**Слайд №1 речь (Титульный слайд):**

Добрый день, уважаемые члены комиссии! Мы, Шаров и Куанышулы, представляем дипломную работу: "Интеграция криптографических методов аутентификации и систем анализа событий безопасности для защиты корпоративных данных." Руководитель — [имя руководителя]. Мы исследовали защиту данных в корпоративных сетях и сейчас изложим основные результаты.

**Слайд №2 речь (Цели, объект, практическая ценность, актуальность):**

Здесь представлены ключевые аспекты исследования. Цель работы — сравнить методы аутентификации PSK и PKI в IPsec, настроить сеть DMVPN, протестировать уязвимости и внедрить мониторинг SIEM. Объект исследования — виртуальный сетевой стенд в PNETLab с маршрутизаторами, центром сертификации и системой Graylog. Практическая ценность заключается в анализе уязвимостей методов PSK и PKI. Тема актуальна, так как технологии VPN и SIEM являются базовыми для обеспечения информационной безопасности.

**Слайд №3 речь (Топология сети):**

На этом слайде показана топология сети, созданная в PNETLab. Она включает маршрутизаторы для VPN-соединений между главным офисом и филиалами, а также клиентский маршрутизатор. В главном офисе размещены сервер центра сертификации для PKI и сервер Graylog. Узел Kali Linux использовался для тестирования уязвимостей. Эта схема обеспечила проведение практических экспериментов.

**Слайд №4 речь (Теоретическая основа):**

Этот слайд посвящён теоретической основе. DMVPN — технология Cisco для автоматического создания VPN-туннелей между главным офисом (hub) и филиалами (spoke) через протокол NHRP, позволяющий филиалам связываться напрямую. IPsec защищает туннели: ESP шифрует данные, AH проверяет подлинность, IKE управляет ключами. Мы сравнили два метода аутентификации: PSK использует общий ключ с алгоритмами HMAC-SHA или AES, PKI — цифровые сертификаты и пару ключей с алгоритмами RSA, ECDSA, Diffie-Hellman, управляемыми центром сертификации.

**Слайд №5 речь (Таблица):**

На этом слайде представлена таблица с итогами сравнения PSK и PKI. PSK проще в настройке и подходит для небольших сетей, но общий ключ имеет ограничения. PKI сложнее, но лучше масштабируется благодаря управлению через центр сертификации. Для крупных сетей предпочтительнее PKI с SIEM-системой, например, Graylog. Далее Асылхат расскажет о развертывании Graylog.

На следующем слайде мы хотели бы показать, как мы смоделировали атаку для проверки уязвимостей PSK и как SIEM-система, такая как Graylog, позволяет легко выявлять подобные события

В завершение хотелось бы сказать: в дипломной работе мы изучили защиту данных с помощью PSK и PKI в IPsec и SIEM-системы Graylog. PKI оказался надёжнее, но сложнее, а PSK проще, но уязвим. Graylog эффективно выявлял угрозы при атаках. Сочетание этих технологий усиливает защиту IT-инфраструктуры.