«Ақпараттық қауіпсіздік негіздері» курсын үшінші курс студенттеріне оқыту тәжірибесі

Авторлары:
Мұсахан Балжан, әл-Фараби атындағы ҚазҰУ, Ақпараттық технологиялар және жасанды интеллект факультетінің 1-курс магистранты.
Максутова Бота Абильсеитовна, әл-Фараби атындағы ҚазҰУ, Компьютерлік ғылымдар кафедрасының оқытушысы.

Қазіргі киберқауіпсіздік ландшафты күрделеніп, шабуылдардың көпшілігі бағдарламалық кодтағы осалдықтарға негізделген. Осыған орай, жоғары оқу орындарында ақпараттық қауіпсіздік пәнін тек теориялық деңгейде емес, екі әртүрлі парадигмадағы бағдарламалау тілдерін (Python және C++) қолдана отырып, практикалық тұрғыдан оқыту ерекше маңызға ие. Бұл тәсіл студенттерге жоғары деңгейлі және төменгі деңгейлі қорғаныс механизмдерін түсінуге мүмкіндік береді.

«Ақпараттық қауіпсіздік негіздері» пәні әл-Фараби атындағы ҚазҰУ-нің «6B06103 — Компьютерлік инженерия» білім беру бағдарламасының үшінші курс студенттеріне арналған. Бұл кезеңде білім алушылар бұрыннан бағдарламалаудың іргелі ұғымдарын (деректер құрылымдары, алгоритмдер, жадымен жұмыс) меңгерген болғандықтан, курс ақпараттық қауіпсіздіктің терең тақырыптарын енгізуге бағытталады. Пәннің ерекшелігі — C++ тілінде жадымен тікелей жұмыс істейтін төмен деңгейлі қорғаныс механизмдерін, ал Python тілінде желілік қауіпсіздік пен криптографиялық алгоритмдерді жүзеге асыру.

Курстың оқу жоспары екі параллель трекке құрылған:

C++ трекі:

- Буферлік толып кету (buffer overflow) осалдықтарын эксперименттік зерттеу
- Стектегі CANARY қорғанысын қолмен енгізу
- Көрсеткіштермен жұмыс істеу кезіндегі қауіпсіз жады бөлу (Secure Dynamic Memory)
- ASLR және DEP механизмдерін талдау

Python трекі:

- Симметриялық және асимметриялық шифрлау (AES, RSA) — `cryptography` кітапханасымен

- Хэштеу функциялары (SHA-256, bcrypt) және парольдерді қауіпсіз сақтау (соль, итерациялар)
- Желілік трафикті талдау және шифрлау (SSL/TLS эмуляциясы)
- Кең таралған веб-осалдықтарды (SQL-injection, XSS) анықтауға арналған сканер прототипін жасау

Зертханалық жұмыстар нақты өмірлік жағдайларға негізделген. Мысалы, бір апталық тапсырма аясында студенттер C++ тілінде «осал сервер» жазып, оған Python арқылы жазылған brute-force шабуылын жүргізеді, содан кейін екі тілде де қорғаныс механизмдерін енгізеді. Мұндай тәсіл студенттердің екі тілді терең меңгеруін қажет етеді және олардың адверсариалды ойлау (adversarial thinking) қабілетін дамытады.

Студенттердің өзіндік жұмысы (СӨЖ) жобалық сипатта болады. Мысалдар:

- Өздерінің шағын VPN туннелін Python + C++ гибридті түрде іске асыру
- Қарапайым rootkit анықтау утилитасын жазу
- Екі факторлы аутентификация (TOTP) генераторын C++-та төмен деңгейлі, Python-да жоғары деңгейлі енгізу және өнімділікті салыстыру

Курстың маңызды бөлігі — кодты аудиттеу және қорғау дағдылары. Студенттер бір-бірінің жазған C++ кодындағы жадымен байланысты осалдықтарды табады, ал Python кодындағы инъекциялық осалдықтарды анықтайды. Бұл нақты индустриялық тәжірибеге жақындатады.

Пәнді қазақ тілінде оқыту арқылы күрделі қауіпсіздік терминдері мен концепциялары (мысалы, «privilege escalation», «non-repudiation», «side-channel attack») ана тілінде түсіндіріліп, студенттердің әр тақырыпты терең игеруіне жағдай жасайды.

Қорытындылай келе, «Ақпараттық қауіпсіздік негіздері» курсының үшінші курс деңгейінде Python және C++ тілдерін интеграциялай отырып оқытылуы — бұл бәсекеге қабілетті киберқауіпсіздік инженерлерін даярлаудың тиімді моделі. Түлектер төменгі деңгейдегі қорғаныс (C++) мен жоғары деңгейдегі қорғаныс (Python) механизмдерін меңгеріп, оларды бір жүйеде қалай үйлестіру керектігін біледі. Бұл — Қазақстанның цифрлық қорғаныс секторына қосылған нақты үлес.