими средствами.**

Вопрос №1. Цели и задачи технической разведки

Основной целью ТР **является обеспечение высшего политического руководства своего государства своевременной информацией по разведываемой стране, по ее Вооруженным Силам (ВС), по военно-экономическому потенциалу.**

Вопрос №1. Цели и задачи технической разведки

Задачей ТР является сбор информации по состоянию и перспективам развития военно-экономического потенциала страны, по составу, численности, дислокации и технической оснащенности войск и сил флота, по состоянию боевой готовности ВС, по размещению на территории страны объектов оборонной промышленности, выпускаемой ими продукции, производственной мощности, по наиболее важным разработкам в области вооружения и военной техники, по эффективности существующего и разрабатываемого вооружения, по проводимым учениям войск и сил флота, по степени подготовки территории страны к ведению боевых действий, по наличию топливно-энергетических, рудных, водных и др. ресурсов страны.

Вопрос №1. Общие сведения.

В основу организации ТР положены следующие принципы:

- **целенаправленность;**
- **централизация руководства;**
- **размещение технических средств на границе вдоль территории страны;**
- **использование для сбора информации неразведывательных систем и средств;**
- **формирование целевых систем разведки;**
- **коллективное использование добытой информации;**
- **привлечение ученых и специалистов для обработки развед. информации.**

Учебный вопрос №2.
Угрозы безопасности информации

Угроза информационной безопасности - **совокупность условий и факторов, создающих опасность нарушения информационной безопасности.**

Вопрос №2. Угрозы безопасности информации

Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

Под угрозой интересам субъектов информационных отношений понимают потенциально возможное событие, процесс или явление которое посредством воздействия на информацию или другие компоненты информационной системы может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

Вопрос №2. Угрозы безопасности информации

Основные принципы информационной безопасности

1. *Целостность данных* - такое свойство, в соответствии с которым информация сохраняет свое содержание и структуру в процессе ее передачи и хранения. Создавать, уничтожать или изменять данные может только пользователь, имеющий право доступа.

Вопрос №2. Угрозы безопасности информации

Основные принципы информационной безопасности

2. *Конфиденциальность* - свойство, которое указывает на необходимость ограничения доступа к конкретной информации для обозначенного круга лиц. Таким образом, конфиденциальность дает гарантию того, что в процессе передачи данных, они могут быть известны только авторизованным пользователям.

Вопрос №2. Угрозы безопасности информации

Основные принципы информационной безопасности

3. *Доступность информации* - это свойство характеризует способность обеспечивать своевременный и беспрепятственный доступ полноправных пользователей к требуемой информации.

4. *Достоверность* – данный принцип выражается в строгой принадлежности информации субъекту, который является ее источником или от которого она принята.

Учебный вопрос №3.
Виды угроз безопасности информации

Под *<u>угрозой информационной безопасности</u>* принято понимать потенциально возможные действия, явления или процессы, способные оказать нежелательное воздействие на систему или на хранящуюся в ней информацию.

Вопрос №3. Виды угроз безопасности информации

По природе возникновения различают *естественные* и *искусственные угрозы*. К первой группе относятся те, что вызваны воздействием на компьютерную систему объективных физических процессов или стихийных природных явлений. Вторая группа – те угрозы, которые обусловлены деятельностью человека.

Вопрос №3. Виды угроз безопасности информации

Также есть разделение *в зависимости от их непосредственного источника*, в качестве которого может выступать природная среда (например, стихийные бедствия), человек (разглашение конфиденциальных данных), программно-аппаратные средства: санкционированные (ошибка в работе операционной системы) и несанкционированные (заражение системы вирусами).

Вопрос №3. Виды угроз безопасности информации

Источник угроз может иметь разное положение. В зависимости от этого фактора также выделяют три группы:

- угрозы, источник которых находятся вне контролируемой группы компьютерной системы (пример – перехват данных, передаваемых по каналам связи);

- угрозы, источник которых – в пределах контролируемой зоны системы (это может быть хищение носителей информации);

- угрозы, находящиеся непосредственно в самой системе (например, некорректное использование ресурсов).