Yang Man
Academic Supervisor: Candidate of Pedagogical Sciences, Sladkykh I. A.
Simon Kuznets Kharkiv National University of Economics

DIGITAL SECURITY IN CHINESE UNIVERSITIES

The current trend of digitalization of higher education in China includes typical scenarios: blended learning, cloud-based collaboration in scientific research, student information systems (course selection / grades), access to academic databases, learning and interaction on social platforms. The share of online courses in universities worldwide exceeds 60% (according to UNESCO, 2023); the level of "smart campus" implementation in Chinese universities exceeds 90% (data from the Ministry of Education, 2022). The main threats in Chinese universities can be identified as technical vulnerabilities: untimely system updates (for example, the risk of SQL injections in outdated learning platforms), weak or default passwords (vulnerability of student accounts to brute-force attacks). Human negligence: clicking malicious links (phishing emails disguised as "academic notifications"), shared use of accounts (several people using one account, which complicates activity tracking). Malicious attacks: ransomware (encryption of educational materials with ransom demands), DDoS attacks (paralysis of course selection systems during peak periods). Data misuse: third-party platforms illegally collect students' behavioral data (for example, tracking viewing history in educational applications for commercial purposes).

Fundamentals of digital security: technical protection through the creation of a robust "firewall." Basic measures include regular system patch updates, deployment of firewalls and intrusion detection systems (IDS), and encryption of confidential data (for example, AES-256 for student ID numbers). Training: anti-cheating technologies for online examinations (facial recognition + screen monitoring), private cloud storage, and access rights differentiation. Politics: implementation of the "Campus Network Security Regulations" and "Standards for the Use of Student Data," based on the principles of "the collector is responsible" and "minimum

necessary volume.” Process control: key operations (file deletion, access granting) require multi-level approval; regular security audits of information systems. A combined case of “technology + management.” For example, one university reduced account theft by 80% through the introduction of two-factor authentication (password + SMS code); a scientific data-sharing platform uses “watermarks + access logs” to prevent leakage of research results.

Practical Approach: Multilateral Model of Shared Governance. • **At the university level**: creation of a "Cybersecurity and Ethics Committee" (involving the information center, academic department, student affairs office, and faculty representatives). • **At the faculty level**: the role of the "primary responsible person" (emphasizing the need for originality in student work and guiding safe data handling in laboratories). • **At the student level**: establishment of the "Digital Security Volunteer Association" to spread knowledge through peer-to-peer education (e.g., posters with "Anti-Fraud Guidelines").

Specific Action Proposals: • Short-term: holding a university-wide "Digital Security Month" (lectures, competitions, rewards for vulnerability reports); mandatory training for first-year students (access to systems only after passing a test). • **Long-term**: inclusion of digital ethics in the comprehensive assessment of students' quality (records of academic integrity influence awards and incentives); collaboration with IT companies to develop specialized security tools, such as lightweight encryption plugins for scientific data.

Recommendations on technical tools: password managers (Bitwarden), VPNs (protection during off-campus access), AI-content detection tools (updated Turnitin). Education: interactive platforms (CyberSecurity Lab with simulated hacking attacks), micro-courses (“How to recognize a phishing email in 5 minutes”).

The information environment of higher education is not only a technological system, but also a digital ecosystem that transmits knowledge and shapes personality. Every teacher and student is a participant in this process; the transition from “passive protection” to “active preservation” of the integrity of the educational space in the digital era.