Рабочая группа по инновациям, информационным технологиям, цифровизации Общественной палаты Тюменской области

625000, Тюмень, Советская, 61
+7 (908) 874-47-47
+7 (3452) 42-60-50

komov75@yandex.ru
http://op72.ru

ИТОГОВЫЙ ОТЧЁТ ПО РЕЗУЛЬТАТАМ КРУГЛОГО СТОЛА

«Противодействие цифровому мошенничеству: требования к банкам и операторам связи по защите граждан»
14.10.2026 г.

Организатор: Рабочая группа по инновациям, информационным технологиям и цифровизации Общественной палаты Тюменской области при поддержке Департамента информатизации Тюменской области.

Дата проведения: 14 октября 2026 года.

Место проведения: г. Тюмень, ул. Советская, 61, Малый зал.

Цель мероприятия: Формирование прикладных рекомендаций по цифровой безопасности для жителей Тюменской области, выработка согласованных мер противодействия цифровому мошенничеству со стороны государства, банков, операторов связи и общественных институтов.

1. Вступительное слово и постановка проблемы

Модератор мероприятия Комов Алексей Васильевич (руководитель рабочей группы по инновациям, ИТ и цифровизации ОП ТО) открыл круглый стол и обозначил, что ущерб от дистанционных преступлений исчисляется миллиардами рублей, и главная задача встречи - перейти от констатации фактов к выработке конкретных предложений по комплексу дополнительных мер защиты граждан.

Чеботарев Геннадий Николаевич (председатель Общественной палаты Тюменской области) в приветственном слове связал противодействие мошенничеству с защитой конституционных прав граждан, отметив необходимость формирования этических и правовых норм в сфере регулирования искусственного интеллекта (ИИ), который всё чаще используется злоумышленниками.

Заместитель Губернатора Тюменской области, директор департамента информатизации Тюменской области Станислав Игоревич Логинов представил региональные практики противодействия цифровому мошенничеству. Так, в Тюменской области работает портал «Детская безопасность в сети», где публикуются реальные истории встреч жителей региона с кибермошенникам, а также интерактивы и викторины. Запущен региональный журнал по детской кибербезопасности «Интернет без опасности» — это цифровой дайджест, где каждый выпуск раскрывает одну тему — от дропперства и видеоигр до личных данных и нейросетей.

Кроме того, в регионе проходят семинары и лекции по кибербезопасности, вебинары по финансовой защите и «Уроки цифры» в школах. Для детей организуют мастер-классы по информационным технологиям в летних лагерях и на базе Центра робототехники и автоматизированных систем управления. Освоить жителем цифровую гигиену помогает программа «Расширяя горизонты». Была отмечена важность интерактивных форматов (игр) и анонимной обратной связи для детей. Логинов С.И. предложил провести для студентов мероприятие, посвященное вопросам кибергигиены, с участием отраслевых экспертов.

2. Анализ выступлений экспертов:

2.1. Банк России: системная защита и статистика

Спикер: Патрактинова Ольга Александровна, заместитель управляющего Отделением по Тюменской области Уральского главного управления Банка России.

- Статистика хищений: за I полугодие 2026 года в России совершено 954,4 тыс. хищений на сумму 14,7 млрд рублей. За весь 2025 год похищено 29,3 млрд рублей (1,6 млн операций). При этом банками предотвращено хищений на 3,7 трлн рублей (34,3 млн операций). Эффективность антифрод-систем оценивается в 99,85%.

- Структура ущерба (2025 г.): 82% хищений — до 20 тыс. руб.; 12% — от 20 до 100 тыс. руб.; 5% — от 100 до 500 тыс. руб.; 0,9% — от 500 тыс. до 1 млн руб.; 0,1% — свыше 1 млн руб.

- Инструменты защиты: с 01.03.2025 работает «Самозапрет на кредиты» (в Тюменской области установлено 344 тыс. самозапретов). С 01.09.2025 внедрен сервис «Второй руки» и «Период охлаждения» (от 4 часов до 2 суток в зависимости от суммы потребительского кредита, займа). Введены ограничения на снятие наличных (до 50 тыс. руб./сутки на 48 часов) при выявлении признаков мошенничества.

- Дропперы: введен лимит 100 тыс. руб. в месяц на переводы и снятие наличных в банкоматах для лиц, находящихся в базе ЦБ. Блокировка карт и онлайн-банка при получении данных от МВД обязательна.

- Метрики блокировок: за 8 месяцев 2026 года Банк России направил на блокировку 20 409 телефонных номеров и 19 710 интернет-ресурсов.

- Обращения граждан: Доля пострадавших, обратившихся и в банк, и в полицию, выросла с 34% (2024 г.) до 39% (2025 г.).

2.2. УМВД России по Тюменской области: оперативная обстановка

Спикер: Попков Вадим Юрьевич, начальник управления по борьбе с противоправным использованием ИКТ УМВД России по Тюменской области, подполковник полиции.

- Динамика преступности: Количество зарегистрированных ИКТ-преступлений снизилось с 8343 до 4727 (снижение на 43,3%). Доля в общей структуре преступности упала с 45,9 до 31,9%.

- Проблема дропперства: Возбуждено более 100 уголовных дел по ст. 187 УК РФ. Отмечен рост стоимости «дроп-комплектов» (карт) на черном рынке с 5 до 50 тыс. рублей. Вовлекаются несовершеннолетние (например, случай в водном колледже).

- Скорость вывода средств: Деньги обналичиваются в течение 5–50 минут после перевода.

- Уязвимости: Повторная продажа SIM-карт (предложено уведомлять Минцифры и ЦБ). Слабая идентификация в микрофинансовых организациях (использование старых фото с отредактированным листом бумаги).

- Взаимодействие: Электронный документооборот налажен с 10 банками (по 5 в 2025 и 2026 гг.), включая Сбербанк, ВТБ, Альфа-Банк, МТС Банк, Совкомбанк. Однако есть проблемы с оперативностью ответов от удаленных банков и получения IP-адресов.

2.3. ПАО Сбербанк: банковский фрод-мониторинг

Спикеры: Цимбота Василий Иванович, начальник управления безопасности Западно-Сибирского отделения № 8647 ПАО Сбербанк; Лейс Виталий Александрович, заместитель управляющего отделением.

- Методы: система фрод-мониторинга в онлайн-режиме выявляет нехарактерную активность. В сложных случаях (когда клиент находится под влиянием мошенников) подключаются сотрудники отделений, руководители, служба безопасности и полиция. Процесс вывода человека из-под гипноза мошенников может занимать несколько дней.

- Инструменты: в приложении реализован сервис «Близкие рядом» (аналог «Второй руки»).

- Профилактика: Банк информирует клиентов о правилах безопасности, подчеркивая, что сотрудники никогда не спрашивают PIN-, CVV-коды и пароли из СМС. Внедрена блокировка подозрительных операций.

2.4. МТС: технологии оператора связи

Спикер: Михайлова Анастасия Михайловна, директор филиала МТС в Тюменской области.

- Метрики и технологии: Предотвращены десятки тысяч инцидентов, сохранены миллиарды рублей. В 2024-2025 гг. нейтрализованы звонки с подменой нумерации. Выявлено 5000 уникальных локаций СИМ-боксов (данные переданы в МВД). Заблокированы звонки с иностранных IP.
- Фрод-трафик: с начала 2026 года совершено более 179 млн фрод-вызовов с МН-нумерацией. Если до августа их доля составляла до 45%, то в сентябре-октябре (после принятых мер) упала до 10-15%.
- Речевая аналитика: МТС формирует базу «вокальных векторов» (акустических отпечатков) мошенников на основе подтвержденных инцидентов. Система в реальном времени сравнивает голос звонящего с базой и блокирует вызов.
- Сервис «Защитник»: Работает на уровне сети, блокирует спам и подозрительные звонки. Доступен абонентам всех операторов, им пользуются свыше 18 млн клиентов.
- Дополнительно: Бесплатный самозапрет на звонки с зарубежных номеров (с сентября 2025 г.), перехват подозрительных вызовов на бота, уведомление близких, страхование от мошенников.

2.5. ПАО «Ростелеком»: комплексная защита

Спикер: Манцурова Татьяна Владимировна, директор по работе с корпоративным и государственным сегментами филиала в Тюменской и Курганской областях ПАО «Ростелеком».

- Система «Сфера»: Базовые сервисы бесплатны для абонентов. Блокируют спам, защищают от подмены номера, блокируют до 95% переходов на фишинговые и вредоносные сайты. Реализована блокировка получения СМС-кодов во время разговора.
- Корпоративный сегмент: Отмечены атаки мошенников под видом сотрудников провайдера на юридические лица.
- Обучение: Внутренние лекции и тестирования сотрудников повысили уровень грамотности на 10 % за год. Компания готова делиться материалами и участвовать в обучении населения.

2.6. Общественный и образовательный сектор

Спикер: Загвязинская Ольга Анатольевна, советник ректора ТюмГУ, член Общественной палаты РФ, председатель Общественной палаты г. Тюмени, заслуженный юрист РФ.

- Опыт ТюмГУ: Системная работа с 2022 года. Разбор реальных уголовных дел (например, история студентки, взявшей кредит под давлением), деловые игры, имитирующие просьбы о помощи от «друзей».
- Масштаб и инфраструктура: Охват 25 500 студентов и 3 500 сотрудников. Рассылки через единый деканат и Яндекс Мессенджер. Работает круглосуточный оперативный дежурный в главном корпусе (24/7).
- Результаты: Обучено 72 лектора (выданы сертификаты). Более 150 обращений от студентов, к которым выходили мошенники (в том числе от имени проректоров). Официальных обращений от преподавателей с 2023 года не зафиксировано.

3. Ключевые выводы по итогам мероприятия

1. Смена парадигмы: Защита отдельных каналов (телефон, карта) неэффективна. Необходима защита всей цепочки взаимодействия человека с цифровой средой, включая психологическое давление (социальную инженерию).
2. Синергия государства и бизнеса: Технологические решения (блокировка СИМ-боксов, речевая аналитика, фрод-мониторинг) дают результат только в связке с законодательными мерами (база ЦБ, «период охлаждения») и оперативным обменом данными с МВД.

3. Уязвимость инфраструктуры: Проблема повторной выдачи SIM-карт и несовершенство удаленной идентификации в МФО остаются «слепыми зонами», требующими нормативного урегулирования.

4. Роль человеческого фактора: Главный щит — это цифровая и финансовая грамотность. Разовые лекции не работают; необходимы постоянные, адресные форматы (игры, разборы кейсов, круглосуточная помощь).

4. РЕКОМЕНДАЦИИ ДЛЯ ГРАЖДАН (ЖИТЕЛЕЙ ТЮМЕНСКОЙ ОБЛАСТИ)

На основе консолидированной позиции всех экспертов сформированы следующие правила цифровой безопасности:

Базовые правила (от Сбербанка и МТС):

- Сложные пароли: от 12 символов, уникальный для каждого сервиса.
- Антивирус: установить на все устройства и регулярно обновлять.
- Коды - табу: Сотрудники банков, полиции, Госуслуг и операторов никогда не спрашивают PIN-, CVV-коды и пароли из СМС.
- Никакого удаленного доступа: Если просят установить AnyDesk, TeamViewer или другое приложение «для защиты счета» — это мошенники. Немедленно прекращайте разговор.
- Отдельная карта: для покупок в интернете используйте дебетовую карту, не храните на ней основные сбережения.

Финансовая гигиена (от Банка России):

- Самозапрет: Установите самозапрет на кредиты через Госуслуги или МФЦ, чтобы мошенники не могли оформить займы.
- Период охлаждения: помните, что по закону у вас есть от 4 часов до 2 суток, чтобы отменить решение о кредите.
- Ограничения: если банк ограничил снятие наличных (до 50 тыс. руб. на 48 часов) - это защитная мера, не паникуйте.
- Проверка инвестиций: Проверяйте организации в официальных реестрах ЦБ РФ. На всех сторонних ресурсах указанная высокая гарантированная доходность организации может быть признаком мошенничества.
- Подключите в банке сервис «второй руки» - доверенное лицо Вас сможет подстраховать на случай совершения мошеннической операции.

Защита в телеком-среде (от МТС и Ростелекома):

- Зарубежные звонки: подключите бесплатный запрет на входящие звонки с зарубежных номеров, если вы не ожидаете их.
- Уведомление близких: Настройте услуги, позволяющие близким получать уведомления о подозрительных звонках на ваш номер.
- Фишинг: Не переходите по ссылкам из СМС и мессенджеров, блокируйте спам.

Что делать, если вы подверглись воздействию мошенников:

1. Немедленно завершите разговор.
2. Позвоните в банк по официальному номеру (с сайта или обратной стороны карты).
3. Заблокируйте карту и доступ к онлайн-банку.
4. Подайте заявление в банк (через приложение) и зарегистрируйте сообщение в полиции (через приложение банка можно сформировать справку для полиции).
5. Если вы подозреваете, что стали жертвой дропперов (передали карту), срочно обратитесь в банк и полицию.

Куда обращаться за помощью: Портал «Стоп, мошенники! 72»; Портал детской безопасности в сети Интернет (для родителей и педагогов); УМВД Росси по Тюменской бласти; Отделение банка; Контакт центр оператора связи

«СТОП! Проверь! Коды не диктуй - звони сам!

Соблюдай цифровую гигиену и помни: твоя безопасность - это личная ответственность. Пароль и деньги - только твои!»

ПРИЛОЖЕНИЕ 1

По результатам круглого стола можно выделить два блока: уже зафиксированные договорённости (в рамках встречи) и перспективные направления для коллабораций (предложения, которые требуют дальнейшей проработки).

1. Зафиксированные договорённости на будущее

Участники не подписывали юридически обязывающих соглашений, но достигли ряда организационных договорённостей:

1. Подготовка итогового документа:
   - Рабочая группа по инновациям, ИТ и цифровизации Общественной палаты Тюменской области обобщит все озвученные предложения и сформирует итоговый документ.
   - Документ будет разослан всем участникам для ознакомления.
2. Проведение совместного мероприятия для студентов:
   - Станислав Логинов (Департамент информатизации) предложил провести совместное мероприятие для студенческой аудитории с участием экспертов и правоохранительных органов.
   - Ольга Загвязинская (ТюмГУ/ОП) поддержала инициативу со стороны университетской площадки.
   - Статус: Договорённость о проведении достигнута, но место, дата и программа требуют согласования.

2. Возможные коллаборации и взаимные мероприятия в будущем

Круглый стол выявил высокий потенциал для межведомственных и межсекторных проектов. Эксперты обозначили следующие направления для сотрудничества:

А) Межведомственные и технологические коллаборации:

- Банки + Операторы связи + Минцифры + Банк России: Проработка механизма уведомления об изменении статуса телефонных номеров (повторная продажа SIM-карт). Вадим Попков (УМВД) предложил инициативу, Анастасия Михайловна (МТС) поддержала её к дальнейшей проработке.

- УМВД + Банки: Ускорение электронного документооборота и обмена данными. Обсуждалось улучшение получения технических данных (например, IP-адресов) и внедрение срочных ограничительных действий по запросу полиции.

- Банк России + Операторы связи: Совместное развитие и участие в разработке законодательных инициатив («Антифрод 2.0» и «Антифрод 3.0»), включая объединение банковских и операторских сигналов риска.

Б) Образовательные и просветительские коллаборации:

- Банк России + Общественная палата + Вузы: Ольга Патрактинова предложила использовать результаты Всероссийского онлайн-зачёта по финансовой грамотности (диагностика знаний) для определения тем и проведения адресных занятий. ОП может выступить площадкой для продвижения.

- Ростелеком + Регион: Татьяна Мансурова заявила о готовности компании использовать свой опыт внутренних лекций и тестирований для внешнего обучения населения.

- ТюмГУ + Департамент информатизации + УМВД: Тиражирование успешной университетской практики (деловые игры, разбор реальных дел, круглосуточные дежурные) на другие учебные заведения региона.

В) Профилактика среди молодёжи (дропперство):

- УМВД + Вузы/Колледжи: Вадим Попков предложил усилить профилактику в учебных заведениях, объясняя подросткам правовые последствия передачи банковских карт. ТюмГУ уже имеет опыт таких встреч (72 подготовленных лектора).

Г) Внешние экспертные площадки:

- Форум «ИНФОТЕХ» и «Сибирские правовые чтения»: Участники договорились продолжить обсуждение на этих площадках. Вадим Попков сообщил о подаче заявки на

участие в «ИНФОТЕХе» в качестве спикера для обсуждения использования ИИ мошенниками.

Резюме

Итог встречи - использование действующей площадки для диалога в дальнейшем. Наиболее реалистичные и близкие к запуску коллаборации - студенческое мероприятие (уже поддержано) и интеграция финансового зачёта в обучение (предложено Банком России). Наиболее сложные, но критически важные для безопасности - технические регламенты обмена данными между операторами, банками и полицией.

Отчёт подготовлен рабочей группой по инновациям, информационным технологиям