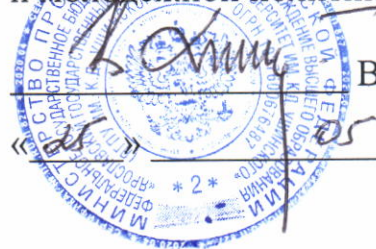


**Министерство просвещения Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования «Ярославский государственный
педагогический университет им. К.Д. Ушинского»**

Утверждаю
проректор по воспитательной работе
и молодежной политике



В.П. Завойстый

2026 г.

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ
ОБЩЕНИЮ ПО ТЕЛЕФОНУ И В СЕТИ ИНТЕРНЕТ**

**Ярославль
2026**

Введение

В современном обществе интернет и цифровые технологии проникли практически во все сферы нашей деятельности. Мы не только совершаем банковские операции и отслеживаем покупки в режиме онлайн, но и обмениваемся важными документами через облачные хранилища, храним личные фотографии на дистанционных серверах и даже используем мобильные приложения для контроля за здоровьем и физической активностью. Всё это кажется удобным и безопасным, однако именно повсеместность интернета может обернуться уязвимостями, о которых многие не задумываются. Современные мессенджеры и социальные сети стали аналогами «цифровых улиц» и «площадей», где мы проводим значительную часть времени, не всегда осознавая, что подобная открытость может привлечь злоумышленников.

Растущая популярность онлайн-игр, дистанционного обучения и телемедицины делает интернет ещё более универсальным пространством, без которого практически невозможно представить сегодняшнюю жизнь. В результате многие начинают относиться к цифровой среде как к чему-то обыденному и перестают внимательно следить за безопасностью собственных данных. Некоторые люди уверены, что преступники интересуются в основном крупными корпорациями, а обычным пользователям бояться нечего. На практике же жертвами фишинга, социальной инженерии или вымогательств становятся самые разные категории людей. Статистика мошенничеств подтверждает, что возраст, уровень образования и социальный статус не гарантируют иммунитета от рискованных ситуаций.

В такой обстановке особенно важно понимать, какие именно угрозы могут возникнуть при повседневной работе в интернете. Можно иметь неплохие технические навыки, но при этом не замечать скрытых уловок мошенников, которые используют психологическое давление или обман доверия. Задача методических рекомендаций по безопасному общению по телефону и в сети интернет – помочь осознать реальные риски, научиться распознавать угрозы и защитить себя и свою семью от потенциальных преступных действий.

Сегодня особую актуальность тема цифровой безопасности приобрела в связи с проведением специальной военной операции (далее – СВО) и развернувшейся вокруг неё масштабной информационной войны. Цифровая среда превратилась в один из важнейших фронтов этого противостояния. Мошенники и преступные группы активно используют технологии социальной инженерии, фишинга и иных видов цифровых угроз, целенаправленно атакуя российских граждан, чтобы сеять панику, дестабилизировать общественное настроение и наносить прямой финансовый ущерб.

Одним из ключевых инструментов информационной войны стали колл-центры, расположенные на территории Украины, сотрудники которых ежедневно осуществляют тысячи мошеннических звонков и рассылок.

Под видом сотрудников банков, госучреждений или правоохранительных органов преступники пытаются получить доступ к личным данным, банковским счетам и аккаунтам россиян. Особенно опасно, что в эти преступные схемы стали массово вовлекаться несовершеннолетние, чья юридическая безграмотность и доверчивость делают их лёгкой мишенью для манипуляций со стороны мошенников.

В условиях СВО подобные схемы приобретают не только финансовый, но и политический характер. Активно используются методы психологического воздействия и дезинформации, направленные на формирование у граждан России тревоги и недоверия к государственным структурам, банкам и друг другу. Особенно уязвимыми оказываются пользователи социальных сетей и мессенджеров, через которые мошенники массово распространяют фейковые сообщения, слухи и вредоносные ссылки.

Именно поэтому сегодня необходимо не только повысить личную осведомлённость о цифровой безопасности, но и осознать её как элемент общей гражданской ответственности. Каждый пользователь, защитив себя и близких от угроз в цифровой среде, вносит вклад в обеспечение информационной безопасности страны. Государственные органы и образовательные учреждения уже ведут активную работу в этом направлении, но только совместными усилиями всего общества можно эффективно противостоять цифровым угрозам в условиях информационной войны.

Личная цифровая безопасность: ключевые понятия

Важным понятием, с которого стоит начать, является **цифровая грамотность**. Многие считают, что это просто умение использовать технические устройства, отправлять сообщения или управлять банковским приложением на смартфоне. Однако цифровая грамотность гораздо шире. Она включает в себя способность пользоваться современными технологиями и глубоко понимать их принципы работы, критически оценивать поступающую информацию, а также постоянно заботиться о защите своих личных данных от возможных угроз. Это умение не только своевременно обновлять программное обеспечение и правильно настраивать гаджеты, но и вовремя распознавать опасности, возникающие в цифровой среде. Грамотный пользователь регулярно расширяет и обновляет свои знания, чтобы эффективно реагировать на стремительные изменения в мире информационных технологий.

Другим ключевым понятием является **социальная инженерия**. Под этим термином подразумевается набор психологических приёмов, с помощью которых мошенники пытаются повлиять на поведение людей. В отличие от технических методов взлома, социальная инженерия направлена на то, чтобы жертва добровольно раскрыла конфиденциальную информацию или совершила действие, необходимое злоумышленникам. Типичный пример – ситуация, когда человек, испугавшись потерять деньги, сообщает

мошенникам свои банковские данные, считая, что помогает «службе безопасности банка» предотвратить кражу. Часто преступники могут использовать чувство жалости, доверия или даже желание помочь, представляясь сотрудниками благотворительных фондов или друзьями, попавшими в беду. К сожалению, даже технически подкованные люди иногда становятся жертвами социальной инженерии, поскольку эмоциональное давление оказывает сильное воздействие и снижает бдительность.

Одной из наиболее распространённых угроз в цифровом пространстве является **фишинг**. Злоумышленники активно создают поддельные сайты, которые внешне практически не отличаются от официальных страниц банков, государственных порталов (таких как Госуслуги) или популярных социальных сетей. Затем мошенники рассылают ссылки на эти ресурсы через электронную почту, SMS-сообщения или мессенджеры, заманивая пользователей различными предложениями: «проверка данных», «подтверждение транзакции» или «срочная авторизация». Особенно опасны ситуации, когда преступники размещают такие ссылки в рекламных объявлениях поисковых систем. Пользователь, ничего не подозревая, переходит по ссылке, вводит личные данные, логины и пароли, после чего информация попадает в руки злоумышленников и используется в преступных целях.

Кроме того, серьёзной опасностью являются **угрозы в социальных сетях и мессенджерах**. Достаточно распространённая схема – взлом аккаунта с целью отправки сообщений от имени настоящего владельца страницы. В таких сообщениях мошенник может просить ваших друзей о срочной финансовой помощи, ссылаясь на экстренную ситуацию или временные финансовые трудности. Также от взломанного аккаунта часто рассылаются ссылки на вредоносные сайты или приглашения в сомнительные «закрытые сообщества». Подобные взломы чаще всего происходят из-за использования простых или повторяющихся паролей, а также при входе в соцсети с небезопасных устройств и общедоступных сетей Wi-Fi.

Ещё один вид угроз связан с **финансовыми операциями**. Многие люди становятся жертвами мошенников, соглашаясь на такие схемы, как «аренда» банковских карт, передача своих SIM-карт третьим лицам, или предоставление электронных кошельков для проведения сомнительных транзакций. Подобные предложения часто звучат очень заманчиво, особенно если человек испытывает финансовые трудности или просто хочет получить дополнительный доход. Однако на практике такие действия всегда несут юридические риски, поскольку банковские карты или SIM-карты затем используются в незаконных схемах по отмыванию денег или мошеннических переводах. Владелец реквизитов зачастую становится первым, к кому приходят сотрудники правоохранительных органов.

Особое внимание стоит уделить понятию двухфакторной аутентификации (2FA). Этот способ защиты аккаунтов становится всё более важным в условиях постоянного роста угроз информационной безопасности. Если раньше для доступа к учётной записи было достаточно лишь одного пароля, то сейчас этого уже недостаточно. Двухфакторная аутентификация

предполагает подтверждение личности пользователя двумя независимыми способами: первым является пароль, а вторым – дополнительный код, полученный через SMS-сообщение, приложение-генератор кодов или даже с помощью физического аппаратного ключа. Такой подход значительно усложняет работу злоумышленников, ведь для успешного взлома им необходимо получить доступ сразу к нескольким устройствам или сервисам, что практически невозможно без непосредственного участия владельца аккаунта.

Понимание этих угроз и механизмов, с помощью которых мошенники пытаются манипулировать жертвами, является обязательным для всех пользователей цифровых сервисов. Именно осознанность и знание основных схем мошенничества помогают значительно снизить риски и защитить себя от серьёзных неприятностей.

Социальная инженерия: как мошенники используют психологические приёмы

Многие думают, что их трудно обмануть, но мошенники часто пользуются эмоциональными «крючками»:

- Давление: «Если вы не сообщите код из SMS, счёт будет заблокирован», «Не передадите доступ – потеряете все деньги». Задача преступника – вывести вас из состояния спокойствия, чтобы вы приняли поспешное решение.

- Вызывание жалости или доверия: «Мы волонтеры, собираем на срочную операцию», «Я ваш коллега, срочно помогите со служебным доступом». Часто используется сочувствие к больным детям или доверие к «официальным лицам». Люди, которые изначально добры и отзывчивы, могут отреагировать на подобные призывы, не перепроверяя факты.

- Лесть и обещание выгоды: «Вы выиграли приз, подтвердите, введя данные карты», «Участвуйте в инвест-проекте, гарантированная доходность 100%». Здесь делают ставку на жадность или самолюбие. Желание получить большой куш или почувствовать себя «избранным» становится причиной неосторожных действий.

Даже опытные пользователи могут попасть в ловушку, когда под эмоциями теряют критическое мышление. Основная рекомендация: если вам предлагают что-то срочно, ссылаясь на угрозу или уникальный шанс, всегда проверяйте информацию.

Многие считают, что «в интернете никто не узнает», если они предоставят доступ к своим аккаунтам или выступят посредниками в переводах. Появляется ложное убеждение о безнаказанности, особенно если речь идёт о незнакомых людях в мессенджерах или о сделках с псевдонимами. Некоторые пользователи верят, что раз общаются под ником, их личность остаётся в тени. Однако правоохранительные органы обладают достаточными техническими средствами, чтобы вычислить истинного владельца платёжного счёта или сим-карты.

Опытные пользователи нередко забывают, что их действия в сети оставляют цифровой след: IP-адреса, лог-файлы, привязки к определённым устройствам. Мошенники могут воспользоваться вашей иллюзией анонимности, убеждая, что «никто ничего не узнает». На практике выясняется, что по цепочке переводов легко выйти на человека, который предоставил свою карту или аккаунт. Незнание закона не освобождает от ответственности, и это ключевой момент, который многие упускают.

Современные мошеннические схемы становятся всё более изощрёнными и разнообразными. Наиболее распространённым способом похищения личных данных остаётся фишинг. Часто пользователи получают поддельные письма якобы от официальных учреждений, банков или популярных сервисов. Такие письма, несмотря на внешнюю правдоподобность и использование официальных логотипов, при внимательном изучении обнаруживают подозрительный адрес отправителя или ошибки в тексте. Пользователь, доверившись, переходит по ссылке и вводит свои данные на фальшивом сайте, который внешне почти не отличается от настоящего. Преступники идут на хитрость, заменяя символы в адресе сайта (например, латинскую букву «l» на цифру «1»). Аналогичные схемы действуют и в виде SMS-или сообщений через мессенджеры. Например, мошенник присылает тревожное сообщение о том, что банковская карта якобы заблокирована, после чего пользователь, испугавшись, передаёт конфиденциальную информацию злоумышленникам.

Одновременно с этим набирает популярность такой вид мошенничества, как дропперство. Дропперами называют людей, которые предоставляют свои платёжные инструменты (банковские карты, SIM-карты, электронные или криптовалютные кошельки) третьим лицам для совершения сомнительных операций. Часто людей привлекает возможность получить «лёгкие деньги»: за небольшое вознаграждение им предлагают «всего лишь предоставить» свои реквизиты или аккаунты. Подобные действия трактуются законом как участие в преступлении, а точнее – пособничество. Банки и правоохранительные органы легко отслеживают цепочки переводов и транзакций, поэтому даже незначительное участие в подобных схемах может привести к серьёзным последствиям, вплоть до реального уголовного наказания.

Важно понимать, что мошенники практически всегда используют дропперов, чтобы сохранить свою анонимность. В итоге реальным исполнителем, на чьё имя зарегистрированы все операции, становится тот, кто согласился передать свои данные. Такая ситуация ставит человека в положение виновного, и доказать свою невиновность или незнание обстоятельств бывает крайне сложно.

Новые законодательные инициативы стремятся ужесточить ответственность за передачу личных платёжных данных и реквизитов третьим лицам. В частности, внесены изменения в статью 187 Уголовного Кодекса Российской Федерации (УК РФ) («Неправомерный оборот средств платежа»), что делает наказание за подобные действия более жёстким. В перспективе даже единичная передача карты, аккаунта или SIM-карты для мошеннических

целей может обернуться крупным штрафом и даже тюремным заключением. Государство стремится пресечь анонимный оборот денежных средств, часто используемый для финансирования преступных группировок, покупки запрещённых товаров и отмывания похищенных денег.

Популярные инструменты, такие как электронные и криптовалютные кошельки (например, Qiwi, ЮMoney или криптовалюты), вопреки распространённому мнению, не обеспечивают абсолютной анонимности. Правоохранительные органы имеют возможность отслеживать транзакции через привязку к телефонам, IP-адресам и другим цифровым следам. Следовательно, любые операции с такими кошельками, особенно передача их третьим лицам, должны вызывать настороженность и понимание, что за подобные действия придётся отвечать владельцу кошелька.

Алгоритмы первичной самопроверки: как распознать мошеннические предложения:

- Кто инициировал контакт? Если к вам обратился незнакомец, требующий конфиденциальных данных или предлагающий «быстрый заработок», уже есть повод насторожиться. Любые внезапные сообщения без предварительной договорённости должны вызывать вопросы.

- Задаёт ли он срочность или давит на эмоции? Фразы «Срочно переведите, осталось 5 минут», «Никому не говорите, это конфиденциальная информация» — типичные сигналы красного уровня. Мошенники используют эффект неожиданности.

- Проверяйте официальные каналы. Если вам пишут якобы из банка, перезвоните по номеру, указанному на обороте вашей карты, или на официальном сайте. Игнорируйте телефон, который продиктовал вам неизвестный человек, и не переходите по ссылкам из сомнительных писем.

- Трезво оценивайте обещанную выгоду. Любая сверхприбыль, особенно «без рисков», должна вызывать сомнения. Финансовые пирамиды, чудодейственные «инвестиционные фонды» и прочие быстрые схемы зачастую являются лишь прикрытием для обмана.

Технологические основы защиты

Одной из основ цифровой безопасности является грамотное использование паролей. Надёжные пароли должны состоять как минимум из 12 символов, включая не только буквы и цифры, но и специальные знаки. Очень важно не использовать одинаковые пароли на разных сайтах и сервисах, поскольку в случае утечки данных мошенники смогут получить доступ сразу ко многим вашим аккаунтам. Старайтесь избегать паролей, содержащих общеизвестные слова, даты рождения, имена близких или другую легко угадываемую информацию. Кроме того, рекомендуется регулярно обновлять пароли, особенно если вы подозреваете, что ваши данные могли быть скомпрометированы.

Чтобы безопасно и удобно хранить большое количество уникальных паролей, стоит использовать специальные программы – менеджеры паролей.

Эти инструменты позволяют автоматически подставлять пароль при входе на сайт или в приложение, избавляя пользователя от необходимости запоминать десятки сложных комбинаций. Использование менеджеров паролей значительно удобнее и безопаснее, чем хранение данных в обычном текстовом файле или записной книжке. Дополнительно многие современные менеджеры могут проверять, не были ли ваши пароли скомпрометированы в результате утечки данных.

Следующим важным элементом цифровой защиты является двухфакторная аутентификация (2FA). Этот метод стоит включать везде, где это возможно: в банковских приложениях, социальных сетях, почтовых сервисах и других ресурсах.

Необходимым элементом обеспечения личной безопасности является использование антивирусного программного обеспечения. Регулярные обновления антивируса позволяют защититься от новых видов вредоносных программ, которые постоянно появляются в сети. Это особенно важно на устройствах, которыми пользуются дети, так как они часто скачивают приложения из непроверенных источников, переходят по ссылкам в социальных сетях или играх, рискуя подхватить вирус или вредоносное ПО. Помимо антивируса полезным инструментом является фаервол (брандмауэр), который отслеживает сетевую активность и блокирует подозрительные соединения, обеспечивая дополнительную защиту данных пользователя.

Не менее важна регулярная проверка и контроль финансовых транзакций. Рекомендуется подключать SMS-или push-уведомления об операциях по банковской карте и регулярно проверять историю платежей через личный кабинет банка. В случае обнаружения подозрительных или несанкционированных операций следует незамедлительно обращаться на горячую линию банка и при необходимости блокировать карту или счёт! Быстрое реагирование на такие инциденты существенно повышает шансы остановить мошенников и вернуть свои деньги.

Применение этих базовых мер значительно снижает риск столкнуться с большинством цифровых угроз. Однако, даже грамотные пользователи, соблюдающие все указанные рекомендации, иногда могут становиться жертвами более изощрённых схем обмана, в основе которых лежит не только техническая уязвимость, но и психологическое давление или недостаток правовой осведомлённости. Именно поэтому так важно развивать комплексный подход к цифровой безопасности, объединяющий технические меры с постоянным повышением уровня личной осведомлённости.

Законодательство о последствиях участия в мошеннических схемах

Законодательство Российской Федерации в последние годы стало уделять повышенное внимание преступлениям, связанным с цифровой средой. Одной из центральных статей, применяемых к таким преступлениям, является статья 159 УК РФ, касающаяся мошенничества. Она предусматривает ответственность за хищение чужих денег или имущества путём обмана или

злоупотребления доверием. Преступник в таких ситуациях сознательно вводит жертву в заблуждение, побуждая её совершать действия, в результате которых он получает незаконную выгоду. Например, мошенник может убедить человека перевести средства на чужой счёт, представляясь сотрудником банка или продавцом на сайте. Важно понимать, что «обман» может происходить не только в оффлайне, но и в интернете, при этом юридическая ответственность остаётся той же.

В некоторых случаях квалификация действий злоумышленников происходит по статье 158 УК РФ («Кража»). Кража подразумевает тайное хищение имущества или денег без ведома владельца. Например, когда преступники получают доступ к банковским счетам или личным аккаунтам человека без его согласия, речь идёт именно о краже. Пользователь может даже не подозревать о том, что его данные были украдены и используются в преступных целях. Подобная ситуация часто встречается в интернете, когда потерпевший лишь спустя какое-то время обнаруживает пропажу денег или несанкционированные транзакции.

Ещё одним важным инструментом борьбы с мошенничеством является статья 187 УК РФ, которая предусматривает ответственность за неправомерный оборот средств платежа. Она охватывает незаконные операции с банковскими картами, электронными кошельками и другими платёжными инструментами. В последние годы законодательство значительно ужесточает ответственность за подобные деяния, особенно если лицо сознательно передаёт свои банковские реквизиты третьим лицам, прекрасно понимая, что они могут использоваться в мошеннических схемах.

Разработан специальный законопроект о дропперах. Он вносит изменения в статью 187 УК РФ, в которых впервые прописано, что передача своих реквизитов третьим лицам для совершения преступлений является уголовно наказуемой. Ранее такие действия могли трактоваться как пособничество мошенничеству, теперь же появится конкретная норма, которая позволит правоохранителям чётко квалифицировать подобные случаи. Новая редакция указанной статьи предполагает штрафы до нескольких сотен тысяч рублей, а в случаях доказанного умысла и участия в серьёзных преступных схемах штраф может достигать нескольких миллионов рублей. Кроме того, за подобные преступления возможно назначение реального срока лишения свободы – от трёх лет и более, в зависимости от степени тяжести и роли человека в мошеннической цепочке.

Ответственность за участие в мошеннических схемах распространяется и на несовершеннолетних. Подростки могут привлекаться к уголовной ответственности начиная с 16 лет, а по отдельным статьям с 14 лет. Если ущерб от действий подростка значителен, возможно назначение наказания в виде лишения свободы. Взрослые участники мошеннических операций рискуют получить крупные штрафы, условные или реальные сроки лишения свободы, особенно если они поощряли или игнорировали незаконные действия своих детей или других близких. Бездействие родителей может квалифицироваться

как пособничество преступлению или неисполнение родительских обязанностей.

Несовершеннолетние, не осознавая серьёзности своих действий, легко становятся соучастниками преступлений, предоставляя доступ к личным аккаунтам, банковским приложениям или электронным кошелькам. Незнание или непонимание ситуации не освобождает их от юридической ответственности, особенно если следствие докажет осознание ребёнком противоправности своих действий.

Рассмотрим пример конкретной истории. Лариса, семнадцатилетняя студентка из областного города, любит проводить время в мессенджере Telegram и нередко заходит в разные каналы, посвящённые играм и розыгрышам призов. Однажды в одном из таких каналов она наталкивается на объявление: «Лёгкий заработок для подростков! Нужны помощники, которые умеют пользоваться мессенджерами и не хотят тратить много времени. Оплата – от 2000 до 5000 рублей в день!» На первый взгляд кажется, что предложение вполне безобидно. В объявлении нет конкретики, кроме призыва написать в личные сообщения, но Ларисе становится интересно – ведь в её окружении многие хотят иметь карманные деньги без особых усилий. **Это первый красный флаг: обещание быстрого заработка без объяснения сути работы.**

Она пишет по указанному нику и получает ответ от человека, который называет себя куратором проекта. Тот утверждает, что никакой противозаконной деятельности нет, а вся суть сводится к помощи в продвижении новых сервисов. На уточняющие вопросы Лариса не получает ясных ответов. Куратор ссылается на секретность и конкуренцию, из-за которых нельзя раскрывать все детали в открытом чате. Он лишь уверяет, что все так делают, и работа элементарная: нужно сдать в аренду некоторым людям на время мессенджер Telegram или аккаунты на Госуслугах и, возможно, оформить SIM-карту. **Это второй красный флаг: собеседник уклоняется от чёткого описания, зачем нужны аккаунты и для каких целей они будут использоваться.**

Когда Лариса говорит, что ей 17 лет, куратор отмечает: «Это даже лучше, ведь несовершеннолетних нельзя всерьёз наказать, максимум пожурят». Он обещает, что её не найдут и не осудят, если что-то пойдёт не так. Более того, куратор рассказывает истории о других детях, которые уже заработали по 5-10 тысяч рублей в месяц, просто передавая мессенджеры в аренду или оформляя SIM-карты на свои данные и далее пересылая коды подтверждения. **Это третий красный флаг: прямое введение несовершеннолетнего в заблуждение о безнаказанности и ставки на возрастную уязвимость.**

Лариса, польщённая идеей легких денег, начинает спрашивать у куратора, что именно нужно делать. Тот просит её оформить новую SIM-карту на её паспорт или родителей (если получится) и установить Telegram на другом телефоне либо на эмуляторе. Затем она должна будет передать доступ к этому Telegram через скриншоты QR-кодов или подтвердить вход в аккаунт

с чужого устройства. Одновременно куратор предлагает ей завести аккаунт на Госуслугах с использованием данных её родителей, если у них нет строгого контроля над документами. По словам куратора, это нужно для рекламы и обзвона клиентов, и детям ничего за это не будет, потому что они якобы не понимают всю глубину ситуации. **Это четвёртый красный флаг: требование предоставить доступ к личным, а тем более к государственным сервисам, открыто указывает на противозаконный характер деятельности.**

Далее куратор обещает перевести на карту девушки аванс, чтобы она могла убедиться в серьёзности намерений. Возможно, это будет всего 500-1000 рублей, но для несовершеннолетнего, не имеющего постоянного заработка, сумма кажется вполне привлекательной. Обрадованная Лариса соглашается выполнить первые задания. В результате она регистрирует новый Telegram на только что приобретённую SIM-карту, передаёт логин и пароль (или код подтверждения) куратору. **Пятый красный флаг: предложение реальных денег для снижения критического восприятия.**

В чате канала, где собраны десятки подобных исполнителей, Лариса видит сообщения от других участников, которые хвастаются, что ничего страшного не случилось и что у них на счету уже пара тысяч рублей. Кто-то пишет, что участвует в проекте уже пару месяцев, и всё хорошо. Но при этом в том же чате периодически всплывают сообщения: «Срочно нужно ещё 10 аккаунтов Telegram» или «Ищу человека, кто оформит кошелёк ЮMoney на свои данные». **Шестой красный флаг: массовые объявления с призывами зарегистрировать банковские карты, SIM-карты, кошельки, причём частично на несовершеннолетних – это признак организованной сети.**

Уверенная в законности действий, Лариса начинает получать от куратора инструкции, чтобы под видом промо-акций обзванивать граждан России или рассылать с её Telegram аккаунта фейковые сообщения. На практике же этот номер используется для мошеннических звонков, где украинские колл-центры (как позднее выясняется) представляются сотрудниками банка и обманывают россиян, заставляя переводить деньги на безопасные счета. В процессе человек видит только часть информации: например, что с её SIM-карты идёт авторизация в Telegram, WhatsApp или Авито. **Седьмой красный флаг: использование аккаунтов для обзвона и переписки с незнакомыми людьми, особенно если кураторы настаивают на соблюдении секретности и молчании.**

Через некоторое время к Ларисе начинают приходить странные SMS с подтверждениями входа, а иногда и сообщения о блокировке SIM-карты. Куратор требует, чтобы она быстро покупала новую SIM, оформляла дополнительные аккаунты и даже предлагала родителям сделать больше банковских карт. Он объясняет это расширением бизнеса. **Восьмой красный флаг: экспоненциальный рост требований, втягивание в новые и новые действия, которые выходят за рамки сдачи в аренду аккаунта.**

Вскоре случается неприятность: мама Ларисиной одноклассницы замечает, что её банк заблокировал карту из-за подозрительных транзакций,

а телефон буквально завален SMS о переводах. Оказывается, одноклассница Ларисы тоже оказалась в этом чате и участвовала в схеме. Родители, обеспокоенные странным поведением дочери, начинают разбираться, и появляются сведения о том, что за всем этим стоят украинские колл-центры, которые обзванивают россиян и вымогают деньги, пользуясь аккаунтами несовершеннолетних. **Девятый красный флаг: информация о прямой связи с мошенниками, появление реальных жертв обмана.**

Родители звонят в полицию, чтобы выяснить, что происходит. Выясняется, что и Ларисина семья тоже может попасть под подозрение, ведь оформленные на неё SIM-карты или аккаунты Telegram были использованы при обмане десятков людей. Полицейские разъясняют, что даже если несовершеннолетний не понимал всей незаконности, по закону возрастают риски привлечения к ответственности. Заявления от пострадавших граждан, чьи деньги похищены, уже поступили в органы внутренних дел. **Десятый красный флаг: прямое взаимодействие с правоохранителями, угроза уголовной ответственности за пособничество или совершение мошенничества.**

Родители Ларисы с ужасом узнают, что дропперам грозит до десяти лет лишения свободы (по статье 159 УК РФ «Мошенничество» или по статье 187 УК РФ «Неправомерный оборот средств платежа») и что возраст подозреваемых варьируется от 10 до 17 лет. Ведомственные отчёты прямо указывают на случаи, когда несовершеннолетние массово вовлекаются под предлогом, что им ничего не будет, что они несовершеннолетние. Мама Ларисы теперь понимает, что отсутствие контроля и разговоров о цифровой безопасности привело к тому, что дочь попала в криминальную схему.

В итоге правоохранительные органы задерживают несколько человек, причастных к организации передачи SIM-карт и аккаунтов в аренду украинским колл-центрам. Выясняется, что через эти аккаунты успели обмануть сотни россиян, а сумма похищенного составила миллионы рублей. В числе задержанных оказываются подростки 14, 16, 17 лет из разных регионов, которым кураторы платили за каждую сданную в аренду страницу или телефонный номер. У многих из них находят и переписки с кураторами, подтверждающие их сознательное участие в схеме.

Лариса, хоть и не успела заработать больших денег, всё же стала соучастницей. Родители вынуждены нанять адвокатов, писать объяснения, надеяться на снисхождение, аргументируя, что несовершеннолетний не понимал всей серьёзности последствий. Но органам следствия нужны доказательства того, что она не осознавала незаконности, и это порой бывает сложно доказать, ведь кураторы обычно указывают прямые способы обхода закона: «Уничтожь SIM-карту после использования», «Не говори родителям или друзьям», «Это всё анонимно». А такие указания указывают на осознанную тайну.

Таким образом, происходит типичная для наших дней ситуация: украинские колл-центры посредством Telegram-каналов и анонимных чатов вербуют подростков, обещая им лёгкую прибыль. Подросткам лгут, что до

18 лет «ничего не будет», и показывают фальшивые «доказательства» успешного заработка. На самом деле риски крайне высоки: вплоть до уголовного дела, длительного тюремного срока, проблем с органами опеки и потери репутации.

Заключение

Защита персональных данных является приоритетным направлением безопасности, включающим использование сложных паролей, двухфакторной аутентификации и ограничение публикации личной информации в сети.

Кибербезопасность обеспечивается через проверку надежности интернет-ресурсов; использование защищенных соединений; регулярное обновление программного обеспечения; осторожность при открытии подозрительных ссылок и вложений.

Профилактика интернет-рисков включает критическое отношение к получаемой информации; отказ от общения с незнакомцами; избегание сомнительных предложений и сделок; своевременное информирование о подозрительных ситуациях.

Социальная безопасность обеспечивается через внимательный отбор контактов; отказ от публикации компрометирующих материалов; проверку подлинности информации; соблюдение этических норм общения.

Системный подход к безопасности предполагает регулярный мониторинг настроек конфиденциальности; обновление знаний о новых угрозах; обсуждение вопросов безопасности с близкими; своевременное обращение за помощью при возникновении проблем.

Соблюдение данных положений позволит существенно повысить уровень безопасности при использовании средств связи и интернета, минимизировать риски и защитить личное пространство от потенциальных угроз.