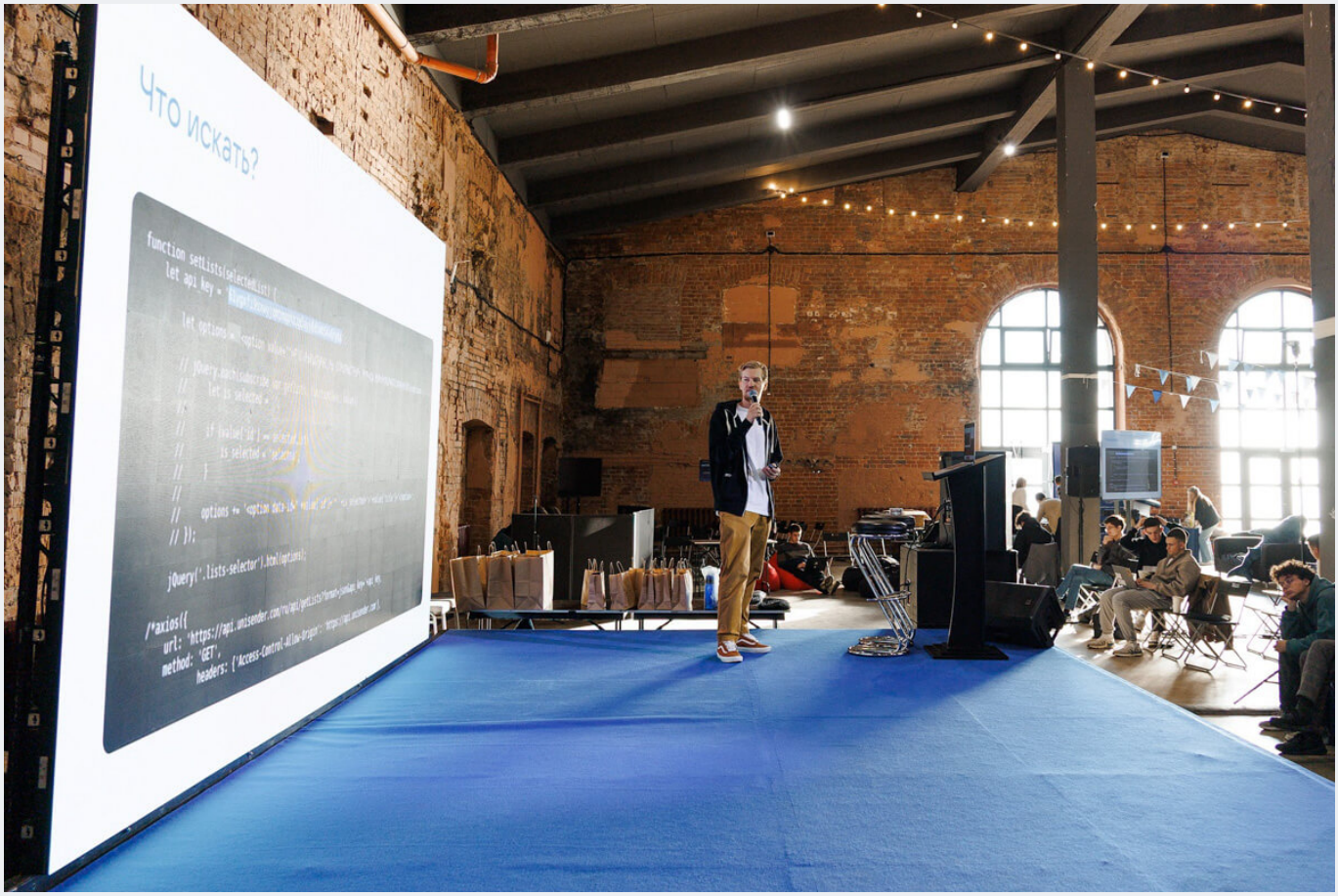
NeoQUEST от Политеха: петербургский фестиваль кибербезопасности

В Брусницын Холле состоялось мероприятие по кибербезопасности NeoQUEST-2025. Ежегодно его организует Институт компьютерных наук и кибербезопасности СПбПУ при поддержке компаний-партнёров. В этом году событие прошло с особым размахом.

NeoQUEST традиционно прошёл в три этапа — онлайн CTF, очная ставка с продолжением CTF и конференцией, а также ночной турнир для финалистов. В 2025 году очная ставка состоялась на территории Брусницын Холла и собрала свыше 400 участников, среди которых студенты и молодые специалисты. Кроме CTF, участники которого спасали Петербург от безумного учёного и решали задания на OSINT, криптографию, реверс, веб и форензику, зрители слушали доклады от экспертов индустрии и проходили мастер-классы.

Политехник Яков Сендов выступил первым и рассказывал о том, как по «безобидным» логам веб-сервера и открытым данным можно собрать портрет конкретного человека, и как формализовать вероятность такой деанонимизации пользователя. Илья Афанасьев, периодически разговаривая со слушателями с помощью голосового помощника, поделился опытом применения машинного обучения в атаках по побочному каналу. Григорий Пагуба в большом мастер-классе проверял желающих из зала на полиграфе и объяснял основные принципы его работы.



> В NeoQUEST я участвую с 2021 года. Это даёт мне возможность создавать новое и необычное, предлагает не совсем стандартные задачи в сравнении с типичными рабочими.
> Он вдохновляет меня на новые идеи. Так, например, на одной из конференций у нас с коллегами зародилась идея попробовать взломать полиграф. Но это, конечно, сложно, и мы решили ломать полиграфолога — естественно, не человека, а ИИ. Особенно интересным вызов казался на фоне сообщений о том, что нейросети распознают ложь лучше экспертов-людей. У тех, кто участвовал в нашем эксперименте и сидел на полиграфе, была возможность его обмануть — дыханием, движениями, сердцебиением. Что ребята, в общем-то, и делали. Совместно пришли к тому, что и сам полиграф, и профессию полиграфолога машинное обучение вряд ли скоро заменит, — поделился многолетний участник NeoQUEST, политехник Григорий Пагуба.

Во второй части мероприятия независимый исследователь Никита Тараканов препарировал безопасность Microsoft Windows. Алексей Лямкин (ВК) разбирался, что такое программы Bug Bounty, зачем они нужны компаниям и чем интересны исследователям ИБ. Анатолий Карпенко (Luntry) описал, каким образом строится SBOM-контейнера, как работают сканеры уязвимостей для Docker-образов и почему не всегда стоит доверять результатам сканеров.

Параллельно с основной программой проходили мастер-классы — по локпикингу, вай-фаю, а также специальный мастер-класс от компании СТЦ. СТЦ, кроме того, подготовил для зрителей специальный КриптоКвест с вопросами про Алана Тьюринга и ассиметричное шифрование. За все активности давали подарки.

> NeoQUEST проходит с 2012 года. В этом году мы расширили площадку, чтобы собрать ещё больше участников. В зоне докладов сфокусировались на трендовых темах — например, про искусственный интеллект и машинное обучение в вопросах кибербезопасности. Стараемся развивать мероприятие таким образом, чтобы у студентов была возможность прямого общения со специалистами отрасли, — рассказывает один из организаторов мероприятия Мария Резникова.

Оригинал статьи