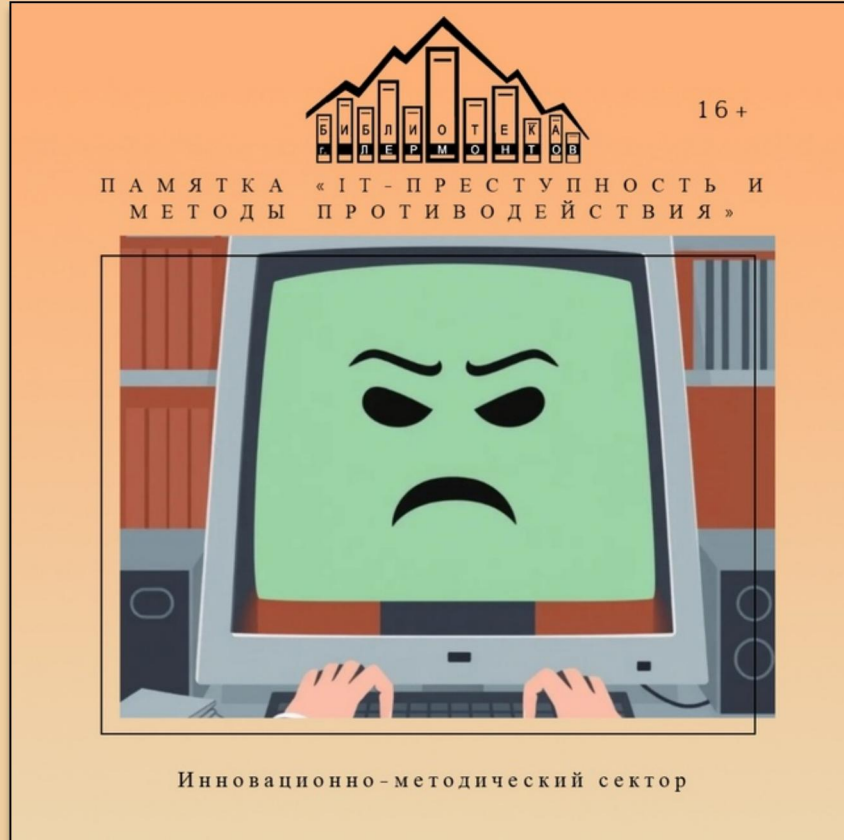




С развитием цифровых технологий злоумышленники активно используют ИТ-инструменты для совершения преступлений. Рассмотрим способы совершения преступлений с использованием ИТ-технологий и методы противодействия им.

Способы совершения преступлений с использованием ИТ-технологий:

Фишинг – способ мошенничества, при котором злоумышленники пытаются узнать жертвы конфиденциальную информацию (логины, пароли, номера кредитных карт или другую личную информацию), выдавая себя за доверенное лицо или организацию, например, банк.

Вредоносные вирусы – способ мошенничества, при котором программы крадут данные, шифруют файлы или дают злоумышленникам контроль над устройством.

DDoS-атаки – способ мошенничества, при котором происходит перегрузка серверов запросами для вывода сайтов и сервисов из строя.

Мошенничество с криптовалютами – способ мошенничества, при котором Вас убеждают сделать выгодную инвестицию, которая на самом деле будет являться фиктивной.

Звонки – способ совершения преступления, при котором мошенник представляется представителем правоохранительных органов или сотрудником банка и просит Вас назвать личные данные. Также звонок может поступить якобы от родственника, который сообщает, что попал в беду и ему срочно необходима финансовая поддержка.

Фейковые или взломанные аккаунты – способ мошенничества, при котором злоумышленники используют личные фотографии, данные лиц, которые Вам знакомы для выманивания денежных средств.

Использование фишинговых сайтов – способ мошенничества, при котором злоумышленники взламывают сайты, на которых размещаются сведения об оказании услуг по реализации авиа, ж/д билетов, бронирование гостиниц, туристические путёвки.

Методы противодействия:

- ✓ Используйте сложные пароли и двухфакторную аутентификацию.
- ✓ Не переходите по подозрительным ссылкам и не открывайте вложения от неизвестных отправителей.
- ✓ Устанавливайте лицензированные программы и регулярно обновляйте их.
- ✓ Проверяйте сайты на признаки фишинга (ошибки, странные адреса сайтов).
- ✓ Не делитесь личными данными в соцсетях и мессенджерах.
- ✓ Используйте антивирусы для защиты от вредоносных атак.
- ✓ Регулярно делайте резервные копии важных данных.

Будьте бдительны!