КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМ. АЛЬ-ФАРАБИ

Факультет информационных технологий
и искусственного интеллекта

Кафедра Искусственного интелекта и Big Data

КОМПЬЮТЕРНЫЕ СЕТИ

Автор:

Джомартова Ш.А. профессор-исследователь, д.т.н., доцент

ЛЕКЦИЯ 15

СЕТЬ КАК СРЕДСТВО ЗАЩИТЫ

И РЕАГИРОВАНИЯ НА УГРОЗЫ

ЦЕЛЬ ЛЕКЦИИ

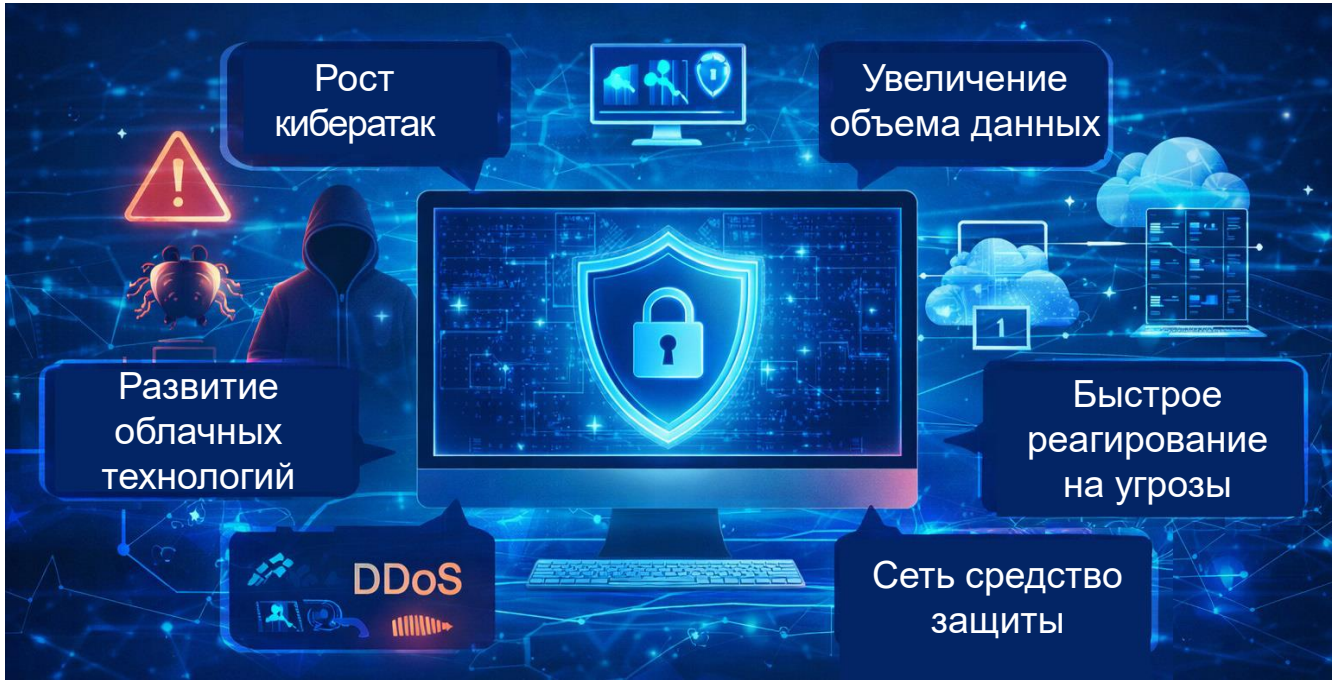
Сформировать у слушателей целостное представление о компьютерной сети как активном инструменте обеспечения информационной безопасности, раскрыть основные принципы сетевой защиты и механизмы реагирования на угрозы.

ПЛАН ЛЕКЦИИ

1. Проблемы защиты сетей.
2. Основные виды угроз.
3. Сетевые системы защиты.
4. Мониторинг и реагирование на угрозы.

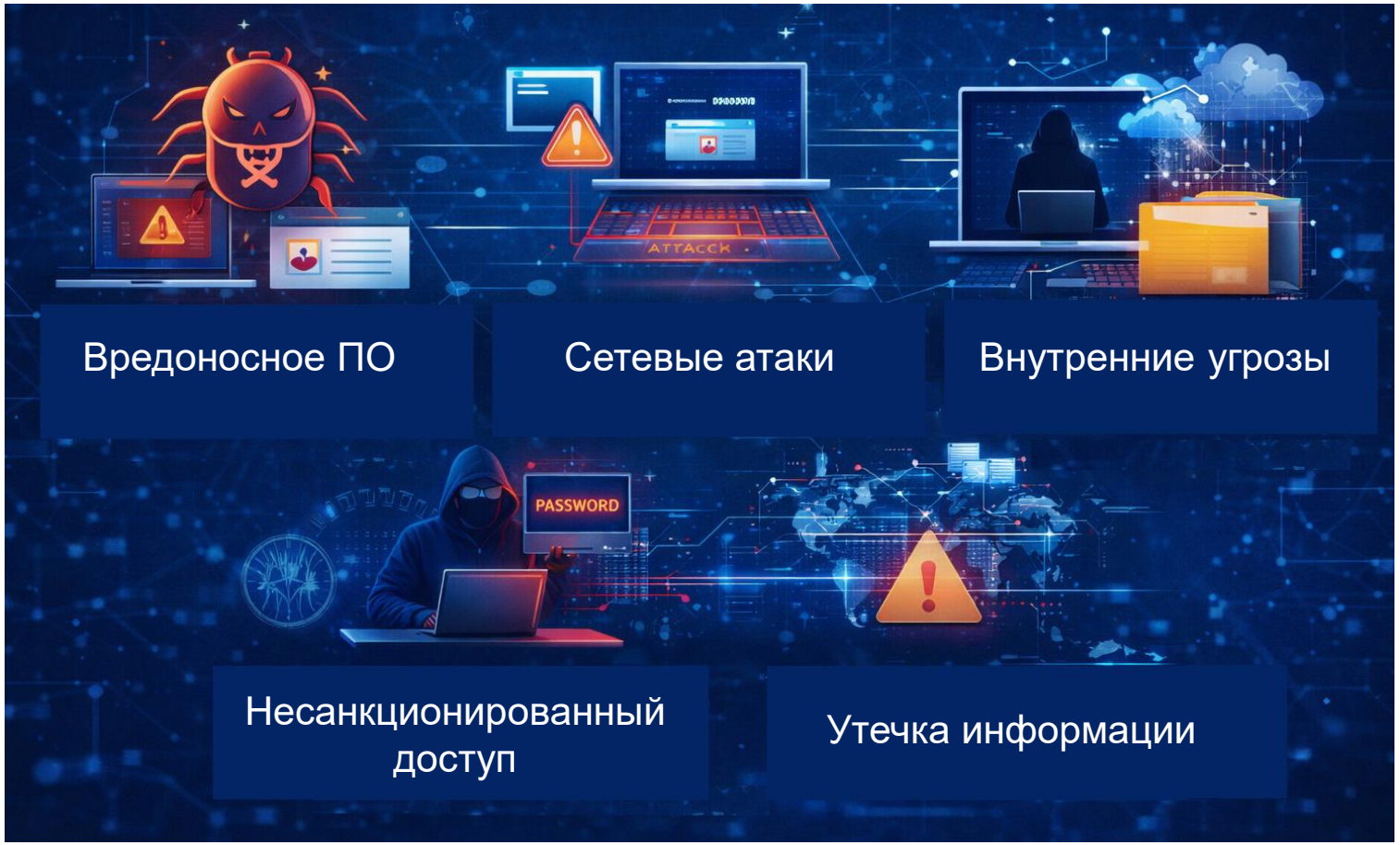
ПРОБЛЕМЫ ЗАЩИТЫ СЕТЕЙ

- Рост числа кибератак и сетевых инцидентов.
- Увеличение объёма передаваемых данных.
- Развитие облачных технологий и IoT.
- Необходимость быстрого реагирования на угрозы.
- Сеть становится не только средой передачи, но и средством защиты.



Изображение сгенерировано ИИ. ChatGPT

ОСНОВНЫЕ ВИДЫ УГРОЗЫ



- Вредоносное ПО (вирусы, трояны, ransomware).
- Сетевые атаки (DoS/DDoS, MITM, spoofing).
- Несанкционированный доступ.
- Утечка информации.
- Внутренние угрозы (ошибки пользователей).

Изображение сгенерировано ИИ. ChatGPT

МЕЖСЕТЕВЫЕ ЭКРАНЫ (FIREWALL)

- Фильтрация входящего и исходящего трафика.
- Блокировка несанкционированных соединений.
- Защита внутренней сети.
- Реализация правил безопасности.



Изображение сгенерировано ИИ. ChatGPT

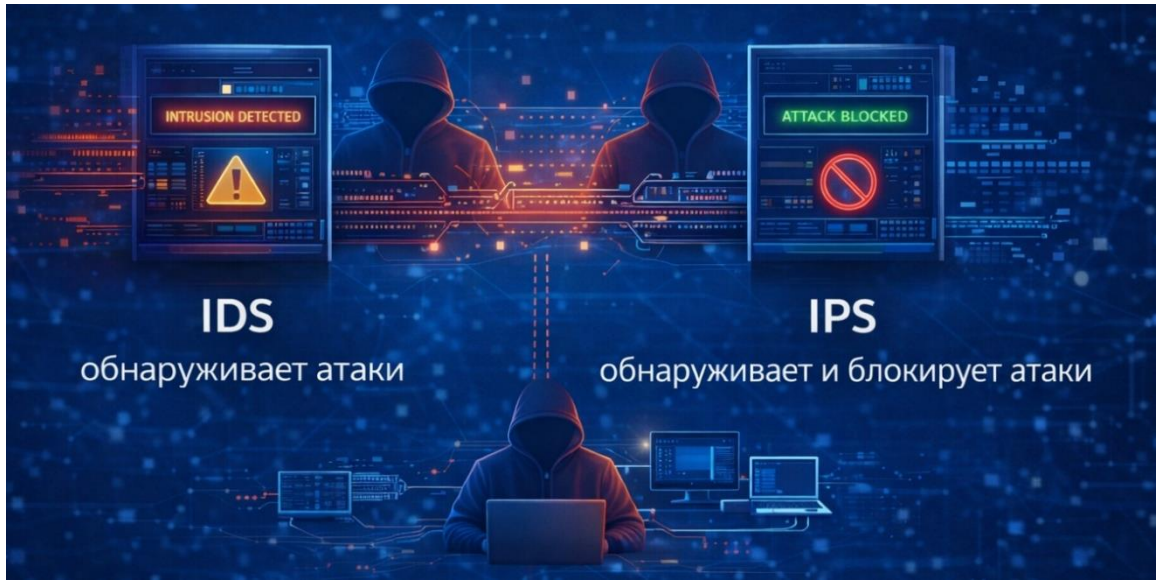
IDS И IPS СИСТЕМЫ

IDS (Intrusion Detection System) – обнаруживает атаки.

IPS (Intrusion Prevention System) – обнаруживает и блокирует атаки.

Роль IDS/IPS в современной архитектуре безопасности

- Анализ сетевого трафика.
- Выявления подозрительной активности.
- Регистрации инцидентов.



Изображение сгенерировано ИИ. ChatGPT

VPN КАК СРЕДСТВО ЗАЩИТЫ

VPN – это «защищённый тоннель»

в небезопасном цифровом пространстве.

- Шифрование передаваемых данных.
- Безопасный удалённый доступ.
- Защиту от перехвата трафика.
- Аутентификацию пользователей.



Изображение сгенерировано ИИ. ChatGPT

МОНИТОРИНГ И РЕАГИРОВАНИЕ НА УГРОЗЫ

Основные задачи мониторинга

- Выявлять атаки в реальном времени.
- Локализовать источник угрозы.
- Изолировать заражённые узлы.
- Передавать данные в центр реагирования (SOC).



Изображение сгенерировано ИИ. ChatGPT



Изображение сгенерировано ИИ. ChatGPT

ЗАКЛЮЧЕНИЕ

1. Защита компьютерных сетей является одной из ключевых задач в условиях роста объёмов информации и числа кибератак.
2. Основные угрозы включают вредоносное программное обеспечение, сетевые атаки, несанкционированный доступ и утечки данных.
3. Для противодействия этим угрозам применяются сетевые системы защиты, такие как межсетевые экраны, IDS/IPS и VPN.
4. Важную роль играет постоянный мониторинг сетевой активности и своевременное реагирование на инциденты.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Основная литература

1. Танненбаум Э., Уэзеролл Д. Компьютерные сети. Питер,2023 – 90, 121-137 с
2. Олифер В., Олифер Н.: Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание: Питер, 2021 – 184-271 с.
3. Сергеев А.Н. Основы локальных компьютерных сетей – СПб: Лань, 2016 – 142-175 с.

Дополнительная литература

1. Одом У. Официальное руководство CISCO по подготовке к сертификационным экзаменам CCNA ICDN2 200-101:маршрутизация и коммутация. - М.: ООО «И.Д. Уильямс», 2020. – 736 с.
2. Костров Б.В, Ручкин В.Н. Сети и системы передачи информации: Академия, 2021. – 288 с.

Интернет-ресурсы

https://www.trendmicro.com/ru_ru/what-is/network-security/network-security-measures.html

https://practicum.yandex.ru/blog/obespechenie-setevoj-bezopasnosti/

https://cloudnetworks.ru/setevaya-bezopasnost/

https://www.trendmicro.com/ru_ru/what-is/network-security.html