

## Методы и способы защиты от телефонных мошенников

Дирекцией по безопасности НИУ ВШЭ проведен анализ информации по обстоятельствам, способствующим совершению преступлений в НИУ ВШЭ, в том числе связанных с дистанционными хищениями денежных средств у обучающихся, сотрудников Университета.

С учетом установленных правовых барьеров, ограничивающих вывод похищенных денежных средств и введения уголовной ответственности за передачу электронных средств платежа и их использование лицами, не являющимися клиентами финансово-кредитных организаций, злоумышленники активно используют в преступных схемах молодых людей в возрасте от 18 до 25 лет, оказывая на них психологическое воздействие под угрозами применения насилия, а также привлечения к уголовной ответственности, якобы, за содействие Вооруженным силам Украины. Преступники, в первую очередь, делают акцент на неокрепшую психику молодых людей, на слабые знания законодательной базы, отсутствия опыта в общении с правоохранительными органами и органами государственной власти Российской Федерации. При согласии их могут использовать для проведения особо тяжких государственных преступлений в совершении террористических актов, диверсий и убийств.

В этой связи, в рамках проводимых профилактических мероприятий, необходимо акцентировать внимание сотрудников, обучающихся Университета на методы вовлечения лица (лиц) в противоправную деятельность, направленные против личности, общества и государства, и довести способы защиты от них.

### **Разъяснить сотрудникам и обучающимся Университета:**

- сотрудники правоохранительной системы Российской Федерации не привлекают граждан к поведению специальной операции по поимке злоумышленников;

- угрозы привлечения граждан и их родственников к уголовной ответственности за спонсирование Вооруженных сил Украины являются триггерными фразами, услышав которые, следует сразу прекратить общение и сообщить о произошедшем в правоохранительные органы;

- финансово-кредитные организации, операторы связи, управляющие компании, службы доставки и иные государственные и коммерческие организации и объединения не запрашивают в ходе телефонных разговоров коды.

Кроме того, в настоящее время одним из актуальных способов введения в заблуждения граждан является распространение, посредством мессенджеров, сгенерированных при помощи искусственного интеллекта медиафайлов – deep fake.

В мессенджере потенциальной жертвы, как правило, приходит видеосообщение от лица из списка контактов, которые может сопровождаться аудиозаписью, содержащей информацию о предстоящем телефонном звонке или контакте с сотрудниками правоохранительных органов (ФСБ России, МВД России, Росфинмониторинга и т.д.), а также требования по неукоснительному соблюдению их указания. В дальнейшем в ходе «оперативной игры» используются классические сценарии совершения преступления: перевод денежных средств на «безопасный» счет, декларирование наличных денежных средств, мнимые сделки с имуществом от лица граждан и иные сценарии. Таким образом осуществляется вербовка в категорию «курьеры», исполнителей поджогов, подрывов различных объектов инфраструктуры.

Отсутствие знаний о способах совершения преступления и методах защиты от них, может привести к значительным финансовым потерям, а в иных случаях к более тяжким преступлениям.

### **Девять признаков, по которым можно распознать deep fake:**

На экране электронного устройства потенциальной жертвы отображается:

- «липкая» кожа вокруг рта и подбородка, смазанные зубы. При артикуляции контуры губ и зубов нечеткие;
- нестыковки морганий глаз, наблюдается эффект «стеклянного» взгляда, либо практически отсутствует моргание глаз или это происходит рывками и не вовремя;
- падающая на лицо тень меняется нелогично, наблюдаются блики на коже, предметах;
- плавающие контуры волос, предметов. Мелкие детали около лица двигаются неестественно или слегка дрожат;
- «ломаются» тексты в видеокадре, искаженные буквы, неровные логотипы;
- рваные швы между кадрами, от перехода между кадрами меняется цвет одежды, мелкие детали фона;
- эмоции не совпадают с речью;
- тембр голоса слишком ровный, почти нет дыхания, пауз, окружающих шумов;
- неестественные или несвойственные фразы, сухой, «текстовый» язык, странный порядок слов, наблюдаются повторы фраз.

**В случае выявления вышеперечисленных признаков в кадре и для организации проверки необходимо:**

- осуществить телефонный звонок лицу на его номер телефона, от которого поступило сообщение;

- выполнить скрин экрана или сохранить фото и осуществить по нему поиск через Google Images, Яндекс.Картинки, TinEye;
- посмотреть/послушать видео и аудио ряд на скорости 0,5x и 1,5x. На замедленном воспроизведении заметно рассинхрон губ и голоса, склейки и скачки мимики;
- сравнить версии на разных платформах. Один и тот же ролик в разных социальных сетях может отличаться длительностью, водяными знаками, качеством;
- проверить метки «altered/synthetic», Content Credentials или Watermark. Многие площадки отмечают ИИ-контент специальными маркерами.

### **Если возникает подозрение по признакам генерации с использованием искусственного интеллекта:**

- «код-фраза + резервный канал» Заранее обговоренные с близкими и коллегами простые код-фразы, при сообщении которых появляется уверенность, что общение проходит с живым человеком, а не с генерированной моделью, созданной с использованием искусственного интеллекта. При условии невозможности абонентом назвать «код-фразу» (условное слово) или подтвердить его присутствие, как абонента через резервный канал, необходимо прекратить общение;
- «свет и ракурс» Попросить повернуться абонента в профиль, провести ладонью перед лицом, снять и надеть очки, наушники или иные аксессуары. При выполнении этих действий у многих deep fake не четко выражены контуры лица, блики и тени;
- «случайные микродействия» Поставьте задачу абоненту по выполнению несложных действий, которые сложно воспроизвести с использованием искусственного интеллекта: Поднять правую бровь, коснуться левого уха, покади пальцами набор цифр 2-4-1, эти действия позволят выявить генерацию. Электронные системы, работающие в реальном времени, часто не успевают корректно перестроить мимику и жесты;
- «аудио проверка» Попросить абонента сделать длинный вдох в микрофон или быстро повторить скороговорку или редкие слова, что позволит увидеть склейки кадров, пропадающие звуки, «стерильный» тембр;
- «смена сцены» Попросить подвинуть лампу или штору, переключиться на камеру телефона. При смене таких условий многие электронные системы начинают функционировать с перебоями.

### **Главные правила сотрудникам и обучающимся Университета:**

- не доверять -аудио-видео информации.
- Принимать решения только после ее перепроверки с использованием резервного канала связи или путем личного общения с абонентом;
- ограничить «чистые» записи голоса.

Не следует выкладывать длинные монологи и аудио записи там, где в этом нет необходимости;

- осторожное отношение к «срочным просьбам».

Фразы «прямо сейчас», «иначе потеряем деньги/контракт», «привлекут к уголовной ответственности» - типичные приемы мошенников.

Привлекать к работе штатных педагогов-психологов. Обращать внимание на лиц, попавших под психологическое влияние, которым свойственно резкая смена поведения, замкнутость и отрешенность, избегающие контакта с внешним миром.

При выявлении подобных признаков необходимо брать под психологический контроль таких лиц в целях недопущения совершения ими противоправных действий.

Директор по безопасности НИУ ВШЭ

10 марта 2026 г.



С.Ю. Чапчиков