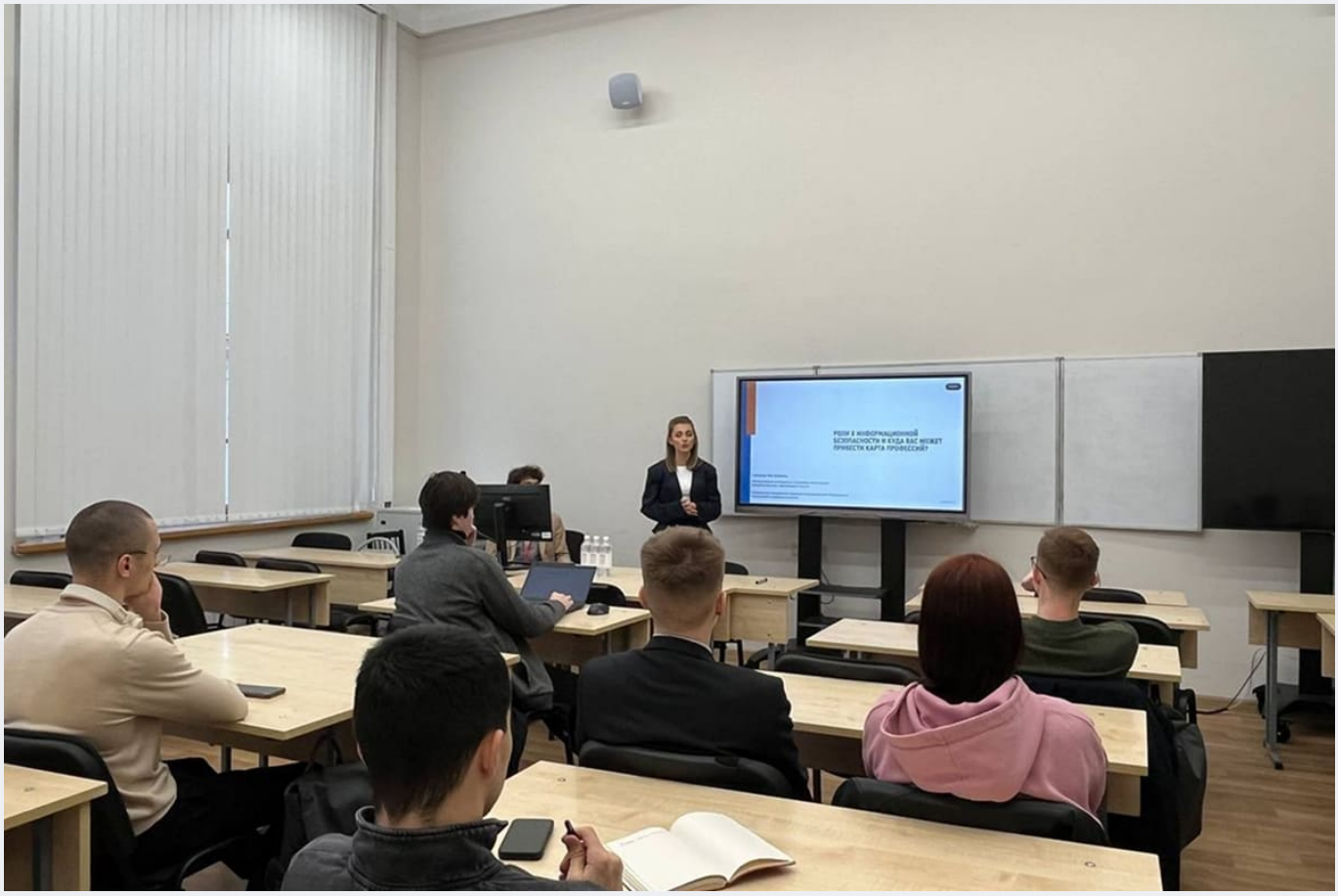
# Взгляд изнутри: как работают специалисты по кибербезопасности в нефтегазе

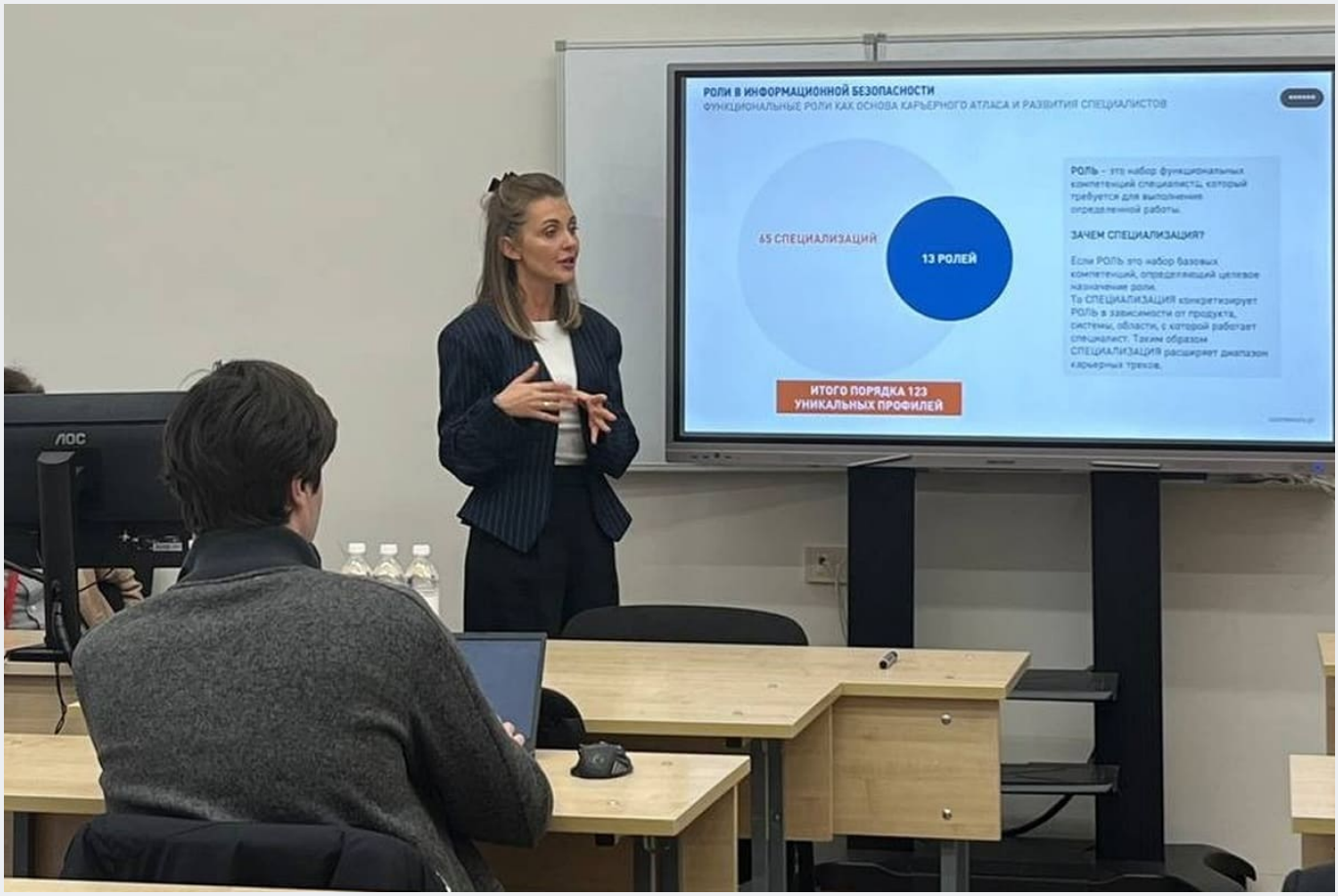


Студенты Санкт-Петербургского политехнического университета Петра Великого погрузились в мир кибербезопасности вместе с экспертами компании «Газпром нефть». Лекция объединила будущих специалистов по информационной безопасности, ИТ-архитектуре и системной инженерии, а также всех, кто интересуется защитой цифровых систем.

Современные вызовы и роли в кибербезопасности

Эксперты обсудили актуальные угрозы в цифровой среде, включая фишинг, вредоносное ПО, атаки на корпоративные сети и критически важные системы. Рассмотрели стратегические задачи кибербезопасности в нефтегазовой отрасли, где безопасность данных и стабильность работы инфраструктуры напрямую влияют на эффективность бизнеса.

Рассмотрели ключевые роли специалистов: аналитики угроз, инженеры AppSec, специалисты SOC (Security Operations Center), архитекторы безопасных систем и консультанты по управлению рисками. Обсудили навыки, необходимые для работы в каждой из ролей, и перспективы карьерного роста.




«Кибербезопасность сегодня — это не только защита данных, но и стратегическое направление развития компаний. Важно понимать, какие роли существуют в этой сфере и какие пути профессионального роста открываются для специалистов», — Яна Галимова, руководитель направления Дирекции информационной безопасности «Газпромнефть-ЦР», корпоративный руководитель программы «Кибербезопасность нефтегазовой отрасли».

Практические аспекты и реальные кейсы

Лекция включала живые кейсы и демонстрации. Иван Стародубцев показал примеры уязвимостей в приложениях и объяснил, как их предотвращать на этапе разработки. Студенты увидели, как анализ кода и тестирование безопасности помогают минимизировать риски атак.


«AppSec — это область, где теория сразу проверяется практикой. Каждое приложение может стать точкой входа для злоумышленников, поэтому важно проектировать безопасность с самого начала. Мы хотим, чтобы молодые специалисты понимали: защита начинается на этапе разработки», —Иван Стародубцев, эксперт «Газпромнефть-ЦР».

Мария Кирюшкина подробно рассказала о направлении Cyber Threat Intelligence, объяснив, что это не просто анализ угроз, а целый процесс: сбор данных, выявление источников атак, оценка рисков и выработка конкретных мер защиты. Студенты увидели, как аналитика киберугроз превращается в практические инструменты для защиты бизнеса. В конце выступления она дала рекомендации по фильмам и документальным материалам, которые помогают лучше понять тему и современные киберугрозы.

«Мы стараемся показать студентам, как теоретические знания превращаются в реальные инструменты защиты бизнеса. Умение анализировать угрозы и понимать их источники — ключевой навык современного специалиста по ИБ», —Мария Кирюшкина, эксперт «Газпромнефть-ЦР».

Также обсуждались автоматизация процессов ИБ, использование машинного обучения для обнаружения аномалий в сетях и предотвращения атак, а также внедрение комплексных политик безопасности в корпоративных системах.

Интерактив и возможности для студентов

Лекция включала вопросы и разбор конкретных ситуаций из реальной работы компании. Студенты интересовались карьерными перспективами, образовательными траекториями, необходимыми сертификатами и навыками для работы в крупных нефтегазовых компаниях. За активное участие в интерактивах студенты были отмечены баллами для поступления на магистерскую программу: «Кибербезопасность нефтегазовой отрасли».

Выводы и вдохновение для будущих специалистов

Студенты увидели, что кибербезопасность — это не просто защита систем, а возможность влиять на судьбу компаний и отрасли. Практические кейсы показали, что знания и навыки можно сразу применять, а профессия ИБ открывает широкие горизонты для профессионального роста.