Совершение преступлений в сфере информационно-коммуникационных технологий

Наиболее актуальной проблемой в структуре и динамике преступности Минской области является рост деяний по линии противодействия киберпреступности.

Анализ статистических данных указывает, что практически каждое третье преступление как на территории Минской области, так и по республике совершается с использованием информационно-коммуникационных технологий (далее - ИКТ). Наблюдается тенденция к возрастанию тяжести последствий таких преступлений, вовлечению несовершеннолетних в преступные схемы.

По итогам 6 месяцев 2026 года в области общее количество преступлений рассматриваемой категории возросло с 1 034 до 1 362, +31,7%. Доля совершенных в сфере информационной безопасности преступлений в общей структуре преступности по области составила 28,7% (20,3%), по республике - 32,0% (27,3%).

Негативные тенденции в части увеличения количества преступлений, рассматриваемой категории, отмечаются и на территории Копыльского района.

По итогам 2025 года на территории района увеличилось количество зарегистрированных уголовно наказуемых деяний в сфере противодействия киберпреступности (+77,8 %; 18 – 32). Удельный вес киберпреступлений от общего количества зарегистрированных составил 21,3% (2024 – 12,1%).

За 6 месяцев 2026 года на фоне общего уменьшения количества преступлений на территории района несущественно снизилось количество зарегистрированных уголовно наказуемых деяний анализируемой категории (-12,5 % или 16 – 14). Удельный вес киберпреступлений в свою очередь увеличился и составил 19,9 % (19,3%).

Активное внедрение современных технологий в различные сферы жизнедеятельности делает всё более актуальным вопрос киберхищений путем фишинга, вишинга, а также кредитных средств, выданных гражданам, которые находились под влиянием кибермошенников.

В условиях активного развития цифровых технологий обеспечение личной кибербезопасности становится обязательным навыком. Для минимизации рисков и защиты персональных данных необходимо строго соблюдать следующие правила:

- **Использование сложных паролей.**

Для каждого ресурса должен быть создан уникальный пароль, состоящий из комбинации букв разного регистра, цифр и специальных символов. Использование одного пароля для нескольких сайтов недопустимо.

- **Двухфакторная аутентификация.**

Включение функции двухэтапной проверки (2FA) на всех критически важных сервисах (почта, соцсети, госуслуги, банкинг) создает дополнительный барьер для злоумышленников, даже если они узнали основной пароль.

- **Конфиденциальность кодов доступа.**

СМС-коды, ПИН-коды, CVC/CVV-коды банковских карт и одноразовые пароли являются строго конфиденциальной информацией. Их нельзя сообщать третьим лицам, кем бы они ни представлялись (сотрудниками банков, спецслужб или техподдержки).

- **Распознавание фишинга.**

Перед вводом личных данных или реквизитов карты необходимо тщательно проверять адресную строку сайта. Мошенники часто создают точные визуальные копии известных сервисов, отличающиеся от оригинала лишь несколькими символами в URL-адресе.

- **Контроль источников скачивания.**

Установка любых программ и мобильных приложений должна производиться исключительно из официальных магазинов (Google Play, App Store) или с проверенных сайтов разработчиков.

- **Использование антивирусной защиты.**

На всех персональных устройствах (включая смартфоны) должно быть установлено актуальное антивирусное программное обеспечение со включенной функцией сканирования в реальном времени.

- **Критическое отношение к сообщениям.**

Не следует переходить по ссылкам и открывать вложения в электронных письмах, мессенджерах или СМС от неизвестных отправителей. Если сообщение с просьбой о финансовой помощи пришло от знакомого, необходимо связаться с ним по альтернативному каналу связи (например, совершить обычный телефонный звонок) для подтверждения личности.

- **Безопасность финансовых операций.**

Для совершения покупок в интернет-магазинах рекомендуется использовать отдельную виртуальную карту с установленным лимитом трат, пополняя её непосредственно перед оплатой товара.

- **Осторожность с публичными сетями.**

Не стоит авторизовываться в личных кабинетах, вводить пароли и проводить платежи при подключении к бесплатному общественному Wi-Fi. При необходимости использования таких сетей следует применять VPN.

- **Защита от удаленного управления.**

Запрещено устанавливать на свои устройства программы для удаленного доступа (например, AnyDesk, TeamViewer) по указанию лиц, звонящих по телефону, кем бы они ни представлялись.

Соблюдение этих базовых правил позволяет значительно снизить риск стать жертвой киберпреступников. Финансовая и информационная безопасность в цифровой среде начинается с личной бдительности.