



ГУ МВД России по Московской области

Управление Министерства внутренних дел
Российской Федерации
на комплексе «Байконур»
(УМВД России на комплексе «Байконур»)

пр. Абая, 1, Байконур,
Республика Казахстан, 468320
тел. (33622) 7-74-00, факс (33622) 7-61-71
01.12.2025 40/26-44465

на № _____ № _____
от _____

О направлении профилактического материала

Первому заместителю
главы администрации
города Байконур

Вербицкому Т.И.

пр. Королева, 33, Байконур,
Республика Казахстан, 468320

Уважаемый Тимур Иванович!

УМВД России на комплексе «Байконур» запланирован комплекс профилактических мер, направленный на предупреждение и пресечение имущественных преступлений, совершаемых с использованием информационно - коммуникационных технологий в отношении жителей города Байконур.

В целях повышения эффективности противодействия противоправным деяниям в IT-сфере и своевременного информирования жителей города Байконур о новых видах, схемах и способах совершения преступлений в IT-сфере, а также о методах соблюдения цифровой безопасности прошу Вас организовать размещение приложенной к настоящему письму информации в ленте событий курируемых групп в социальных сетях и мессенджерах, а также на странице официального сайта администрации города Байконур.

Для оперативного взаимодействия по вопросам профилактики (в том числе при возникновении рассматриваемых событий) от УМВД России на комплексе «Байконур» определен старший оперуполномоченный группы по борьбе с мошенничествами отдела уголовного розыска майор полиции Гуськов Иван Витальевич (контактный номер телефона: +7 771 317 4501).

Приложение: профилактические материалы, на 8 листах, только в адрес.

С уважением,

Врио начальника

Исп. И.В. Гуськов
87713174501



ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат C594F56AEEC286B287C572F333BF56DA
Владелец Звягинцев Сергей Михайлович
Действителен с 25.08.2025 по 18.11.2026

С.М. Звягинцев

Приемная первого заместителя Главы
администрации города Байконур

Входящий

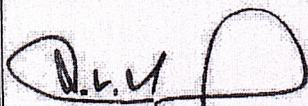
№ 02/10 - 3460

«02» 10 2025

на 9 листах

**ПЕРВЫЙ ЗАМЕСТИТЕЛЬ
ГЛАВЫ АДМИНИСТРАЦИИ
ГОРОДА БАЙКОНУР**

Волкову С.А., Петелину С.П., Бобровице
Для сведения А.Г. и Агееву Н.П.
Урусову О.А. Для курьерского задания
Для работы установленным порядком



Т.И. Вербицкий

«02» 10 2025 г.

№ 02/10-3460 от 02.10 2025 г.

Сведения о новых видах, схемах и способах совершения дистанционных преступлений, а также о модернизации «старых» преступных схем

Мошенничество с билетами!

В предновогодний период мошенники активизируют распространение и продажу поддельных билетов на культурные мероприятия (новогодние представления, концерты, балет и т.д.).

Мошенники массово осуществляют продажу поддельных билетов на различные мероприятия, используя фейковые сайты, поддельные страницы в соцсетях и рассылки.

Чтобы не оказаться в подобной ситуации:

! Покупайте билеты только на официальном сайте театра или у проверенных билетных операторов.

! Не переходите по ссылкам из рекламных сообщений и рассылок – вводные страницы часто маскируются под оригинал.

! Проверяйте URL – одно лишнее слово или странный домен обычно выдает подделку.

! Оплачивайте картой через защищенные платежные формы; избегайте переводов на неизвестные реквизиты и криптовалюту.

! Если покупаете у частного продавца – просите фото билета, чек и документы, встречайтесь в безопасном месте.

! Избегайте сайтов-однодневок и площадок-двойников с нерабочими контактами или подозрительно низкими ценами.

! При сомнениях уточняйте информацию по официальному телефону театра.

Мошенники в фан-клубах!

Мошенники все чаще ищут жертв среди поклонников на официальных сайтах фан-клубов и в социальных сетях. Они выдают себя за ассистентов или самого кумира, обещая личное общение и даже встречу.

Сначала начинается длительная переписка – иногда неделями. Мошенник рассказывает трогательную историю, что именно вы – избранный фанат, с которым артист хочет познакомиться лично. Затем следует просьба перевести деньги на билет или другие «необходимые расходы» для встречи. Эти деньги вы уже не увидите!

Чтобы не оказаться в подобной ситуации:

! Никогда не переводите деньги незнакомцам, даже если они кажутся связанными с вашим кумиром.

! Проверяйте информацию через официальные каналы артиста: сайт, соцсети или проверенные фан-страницы.

! Помните, что реальные звезды не просят напрямую оплатить что-то через сообщения.

Мошенники подменяют QR-коды!

Злоумышленники наклеивают свои поддельные QR-коды поверх оригинальных на афишах, парковках, в кафе и других местах.

Выглядит очень убедительно: на коде сохранен логотип, фон совпадает, поэтому сразу не отличить. Но после сканирования вы попадаете на фишинговый сайт, где просят ввести личные данные – и вы становитесь жертвой кражи информации.

Как не попасться на эту цифровую ловушку:

! Не сканируйте все подряд! Если QR-код вы видите на улице или на листовке, будьте осторожны.

! Проверьте адрес перед переходом: большинство смартфонов показывают ссылку до открытия сайта.

! Для оплаты используйте только официальные приложения. Ни в коем случае не переходите по подозрительным ссылкам.

! Обращайте внимание: QR-код должен быть напечатан на афише, а не наклеен сверху.

Кражи аккаунтов в мессенджерах через объявления

Злоумышленники размещают объявления в соцсетях и на площадках с QR-кодами или ссылками, ведущими на фальшивые страницы авторизации популярных мессенджеров. Пользователю предлагают ввести номер телефона и код подтверждения, который в итоге попадает к мошенникам: с его помощью они получают доступ к аккаунту жертвы.

После входа в мессенджер злоумышленники просматривают переписку, копируют личные данные и фотографии, а затем используют их для шантажа или рассылки новых фишинговых ссылок от имени взломанного пользователя.

Что нужно помнить:

✓ Для защиты аккаунтов необходимо проверять адрес сайтов перед вводом данных, не переходить по ссылкам из подозрительных объявлений и обязательно включить двухфакторную аутентификацию.

✓ В случае потери доступа следует немедленно обратиться в поддержку мессенджера и сменить пароли во всех связанных сервисах.

Мошенничества в налоговой сфере

1) Мошенники атакуют перед праздниками под предлогом выплаты 13-й зарплаты!

Аферисты ловко используют праздничное настроение и сниженную бдительность, чтобы выманить у россиян деньги или личные данные. Жулики требуют оплату налогов, комиссий или просят предоставить личные данные для получения «премии». При этом они активно используют фишинговые сайты, поддельные письма, SMS и звонки якобы от банков или госорганов.

Что нужно помнить:

- ✓ Перед праздниками будьте максимально внимательны с финансовыми операциями.
- ✓ Никогда не переходите по подозрительным ссылкам и не вводите личные данные на неизвестных сайтах.
- ✓ Не платите никаких «налогов» или «комиссий» незнакомым людям и организациям.
- ✓ При сомнениях связывайтесь напрямую с банком или государственным учреждением по официальным каналам.

Рекомендации для безопасности:

- ! Проверяйте отправителя сообщений и звонков.
- ! Используйте двухфакторную аутентификацию для онлайн-банкинга.
- ! Не спешите и всегда уточняйте информацию через официальные источники.

2) Мошенничества с налоговыми вычетами!

Аферисты звонят через мессенджеры и обещают помощь в получении налогового вычета. Они просят включить демонстрацию экрана, чтобы якобы «грамотно оформить декларацию».

Когда жертва соглашается, на её телефон приходит код с портала «Госуслуги». И вот тут начинается обман – мошенник получает доступ к аккаунту и может похитить личные данные и деньги!

Чтобы не оказаться в подобной ситуации:

- ! Никогда не соглашайтесь показывать экран незнакомцам.
- ! Не передавайте коды подтверждения, которые приходят на телефон – это личная информация!
- ! Проверяйте звонки и сообщения через официальные каналы.
- ! Если вам обещают выплаты или вычеты – обращайтесь напрямую в налоговую и через портал Госуслуг.
- ! Установите антивирус и обновляйте программы на вашем устройстве.

3) Мошенники подделывают уведомления ФНС!

В период подготовки налоговой отчётности участились случаи мошенничества, когда злоумышленники под видом инспекторов ФНС пытаются получить доступ к банковским счетам граждан.

Гражданам стали чаще звонить мошенники, представляясь сотрудниками налоговой службы. Звонящий озвучивает подробные персональные данные жертвы: адрес регистрации, номер телефона, почту, ФИО и другие сведения. Такая детализация вызывает доверие, после этого злоумышленник часто обвиняет человека в том, что тот не подал налоговую декларацию за прошлый год, а затем предлагает записаться на прием в ФНС. Для подтверждения записи приходит СМС с кодом (чаще всего для доступа к Госуслугам), который мошенник просит озвучить.

Такие атаки становятся возможными из-за регулярных утечек баз данных с популярных сервисов. Мошенники собирают данные из множества источников, таких как утечки баз крупных онлайн-магазинов, сервисов и банков, списки персональных данных у data-брокеров и на даркнет-рынках, публичные профили и блоги в соцсетях и мессенджерах, а также инсайдерские сливы. Комбинируя фрагменты из разных утечек, злоумышленники формируют полные «профили» жертв и используют их для убедительных сценариев обмана.

Важно помнить:

- ✓ Запись на приём в налоговую осуществляется исключительно через личный кабинет на сайте ФНС или через Госуслуги.
- ✓ Налоговая инспекция НЕ связывается с гражданами по телефону или через мессенджеры.
- ✓ Никогда не вводите коды из СМС по просьбе незнакомцев!
- ✓ Проверяйте всю информацию только через официальный сайт и личный кабинет.

Чтобы не оказаться в подобной ситуации:

- ! Если подозреваете, что звонок – мошенничество, положите трубку.
- ! Свяжитесь с налоговой службой напрямую через официальный сайт или телефон.
- ! Никому не передавайте свои пароли и коды из сообщений!

Мошенничества в сфере доставки товаров (подарков)

Мошенники выдают себя за «Yandex Delivery» и крадут данные карт через фейковые сайты доставки.

Злоумышленники представляются сотрудниками несуществующего сервиса «Yandex Delivery» и других курьерских служб.

Жертвам рассылают письма и SMS со ссылками на поддельные сайты.

В сообщениях говорится о выплате за доставку товара или «успешной регистрации» в сервисе. После перехода по ссылке пользователю предлагают ввести данные банковской карты и телефон, якобы для подтверждения перевода. На деле информация сразу уходит мошенникам.

Атака выглядит убедительно так как: фишинговые страницы копируют дизайн известных компаний и используют названия, похожие на реальные бренды, например, «Yandex Delivery» вместо «Yandex Go» или «Delivery Club». Это снижает настороженность пользователей и повышает шансы злоумышленников на успех.

Важно помнить:

- ✓ При получении подобных сообщений важно сохранять бдительность.
- ✓ Не следует переходить по ссылкам из писем или SMS, особенно если в них обещают выплату или вознаграждение.
- ✓ Адрес сайта лучше вводить вручную через поиск и внимательно проверять доменное имя – мошенники часто используют схожие варианты с орфографическими ошибками.
- ✓ Также нельзя вводить данные банковских карт на страницах, полученных по ссылке из мессенджеров или социальных сетей.

Рекомендации для безопасности:

- ! Не сообщайте коды подтверждения неустановленным лицам.
- ! Проверяйте наличие и статус доставок только на официальных сайтах.
- ! Не сообщайте данные о себе и банковские реквизиты по телефону!

Поддельные интернет-магазины, торгующие красной икрой и другими морепродуктами.

С приближением новогодних праздников участились случаи, когда злоумышленники создают сайты, оформленные как легитимные витрины с деликатесами. Покупатель выбирает товар, оплачивает заказ, но продукт к нему так и не приходит. Такие схемы особенно эффективны из-за роста популярности онлайн-покупок и стремления людей сэкономить.

Создать фишинговый сайт сейчас не составляет труда. Достаточно наполнить его привлекательными картинками и скопировать внешний вид настоящего магазина. Это создаёт иллюзию доверия и облегчает мошенникам задачу.

- ✓ Рекомендуется покупать продукты только в проверенных магазинах и маркетплейсах, а при заказах в новых магазинах не оставлять предоплату и не передавать данные банковских карт. При покупке икры на развес важно учитывать условия хранения и транспортировки, поскольку недобросовестные продавцы часто их нарушают.

Мошенничества, связанные с ТСЖ

Злоумышленники создают в мессенджерах («WhatsApp», «Telegram» и т.д.) фальшивые группы от имени председателя, используя его фотографию и имя.

В таких группах рассылаются сообщения якобы об обновлении списка жильцов ТСЖ.

Цель мошенников – получить доступ к системе ГИС ЖКХ, связанной с государственными услугами.

Чтобы не оказаться в подобной ситуации:

! Никогда не переходите по ссылкам и не предоставляйте личные данные через непроверенные каналы.

! Официальные уведомления от ТСЖ публикуются только в проверенных и официальных источниках.

! Если вы получили подозрительное сообщение, уточняйте информацию напрямую у председателя или органов ТСЖ.

! Не сообщайте пароли и данные от Госуслуг никому!

! Если заметили подобные группы – сообщите в администрацию ТСЖ.

Мошенники притворяются благотворителями и обещают выплаты семьям участников СВО

Злоумышленники создают фейковые сайты благотворительных организаций и от имени НКО предлагают семьям участников СВО якобы государственные выплаты, используя поддельные документы, дипфейки и ссылки на «приказ президента».

Аферисты маскируются под легитимные фонды, обещая по 500 000 рублей в месяц в рамках вымышленных «инвестиционных программ». Для убедительности они утверждают, что «вклады застрахованы», а в поддержку своих слов публикуют видеоролики с дипфейковыми «отзывами бойцов».

Мошенники действуют не только через сайты-двойники, но и в социальных сетях, где фальшивые страницы «фондов» собирают лайки и репосты, публикуют трогательные посты и просят перевести деньги на «помощь фронту».

Рекомендации для безопасности:

! Проверяйте отправителя сообщений и звонков.

! Используйте двухфакторную аутентификацию для онлайн-банкинга.

! Не спешите и всегда уточняйте информацию через официальные источники.

✓ Участники СВО и члены их семей могут получить помощь и консультацию в Московском областном отделении Всероссийской организации ветеранов «БОЕВОЕ БРАТСТВО» (Московская область, г. Химки, ул. Панфилова, владение 19, строение 4, тел.: +7 (499) 601-20-77, электронный адрес: bb_mosobl@mail.ru).

Дипфейк-мошенники набирают обороты!

Теперь, чтобы обмануть, не нужен актёр – достаточно **нейросети**. Мошенники создают видео и аудио с поддельными лицами и голосами, чтобы убедить людей перевести деньги или раскрыть личные данные.

Как это выглядит:

«Звонит» ваш начальник и просит срочно отправить деньги партнёрам – голос и лицо совпадают.

Родственник «попал в беду» и записывает видео, умоляя о помощи.

Известный блогер «рекламирует» инвестиции с гарантированной прибылью.

Рекомендации для безопасности:

- ! Не принимайте решения на эмоциях.
- ! Проверяйте информацию другими каналами связи.
- ! Используйте стоп-слово с близкими – короткий код, по которому можно проверить, что это действительно они.
- ! Будьте особенно внимательны к «срочным» просьбам о деньгах.

✓ **Помните: дипфейк звучит и выглядит реально, но не всегда истинно. Не дайте технологии сыграть против вас!**

Риски, связанные с раскрытием и публикацией информации о своих перемещениях в реальном времени, включая использование геометок

Делясь в соцсетях отпускными снимками, вы рискуете своей личной безопасностью. Подобные действия могут привлечь внимание злоумышленников. По геометкам и контенту в соцсетях злоумышленники легко понимают, что дом владельца пуст, и могут воспользоваться этим.

Мошенники могут собирать в соцсетях информацию о человеке, его увлечениях и маршрутах, чтобы придумывать убедительные фишинговые или скам-схемы, а фото и видео использовать для создания дипфейков, шантажа.

Рекомендации для безопасности:

- ! Выкладывайте фотографии уже после возвращения из отпуска.
- ! Ограничивайте круг зрителей и внимательно проверяйте настройки приватности.

Фейковые SMS от Антифрод-систем от имени банков

Злоумышленники рассылают поддельные SMS якобы от Антифрод-систем банков и требуют от жертв перевести «небольшую сумму» для подтверждения операции.

Аферисты представляются службой безопасности банка и просят совершить перевод, чтобы «подтвердить отсутствие кражи». Особенность схемы – использование некруглых сумм, например, 49 990 рублей. Мошенники делают это для обхода настоящих Антифрод-систем, которые автоматически фиксируют крупные переводы на круглые суммы как подозрительные.

Мошенники всё чаще комбинируют рассылку SMS с обратными звонками.

✓ **Важно помнить: подобные SMS не имеют отношения к банкам.**

Распространённые фразы мошенников, по которым можно быстро распознать обман

! «Переключаю вас на сотрудника Центробанка, правоохранительных органов, финансового надзора»

! «Это ты на фото?»

! «Ваш аккаунт на портале «Госуслуг» взломан»

! «Финансирование запрещённой (экстремистской) организации»

! «Звоню по поводу удалённой работы»

! «Это отдел курьерской доставки, на ваше имя поступило заказное письмо (посылка)»

! «На ваших банковских счетах обнаружены неучтённые средства»

! «Необходимо задекларировать денежные средства и ценности»

! «Беспокоит директор департамента (руководитель компании). Связываюсь с вами из-за текущей проверки»

✓ **Если вы или ваши близкие услышали эти слова по телефону, просто положите трубку!**

**И.о. заместителя Главы
администрации города Байконур**

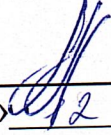
Квядарас А.С.

Осипяну А.Р.

Горьковому С.Н.

Киму А.Н.

Прошу довести указанную информацию
до сведения подчиненных сотрудников

 **С.П. Лetyагин**
« 03 » 12 2025 г.

№ 03/17-2806 от 03.12. 2025 г.