МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по профилактике мошенничества в отношении граждан под предлогом выплат, наград и иных «льгот» в связи с участием родственников в СВО

Практическое пособие для населения

Цель рекомендаций — помочь гражданам распознавать типичные мошеннические схемы, связанные с сообщениями о государственном награждении, выплатах, поиске пропавших, компенсациях, «безопасных счетах» и иных вопросах, затрагивающих родственников военнослужащих.

Ключевой принцип: любые требования срочно перевести деньги, оплатить «госпошлину», «доставку награды», «комиссию», «страхование», «проверку данных» или сообщить коды из СМС являются высоковероятным признаком мошенничества.

2026 г.

1. Актуальность проблемы

Мошенники используют темы, которые вызывают у людей сильные эмоции: здоровье и безопасность близких, участие родственников в боевых действиях, вопросы статуса военнослужащего, положенных выплат, компенсаций и наград. Особую опасность представляют звонки и сообщения, в которых злоумышленники заявляют, что сын, муж, брат или иной родственник «представлен к награде», «включен в список на выплату», «нуждается в срочном подтверждении данных» либо «может быть найден или освобожден только после оплаты услуг».

Расчет строится на шоке, тревоге и дефиците времени. Человеку внушают, что решение необходимо принять немедленно: заплатить за изготовление удостоверения, доставку награды, госпошлину, перевод документов, связь с «куратором», розыск, адвоката, медицинскую транспортировку, разблокировку счета или «защиту» денежных средств. В действительности такие требования не соответствуют нормальному порядку взаимодействия государственных органов и кредитных организаций.

Официальные разъяснения указывают, что злоумышленники используют легенды о «безопасном счете», звонки якобы от силовых ведомств, рассылку вредоносных файлов, а также попытки получить персональные и банковские данные. МВД рекомендует руководствоваться принципом «никому не доверяй без проверки», а информацию перепроверять по официальным каналам.

2. Наиболее распространенные схемы обмана

2.1. «Ваш родственник представлен к государственной награде, положена военная пенсия или ее индексация»

Мошенник сообщает, что родственник награжден или представлен к награде, после чего требует оплатить «оформление», «изготовление документов», «доставку», «госпошлину», «услуги курьера», «архивную справку», «перевод средств для получения выплаты вместе с наградой».

Дополнительно могут просить фото паспорта, СНИЛС, банковской карты, реквизиты счета, коды из СМС. Иногда представляются сотрудниками военкомата, части, министерства, администрации, банка или «специальной комиссии»,

2.2. «Положена компенсация, субсидия, единовременная выплата», «получение денежной выплаты взамен получения земельного участка»

Жертве обещают крупную выплату в связи с участием родственника в СВО либо «помощь в оформлении документов для получения выплаты», ранением, статусом без вести пропавшего, гибелью, награждением, обучением детей, оплатой ЖКУ, также жертве сообщают, что рядом с местами где выделяют земельные участки находятся кладбища и химические заводы (земельные участки токсичны) т.п. Для получения денег предлагают внести «небольшой предварительный платеж» или подтвердить личность кодом из СМС.

Цель преступников — похитить деньги сразу либо получить доступ к онлайн-банку и порталу государственных услуг, а также убедить перевести денежные средства на безопасный счет.

2.3. «Срочный поиск, освобождение, лечение или транспортировка»

Родственникам, потерявшим связь с военнослужащим, предлагают за деньги «ускорить розыск», «помочь с обменом», «найти в госпитале», «подтвердить пребывание в плену», «оформить ДНК», «помощь в получении геномной экспертизы», «получить список раненых»

Официальные ресурсы прямо предупреждают: не следует реагировать на платные предложения по поиску и не нужно передавать таким лицам персональные данные бойца и членов семьи.

2.4. «Откройте файл со списком, фото, приложением Красного Креста»

Мошенники присылают файлы или ссылки с названиями вроде «список военнопленных», «приложение Красного Креста», «фотоальбомы пленных», предлагая срочно скачать материал. Подобные файлы могут содержать вредоносное программное обеспечение, предназначенное для кражи данных и доступа к банковским приложениям.

2.5. «Мы из банка / полиции / Росфинмониторинга / оператора связи»

В рамках комбинированной схемы человеку говорят, что на его имя оформляют кредит, счет взломан, нужно срочно перевести средства на «безопасный счет», подтвердить личность или установить программу «защиты». Иногда несколько мошенников звонят по очереди, изображая банк, силовое ведомство и техническую поддержку.

3. Признаки, по которым можно распознать мошенников

Ниже приведены основные «красные флаги». Наличие даже одного из них требует немедленно прекратить разговор и начать проверку информации.

Признак	Почему это опасно
Требование срочно перевести деньги	Государственные органы не получают «предварительные платежи» на личные карты и не решают вопрос награждения или выплаты через анонимные переводы.
Просьба сообщить код из СМС	Код подтверждения нужен для входа в сервисы, смены пароля или совершения операции. Передача кода = передача контроля над учетной записью.
Давление и запугивание	Мошенник стремится лишить человека времени на проверку: «срочно», «иначе все отменят», «никому не говорите», «это секретная информация».
Звонок с неизвестного номера или в мессенджере	Подмена номера и контактов широко используется; внешний вид звонка не подтверждает полномочия собеседника.
Просьба установить приложение или открыть файл	Это может дать злоумышленнику удаленный доступ к телефону и банковскому

Признак	Почему это опасно
	приложению.
Просьба прислать фото документов, карт, захоронений, удостоверений	Собранные сведения используют для дальнейшего обмана, шантажа, кражи учетных записей и оформления фиктивных заявлений.

4. Алгоритм действий при подозрительном звонке или сообщении

- Сохраняйте спокойствие. Не принимайте решений под давлением и не вступайте в длинную дискуссию.
- Не сообщайте никаких персональных данных: паспорт, СНИЛС, ИНН, номера карт, CVV/CVC, коды из СМС, логины и пароли.
- Не переводите деньги ни на какие счета, карты и номера телефонов, даже если их называют «служебными», «депозитными», «страховыми» или «безопасными».
- Не открывайте ссылки и файлы из сообщений, не устанавливайте приложения по указанию звонящего.
- Прекратите разговор. Самостоятельно свяжитесь с организацией по официальному номеру, указанному на официальном сайте или документе.
- Проверьте сведения о родственнике только по официальным каналам: через военный комиссариат, Военно-социальный центр Минобороны России, региональный филиал фонда «Защитники Отечества», официальный сайт Минобороны России.
- Сообщите о попытке обмана близким, особенно пожилым родственникам, чтобы предупредить повторные звонки от той же группы мошенников.

> ВАЖНО: если собеседник говорит: «Оплатите доставку награды за сына», «внесите пошлину за удостоверение», «переведите сумму за получение выплаты», — это необходимо воспринимать как мошеннический предлог до тех пор, пока информация не подтверждена через официальный орган по официальному каналу связи.
>
> Правильная реакция: завершить разговор, не спорить, не оправдываться, не объяснять свое финансовое положение, не продолжать переписку.

5. Действия, если гражданин уже сообщил данные или перевел деньги

- Немедленно позвонить в банк по номеру, указанному на банковской карте или официальном сайте, сообщить о мошенничестве и потребовать заблокировать карту, операции и при необходимости доступ к дистанционному банковскому обслуживанию.
- Сменить пароли от мобильного банка, электронной почты, портала госуслуг, мессенджеров и иных важных сервисов.
- Проверить телефон на наличие неизвестных приложений. При подозрении на удаленный доступ отключить интернет, удалить подозрительные программы, при необходимости выполнить сброс устройства и повторную настройку.
- Сохранить доказательства: номера телефонов, скриншоты переписки, ссылки, квитанции, время звонков, реквизиты переводов, голосовые сообщения.

- Подать заявление в полицию и приложить все имеющиеся материалы. Чем быстрее направлена информация в банк и правоохранительные органы, тем выше шанс остановить либо оспорить операцию.

6. Куда обращаться для проверки сведений и получения помощи

При отсутствии связи с военнослужащим или при получении сомнительной информации следует использовать только официальные каналы. По данным государственного ресурса «Объясняем.рф», уточнить статус военнослужащего можно через военкомат; также родственникам рекомендовано обращаться в Военно-социальный центр Минобороны России, региональные филиалы фонда «Защитники Отечества», а электронное обращение подавать через официальный сайт Минобороны России в «Личном кабинете гражданина». Платные посредники, обещающие «ускорить» поиск, являются зоной повышенного риска.

Куда обращаться	По какому вопросу	Рекомендуемое действие
Банк	Если сообщены реквизиты карты, код из СМС, выполнен перевод	Позвонить самостоятельно по официальному номеру, попросить срочную блокировку и зарегистрировать обращение.
Полиция / экстренные службы	Мошенничество, угрозы, шантаж, попытка хищения	Подать заявление, приложить скриншоты и реквизиты перевода.
Военкомат	Проверка статуса военнослужащего, отсутствие связи	Обращаться лично или по официальным контактам, не через посредников.
Военно-социальный центр Минобороны России	Официальные консультации для родственников военнослужащих	Использовать официальный контактный канал.
Фонд «Защитники Отечества»	Сопровождение и помощь семьям военнослужащих и ветеранам	Обращаться в региональный филиал самостоятельно.
Официальный сайт Минобороны России	Электронное обращение, проверка официальной информации	Не переходить по ссылкам из чатов; заходить вручную по официальному адресу.

7. Типовые сценарии и правильная модель поведения

Сценарий 1. «Награда уже оформлена, нужно оплатить доставку»

Правильное действие: не переводить деньги и не уточнять, сколько именно нужно заплатить. Достаточно сказать, что информация будет проверена лично через официальный орган, после чего прекратить разговор. Далее необходимо самостоятельно связаться с военкоматом или иным официальным учреждением.

Сценарий 2. «Сын ранен, срочно нужны деньги на перевозку или лекарство»

Правильное действие: завершить разговор, не поддаваться эмоциональному шантажу, связаться с родственниками и официальными медицинскими либо военными каналами. Нельзя переводить деньги на карту неизвестного физического лица.

Сценарий 3. «Есть список пленных/раненых, скачайте файл»

Правильное действие: не открывать вложение и не переходить по ссылке. Нужно удалить сообщение, заблокировать отправителя и сообщить о рассылке близким, чтобы они также не открывали файл.

Сценарий 4. «Ваши деньги нужно перевести на безопасный счет, чтобы сохранить выплату»

Правильное действие: немедленно прекратить разговор. Самостоятельно позвонить в банк по номеру на карте. Любые переводы на «безопасный счет» следует рассматривать как мошенническую схему.

Сценарий 5. «Никому не говорите, это служебная информация»

Правильное действие: считать такую фразу дополнительным признаком мошенничества. Законные организации не запрещают гражданину советоваться с близкими и перепроверять сведения по официальным каналам.

8. Рекомендации для профилактической работы с населением

При информировании граждан необходимо использовать простые и запоминающиеся формулы поведения: «не переводи», «не сообщай код», «не открывай файл», «проверь сам», «клади трубку».

Особое внимание следует уделять пожилым людям, семьям военнослужащих, а также гражданам, которые уже испытывают стресс из-за отсутствия связи с родственником.

Профилактические материалы рекомендуется размещать в МФЦ, администрациях, медицинских организациях, образовательных учреждениях, отделениях почты, банках, военкоматах, филиалах фонда «Защитники Отечества», а также распространять через управляющие компании, родительские чаты и общественные приемные.

При проведении бесед целесообразно разбирать не только общие правила безопасности, но и конкретные легенды мошенников: «госнаграда за сына», «срочная выплата», «безопасный счет», «список пленных», «поиск без вести», «компенсация детям», «помощь с лечением».

Рекомендуется использовать карточки-вопросы: «Кто звонит?», «С какого официального номера?», «Почему вы просите деньги?», «Почему вопрос нельзя решить лично?», «Почему нужно сообщить код из СМС?». Эти простые вопросы помогают человеку выйти из эмоционального давления и вернуться к рациональной оценке ситуации.

9. Форма первичной фиксации инцидента

При обращении в банк, полицию или иную организацию гражданину полезно заранее зафиксировать минимальный набор сведений о событии:

Что зафиксировать	Пример сведений
Дата и время контакта	24.02.2026, 14:35
Способ связи	Телефонный звонок / WhatsApp / Telegram / СМС
Номер или имя аккаунта	+7…, имя профиля, ссылка на чат
Содержание легенды	«Нужно оплатить доставку награды за сына»
Какие данные просили	Паспорт, номер карты, код из СМС, фото документов
Какие действия уже совершены	Переведен 1 платеж / отправлен скриншот / разговор прекращен
Имеющиеся доказательства	Скриншоты, аудио, квитанции, реквизиты получателя

10. Памятка гражданину: краткий чек-лист

Нужно сделать	Нельзя делать
• Перепроверить информацию через официальный номер или личное обращение.	• Платить за «получение награды», «доставку» или «госпошлину».
• Сохранить номер звонившего и переписку.	• Сообщать код из СМС, реквизиты карты и пароли.
• Предупредить родственников о попытке обмана.	• Устанавливать приложения из чатов и мессенджеров.
• При переводе денег срочно связаться с банком и полицией.	• Отправлять фото документов, карт, удостоверений и захоронений.
• Использовать только официальные сайты и каналы связи.	• Верить словам «не кладите трубку, иначе все аннулируется».

11. Пример речевой формулы отказа мошеннику

Для граждан полезно заранее отработать нейтральную и короткую фразу, после которой разговор немедленно прекращается:

> *«Я не обсуждаю такие вопросы по телефону. Информацию проверю самостоятельно через официальный орган. Денег не перевожу, коды не сообщаю. До свидания.»*

12. Заключение

Наиболее эффективная защита от таких преступлений — сочетание личной осторожности, проверки информации по официальным каналам и немедленного прекращения подозрительного контакта. Вопросы, связанные с военнослужащими, выплатами, наградами и поиском пропавших, должны решаться только через уполномоченные органы и официальные сервисы.

Любая просьба предварительно оплатить получение награды или выплаты, сообщить код подтверждения, установить приложение, перейти по ссылке или передать персональные данные должна восприниматься как возможное мошенничество. Для профилактики важно регулярно доводить эту информацию до семей военнослужащих, пожилых граждан и иных лиц, находящихся в эмоционально уязвимом состоянии.

Приложение. Рекомендуемые источники для проверки информации

1. Объясняем.рф. Телефонные мошенники: куда жаловаться. Памятка о схемах телефонного мошенничества и правилах безопасного поведения.

2. Объясняем.рф. Что делать, если военнослужащий долго не выходит на связь? Материал с перечнем официальных каналов для родственников.

3. Объясняем.рф. Как мошенники обманывают родственников бойцов СВО? Материал о фальшивых чатах, опасных файлах и сборе персональных данных.

4. Объясняем.рф. Россиянам объяснили, как защититься от мошенников. Публикация с рекомендациями МВД РФ.

5. Финансовая культура (Банк России). Аферисты начали красть деньги военнослужащих. Материал о легенде «безопасного счета» и рисках потери средств.

Дополнительные разъяснения для граждан

1. Сам факт того, что собеседник знает фамилию, имя, отчество родственника, номер части, место жительства или иные подробности, не подтверждает его полномочия. Эти сведения могли быть получены из открытых источников, утечки данных, социальных сетей или предыдущих телефонных разговоров.

2. Государственные и муниципальные органы, банки и официальные фонды не требуют переводить деньги на карты физических лиц для решения вопроса о награде, выплате, подтверждении статуса, лечении или поиске человека. Любое подобное предложение должно восприниматься как крайне подозрительное.

3. Даже если звонящий ведет себя уверенно, использует профессиональные термины, называет должности и ведомства, это не является доказательством его отношения к официальной структуре. Мошенники часто заранее готовят сценарий разговора и используют психологические приемы давления.

4. Для семей военнослужащих полезно заранее договориться о простом семейном кодовом слове или контрольном вопросе. Такой прием особенно важен в условиях распространения поддельных голосовых сообщений и попыток имитации речи знакомого человека.

5. Необходимо регулярно обсуждать тему телефонного мошенничества с пожилыми родственниками. Лучше заранее проговорить правило: при любых тревожных новостях о близком

человеке сначала кладем трубку, затем перезваниваем сами по известному официальному номеру или связываемся с родственниками по проверенному каналу.