Конспект по теме: «Актуальные способы совершения киберпреступлений»

Электронные сервисы, интернет-банкинг, удаленная работа и учеба, социальные сети, интернет-магазины и маркетплейсы прочно вошли в нашу повседневность. Однако, чем глубже мы погружаемся в мир информационно-коммуникационных технологий, тем уязвимее становимся для интернет-преступников. Киберпреступность активно развивается: с появлением новых технологий меняются схемы и способы обмана. Особое беспокойство вызывает применение искусственного интеллекта в преступной деятельности.

В нашей стране среди основных способов совершения таких преступлений выделяются телефонное мошенничество (вишинг), хищения под предлогом продажи товаров через интернет, а также схемы, связанные с обещаниями быстрого заработка и инвестирования. Преступники постоянно адаптируют свои схемы под актуальные общественные тенденции и популярные услуги. Главным рычагом воздействия для них выступают эмоции: они стремятся напугать человека, создать ощущение срочности и лишить возможности спокойно оценить ситуацию или посоветоваться с близкими, из-за чего в ловушку попадаются не только пожилые, но и молодые, образованные граждане.

Основные схемы и способы киберпреступлений.

Телефонное мошенничество (вишинг)

Злоумышленники массово совершают звонки, представляясь сотрудниками банков, правоохранительных органов, мобильных операторов или коммунальных служб. Под предлогом замены домофона, продления договора на услуги или подключения нового тарифа они пытаются выманить личные данные или СМС-коды.

Затем следует второй звонок – уже от «сотрудника правоохранительных органов», который сообщает, что персональными данными завладели преступники, счета находятся под угрозой, а для их спасения необходимо перевести средства на «безопасный счет», оформить кредит или передать наличные курьеру для декларирования. Для убедительности мошенники используют видеосвязь, демонстрируют фальшивые удостоверения и называют реальные фамилии должностных лиц.

Важно: сотрудники милиции никогда не предлагают гражданам переводить деньги на «безопасные счета», оформлять кредиты или передавать сбережения курьерам. При появлении таких требований разговор необходимо немедленно прекратить.

Мошенничество при покупке товаров через Интернет

С развитием торговли через Instagram, TikTok, Telegram и другие площадки преступники создают убедительные интернет-магазины-клоны с красивыми фотографиями, положительными отзывами и большой аудиторией, где популярная техника или одежда продается по очень привлекательным ценам. После внесения покупателем предоплаты или полной стоимости продавец удаляет страницу и перестает выходить на связь. Наличие красивого оформления и множества подписчиков не гарантирует надежности продавца, поскольку мошенники просто копируют их у реальных магазинов.

Как защититься: остерегайтесь подозрительно низких цен, не переводите предоплату, выбирайте наложенный платеж. Проверяйте наличие у продавца официального сайта в белорусском сегменте интернета и созванивайтесь по телефону.

Фальшивые инвестиционные и криптоплатформы

Используя стремление людей улучшить свое финансовое положение, мошенники размещают рекламу о высоком доходе от вложений в акции, криптовалюту или торговлю на финансовых рынках. После регистрации на специальной платформе и внесения минимальной суммы с жертвой связывается «финансовый консультант», который помогает совершать сделки, демонстрируя на экране фиктивный рост прибыли (иногда позволяя вывести небольшую сумму для создания иллюзии надежности). Затем человека склоняют к крупным вложениям, оформлению кредитов и продаже имущества, а при попытке вернуть средства требуют дополнительно оплатить комиссию, налог или страховку, забирая все деньги себе. Обещания гарантированного высокого дохода без риска всегда свидетельствуют о мошенничестве.

Кибермошенничество в отношении несовершеннолетних

Дети и подростки активно пользуются смартфонами и онлайн-играми, где виртуальная валюта, редкие предметы и скины имеют реальную стоимость. Мошенники обманывают детей под видом дешевой продажи игровых предметов, предложений бесплатной игровой валюты или участия в розыгрышах, заставляя переходить по фишинговым ссылкам и вводить учетные данные. Получив доступ к аккаунту, злоумышленники могут украсть игровые ценности и поставить под угрозу привязанные родительские банковские карты. Кроме того, доверчивость подростков используется для вовлечения их в противоправную деятельность в качестве «дропов» для перевода похищенных денег.

Особую опасность представляет жесткое психологическое давление: выдавая себя за сотрудников правоохранительных органов или спецслужб, преступники запугивают детей, внушают им чувство вины или страха за безопасность родителей. Ребенка убеждают в том, что его семья якобы замешана в преступлении, после чего манипуляторам удается заставить школьников выполнять любые указания, включая поиск и передачу крупных семейных сбережений. Родителям необходимо регулярно контролировать цифровую жизнь детей, объяснять им правила безопасности и использовать специальные инструменты родительского контроля (Google Family Link для Android и «Экранное время» для iPhone).

Наглядные примеры подобного давления и его последствий:

август 2026 года (Минск): 10-летнего школьника под предлогом замены домофона убедили назвать код из SMS. Лжеправоохранитель по видеосвязи заявил, что семья подозревается в мошенничестве, и потребовал «задекларировать» накопления. Школьник вынес из дома 160 тыс. долларов, 30 тыс. евро и 30 тыс. рублей, оставив их в кустах поблизости.

октябрь 2025 года (Минский район): школьника после отправки геолокации запугали терактом и заставили вынести 70 тыс. долларов, оставив их в лесу.

ноябрь 2026 года (Минск): третьеклассник продиктовал код для «замены домофона», после чего испуганный ребенок отдал незнакомцу в подъезде 12 тыс. долларов.

Вымогательство за разблокировку iPhone

Мошенник в переписке узнает о наличии у жертвы iPhone и под предлогом помощи (восстановление фото, сохранение диплома, прокачка игрового персонажа) убеждает войти в чужой iCloud. После этого смартфон блокируется, а за разблокировку требуют выкуп (от 1000 рублей и выше в зависимости от модели).

Поддельные мобильные приложения и NFC-мошенничество

Аферист звонит под видом сотрудника банка или оператора связи (Белтелеком, A1, МТС) и убеждает обновить мобильное приложение, скачав файл (*.apk) из мессенджера. Поддельное приложение открывает удаленный доступ к устройству. Мошенник может попросить пин-код и приложить банковскую карту к задней крышке телефона (к модулю NFC), чтобы создать цифровой дубликат карты и похитить деньги.

Профилактические рекомендации гражданам

Защита личной информации: необходимо проверить настройки конфиденциальности в смартфоне и мессенджерах, ограничив доступ посторонних лиц к номеру телефона, фотографии профиля, списку

контактов, геолокации, камере и микрофону. Не следует размещать в открытом доступе личные данные, адреса и сведения о поездках.

Базовая цифровая гигиена: рекомендуется включить двухэтапную проверку входа в аккаунты, использовать надежные пароли, категорически отказаться от установки приложений по указанию неизвестных лиц и никогда не сообщать никому коды подтверждения и пароли от интернет-банкинга. Для безопасных покупок в сети целесообразно завести отдельную банковскую карту с ограниченным балансом.

Алгоритм экстренных действий: если гражданин уже сообщил мошенникам свои данные или перевел деньги, ему необходимо незамедлительно обратиться в банк для блокировки операций, принять меры по защите аккаунтов и срочно сообщить о случившемся в милицию, так как оперативность обращения повышает шансы на предотвращение ущерба.

Главные правила безопасности:

никогда не выполняйте финансовые операции по указанию незнакомцев, кем бы они ни представлялись;

не поддавайтесь панике: как бы вас ни запугивали по телефону или видеосвязи, сохраняйте критическое мышление;

не устанавливайте сторонние приложения по ссылкам из мессенджеров и никому не передавайте коды из SMS.

Конспект предназначен для использования личным составом ОВД при проведении профилактических мероприятий среди населения.