



Знать, чтобы защититься

Анна БАРАНОВ/
фото Виктора Орлова

В среду, 23 сентября, на базе Полоцкого государственного университета имени Евфросинии Полоцкой состоялся семинар «Основы кибербезопасности в современном информационном пространстве», организованный по инициативе Новополоцкого городского исполнительного комитета.

Киберпреступность остается одной из самых острых проблем современности. Именно этим вызовом был посвящен семинар, на котором проводилось обучение руководителей, сотрудников и идеологов предприятий, организаций и учреждений. Открытие началось с приветствен-

ного слова ректора Юрия Романовского. Затем начальник отделения по противодействию киберпреступности Новополоцкого ГОВД Андрей Зубок рассказал о профилактике киберпреступности в Республике Беларусь. По его словам, злоумышленники постоянно совершенствуют схемы: сейчас мошенниками разыгрываются целые продуманные сценарии, противостоять которым бывает крайне сложно.

Особое внимание на семинаре уделили правовым аспектам защиты персональных данных. Юриконсульт отдела безопасности ПГУ им. Евфросинии Полоцкой Алеся Дроздова-Лупова разъяснила, как законодательство регулирует эту сферу и какие меры необходимо предпринимать для защиты личной информации.

Заведующий кафедрой математики и компьютерной безопасности Ирина Бураченко раскрыла тему киберугроз в новой реальности. Она рассказала о современных вызовах, с которыми сталкиваются поль-



Спикеры напомнили присутствующим важнейшие аспекты киберграмотности

зователи: от фишинговых атак до использования технологий искусственного интеллекта в преступных целях. Отдельный блок был посвящен важнейшим аспектам цифровой грамотности – безопасности и конфиденциальности работы на компьютере и в Интернете.

По словам специалистов, ключ к защите – это бдительность. Мошенники часто действуют через мессенджеры, представляясь сотрудниками банков, правоохранительных органов или коммунальных

служб. Они могут использовать новые предлоги: «декларирование денег», «оформление электронной медкарты», «замена счетчиков или домофона». Цель одна – выманить код из СМС или убедить перевести деньги на «безопасный счет».

Правоохранители напоминают: ни один банк, ни одна государственная организация не связываются с гражданами в мессенджерах и не требуют сообщать конфиденциальные данные. При любых сомнениях лучше прервать разговор

и перезвонить по официальному номеру. А если мошенники все же получили доступ к деньгам – следует немедленно обратиться в милицию по номеру 102.

Семинар завершился обсуждением итогов. Участники отметили, что такие встречи помогают получить новые знания и сформировать привычку проверять информацию, не действовать импульсивно. В современном цифровом мире безопасность начинается с каждого из нас.