



**УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
по ВЫБОРГСКОМУ РАЙОНУ ЛЕНИНГРАДСКОЙ ОБЛАСТИ
(УМВД России по Выборгскому району ЛО)**

ВЫБОРГСКАЯ ГОРОДСКАЯ ПРОКУРАТУРА

**ОСНОВНЫЕ ВИДЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА И
РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ О ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ**

Информационно-профилактический сборник

г. Выборг

2026 год

Подготовлено совместно:

- УМВД России по Выборгскому району Ленинградской области
- Выборгской городской прокуратурой

Сборник предназначен для:

- для граждан всех возрастных категорий
- работников организаций
- образовательных учреждений
- органов местного самоуправления

Цель издания: повышение правовой грамотности населения и предупреждение преступлений, совершаемых с использованием средств связи и информационно-телекоммуникационных технологий.

СОДЕРЖАНИЕ

1. Введение
2. Основные схемы мошенничества
3. Признаки мошеннических действий
4. Правила защиты граждан
5. Алгоритм действий при совершении мошенничества
6. Полезные контакты
7. Заключение
8. Приложения

1. Введение

Телефонные и интернет-мошенничества остаются одними из наиболее распространенных способов хищения денежных средств. Злоумышленники используют психологическое давление, подмену номеров, современные технологии и методы социальной инженерии, чтобы заставить граждан самостоятельно перевести деньги или сообщить конфиденциальные данные.

Главное правило безопасности: **ни сотрудники банков, ни правоохранительные органы, ни государственные органы никогда не требуют переводить деньги на «безопасные счета» и не запрашивают коды из SMS.**

2. Основные схемы мошенничества

2.1. «Сотрудник банка» или «службы безопасности»

Мошенники представляются сотрудниками Сбербанка России, Банк ВТБ, Т-Банк или других банков и сообщают:

- о подозрительной операции по счету;
- попытке оформления кредита;
- необходимости срочно перевести деньги на «безопасный счет»;
- необходимости сообщить код подтверждения.

Как действовать:

- немедленно прекратите разговор;
- не сообщайте реквизиты карты, CVV-код, PIN-код и SMS-коды.
- самостоятельно позвоните в банк по номеру, указанному на карте или официальном сайте.

2.2. «Сотрудник полиции, ФСБ, прокуратуры или Центрального банка»

Злоумышленники представляются сотрудниками Федеральной службы безопасности Российской Федерации, Банка России, МВД или прокуратуры и утверждают, что:

- ваши счета используются в преступной схеме;
- проводится «секретная операция»;
- необходимо сохранить конфиденциальность;
- нужно перевести деньги или оформить кредит.

Как действовать:

- помните: государственные органы не требуют финансовых операций по телефону;
- не поддавайтесь давлению и угрозам;
- при необходимости самостоятельно обратитесь в ближайший отдел полиции или прокуратуру.

2.3. «Ваш родственник попал в беду»

Мошенники сообщают, что близкий человек стал виновником ДТП, задержан или находится в больнице, и требуют срочно передать деньги.

Как действовать:

- сохраняйте спокойствие;
- свяжитесь с родственником лично;
- уточните информацию у других членов семьи;
- не передавайте деньги незнакомым лицам.

2.4. «Продление договора связи» или «замена SIM-карты»

Злоумышленники представляются сотрудниками МТС, МегаФон, Билайн или Теле2 и просят назвать код из SMS.

Как действовать:

- не сообщайте коды подтверждения.
- уточняйте информацию только через официальный кабинет или по номеру оператора.

2.5. «Портал Госуслуг»

Мошенники сообщают о взломе учетной записи в Единый портал государственных и муниципальных услуг и требуют сообщить код подтверждения.

Как действовать:

- не передавайте логины, пароли и SMS-коды;
- проверяйте уведомления только через официальный сайт или приложение;
- используйте двухфакторную аутентификацию.

2.6. «Инвестиции и быстрый заработок»

Под видом сотрудников инвестиционных компаний предлагают вложить деньги в акции, криптовалюту или «гарантированные проекты».

Как действовать:

- проверяйте наличие лицензии у Банк России;
- не переводите деньги незнакомым людям;
- оценивайте риски и избегайте обещаний «гарантированного дохода».

2.7. «Покупка или продажа товаров в Интернете»

При сделках на сайтах объявлений мошенники направляют поддельные ссылки для оплаты или получения средств.

Как действовать:

- используйте только официальные сервисы площадок;
- не вводите данные карты на подозрительных площадках;
- проверяйте адрес сайта и наличие защищенного соединения.

3. Признаки мошеннических действий

- требование срочно принять решение;
- запугивание уголовной ответственностью;
- указание сохранять разговор в тайне;
- просьба назвать код из SMS;
- требование оформить кредит или перевести деньги;
- использование слов «безопасный счет», «специальная операция», «финансовая защита»;
- звонок с неизвестного номера или через мессенджеры.

4. Правила защиты граждан

1. Никому не сообщайте:

- PIN-код;
- CVV/CVC-код;
- пароли;
- коды из SMS;
- данные паспорта без необходимости.

2. Не переводите деньги по указанию незнакомых лиц.
3. Не устанавливайте программы удаленного доступа.
4. Проверяйте информацию самостоятельно.
5. предупредите пожилых родственников и детей.
6. Используйте антивирусное программное обеспечение.
7. Подключите уведомления по банковским операциям.

5. Алгоритм действий при совершении мошенничества

1. Немедленно заблокируйте банковские карты и счета.
2. Обратитесь в банк с заявлением о спорной операции.
3. Измените пароли от важных сервисов.
4. Подайте заявление в полицию.
5. Сохраните переписку, записи разговоров, номера телефонов и чеки.

6. Полезные контакты

- Единый номер экстренных служб - 112;
- Дежурная часть УМВД России 8(81378)3-03-07
- приемная Выборгской городской прокуратуры 8(81378)2-47-34
- служба поддержки вашего банка.

7. Заключение

Будьте внимательны и осторожны. Не передавайте свои персональные данные и денежные средства неизвестным лицам. При возникновении сомнений незамедлительно прекращайте разговор и обращайтесь в официальные органы.