ПРОФИЛАКТИКА КИБЕРУГРОЗ: КАК НЕ СТАТЬ ЖЕРТВОЙ ТЕХНОЛОГИЙ И ИНФОРМАЦИИ

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

В условиях стремительного развития технологий и цифровизации нашей жизни кибермошенничество становится одной из самых значимых угроз современного общества. С ростом использования онлайн-сервисов и мобильных приложений не только люди становятся более уязвимыми для манипуляций и атак, но и государственные и частные компании.

По данным Следственного департамента МВД, за первые семь месяцев 2024 года зарегистрировано 577 000 IT-преступлений, из них 437 000 – это мошенничество и хищения. Ущерб от таких преступлений оценивается в 99 млрд руб.

По данным Банка России, в I квартале 2024 года количество мошеннических операций выросло почти на 17%. За этот период злоумышленникам удалось похитить у клиентов банков 4,3 млрд рублей. Наибольший объем хищений зафиксирован через банковские карты — 1,9 млрд руб. Если в прошлые годы большинство операций без согласия клиентов приходилось на оплату товаров и услуг в Интернете, в последнее время злоумышленники сфокусировались на дистанционных банковских сервисах. Мошенники не только похищают у человека средства со счета, но и оформляют на него кредит.

Не менее серьезной угрозой становятся и фейковые (ложные) новости, которые распространяются через социальные сети, мессенджеры и другие цифровые платформы. Ложная информация может привести не только к материальному ущербу, но и к разрушению общественного доверия, дестабилизации политической ситуации и социальной напряженности. Фейковые новости часто используются для манипуляции мнением граждан, создания паники или разжигания конфликтов. Согласно данным социологического IT-центра «Диалог», число фейков, сгенерированных нейросетью, выросло почти на 75% за 2024 год по сравнению с аналогичным периодом.

Раскрываемость киберпреступлений остается стабильно низкой и не превышает 27%. В этих условиях недостаточно рассчитывать на усилия правоохранительных органов — нужно активно повышать осведомленность граждан о киберугрозах. В памятке собрана информация о самых распространенных на сегодняшний день видах онлайн-мошенничества, а также простые и эффективные способы борьбы с ними.

ЧТО ТАКОЕ ФАКТЧЕКИНГ

ФАКТЧЕКИНГ

Это процесс проверки информации на достоверность, фактическую точность

Поиск и анализ первоисточника

Не доверяйте репостам. Источник информации должен быть авторитетным и надежным

Правило нескольких источников

Даже если первоисточник надежный, сравните эти данные с разными источниками

Проверка цитирования

Цитирование должно быть точным, полным, не вырванным из контекста

Анализ контекста

Иногда данные могут быть истинными в одном контексте и ложными в другом. Изучите обстоятельства, в которых была получена информация

Проверка фото и видео

Используйте обратный поиск изображений для определения даты первоначального размещения

Проверка статистических данных

Данные должны быть подтверждены достоверными источниками и правильно интерпретироваться

Оценка стиля письма

Наличие ярких эмоциональных утверждений в тексте публикаций может указывать на недостоверную информацию

Проверка даты публикации

Информация должна быть актуальной и неустаревшей

Оценка заголовков и содержания

Заголовки могут быть утрированными или слишком эмоциональными. Читайте статью целиком для получения достоверной информации

Исключение подтасованных данных

Информация не должна быть манипулятивной или представлять только одну точку зрения

Проверка качества ссылок

Все ссылки должны вести на надежные и авторитетные источники

Внимательность к анонимным источникам

Информация может быть менее достоверной или представлять интересы определенной стороны

ФЕЙКИ И КАК ИХ ОПРЕДЕЛИТЬ

Фейки — заведомо недостоверная, сфальсифицированная информация, призванная ввести в заблуждение. Маркеры фейка в публикациях не всегда подтверждают ложность информации, но указывают на необходимость более тщательной проверки сообщения.

Самые распространенные маркеры

Информация вызывает сильные эмоции: испуг, страх, возмущение

“ Предсказан конец света!

Анонимная подача информации от якобы авторитетного лица

“ Близкий к руководству человек сказал...

Предоставление оценочных суждений, выгодных автору, без подтверждения

“ Опросы показывают высокий уровень поддержки N

Использование догадок и домыслов в качестве аргументов

Это любые возможные, но не доказанные факты и события

Прогнозирование событий по катастрофическому сценарию

“ Коронавирусом переболеет 90% населения земного шара

Конспирологическая аргументация (ссылка на некий заговор)

“ Десятилетиями от нас скрывали... Тот самый запретный выпуск

Оценка текущих событий с точки зрения широкого исторического контекста

“ Россия всегда была агрессивным государством

Наличие в тексте ошибок

Это могут быть опечатки, пунктуационные и речевые ошибки, наличие сленговых и жаргонных выражений

Фейковые сообщения в мессенджерах

Характерные особенности

01 Не имеют авторства и ссылки на конкретный ресурс (в отличие от фейков в СМИ)

02 Имеют целью получить большой охват аудитории, мотивируют к частой пересылке

03 Эмоциональны, обращены «лично» к адресату

04 Содержат недостоверную информацию и часто орфографические ошибки

05 Привязаны к актуальным событиям в обществе

06 Негативны по содержанию, сеют панику

Типичные признаки фейковых рассылок

Написание заголовков и предложений прописными буквами с обилием восклицательных знаков	«ПРЕДУПРЕЖДЕНИЕ», «МАКСИМАЛЬНЫЙ РЕПОСТ!!», «РАСПРОСТРАНИТЬ СРОЧНО! ВО ВСЕХ СЕТЯХ!!!!».
Использование эмодзи, специальных значков, идеограмм и смайликов, характерных для сообщений и переписки в мессенджерах	«❗❗❗ СРОЧНО ❗❗❗»
Прямое обращение к адресату по профессии или роду деятельности, а также эмоциональные прилагательные, которые сокращают дистанцию между автором и читателем	«Родные мои!», «Братья и сестры!», «Коллеги, друзья! Эта памятка для ВАС»
Опечатки, пунктуационные, орфографические, речевые ошибки	Вероятно, автор послания сознательно имитирует речь простого человека.. Важно помнить, в официальных текстах ошибки не допускаются
Использование лексики, касающейся базовых ценностей: здоровье, безопасность, жизнь, питание, жилище, дети, деньги	«И тогда не нужны уже будут нам ни сотовые, ни квартиры, ни образование детям, ни машины, ни отдых комфортабельный за границей»
Ложная ссылка на авторитетные источники	«Только представьте себе, о чем в «колокола бьет» не только старец Илия, но и Афонские старцы»; «Источник: ГЕРМАНИЯ, Министерство здравоохранения»
Прогнозирование развития событий по катастрофическому сценарию	«Вот-вот все рванет, и извне, но более опасен для России всегда был враг внутренний»
Использование эмоциональной лексики, давление на человеческие чувства, морализаторство	«Не будьте безразличны, не отмахивайтесь...», «ПОДЕЛИТЕСЬ, ЧТОБ ВЕСЬ МИР ЗНАЛ!!!»
Настойчивый призыв к действию и распространению информации	«Передайте это своей семье, всем соседям, знакомым, друзьям, коллегам»

БАЗОВАЯ ПРОВЕРКА ИЗОБРАЖЕНИЙ

Подозрительное фото/видео можно проверить с помощью сервиса «Яндекс.Картинки». Так вы определите, как давно изображение появилось в сети, найдете оригинал, обрезанные и необрезанные версии. Возможно, окажется, что картинка стоковая — это тоже признак фейка

ЧТО ТАКОЕ ДИПФЕЙК

Дипфейк (Deepfake)

Это технология, основанная на искусственном интеллекте, которая позволяет создавать фальшивые медиафайлы, заменяя на видео лица или манипулируя изображениями таким образом, что результат выглядит вполне правдоподобно

Категории дипфейков

01
Генерация текста и визуального контента с использованием нейросетей

02
Дипфейки в реальном времени

03
Спуфинг. Нейросети могут «клонировать» голос любого человека на основе аудиозаписей этого голоса

04
Фальшивые аккаунты. Алгоритмы ИИ могут быть использованы для создания поддельных профилей в интернете

Отличительные особенности дипфейков

Видеоконтент

- Неестественные движения глаз. Например, нерегулярное моргание
- Несинхронные или резкие движения различных частей тела
- Рассинхронизация движения губ с произносимой речью
- Смещение яркости на разных кадрах
- Несоответствие цвета лица и остальных частей тела

Фотографии

- Нейросетям еще не удается повысить качество прорисовки пальцев рук (например, шесть пальцев или их отсутствие)
- Если на картинке видны зубы, стоит присмотреться. Аналогично прорисовке пальцев нейросетью

Аудиозапись

- Резкая, неестественная смена интонаций
- Отсутствие окончаний слов и предложений
- Односложные, излишне простые предложения. Например, нетипичная речь у политиков, которые обычно любят «извилистые» конструкции

РАСПРОСТРАНЕННЫЕ ПРИМЕРЫ ДИПФЕЙКОВ

Фейк

Жителям Курской области необходимо приготовиться к эвакуации, которая может начаться в ближайшее время. В Сети распространется видео врио губернатора Курской области Алексея Смирнова

Ссылка на фейк

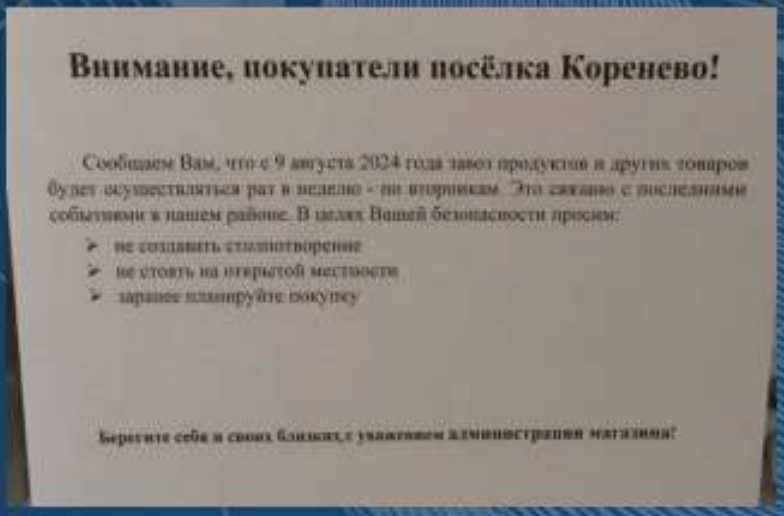
https://t.me/kursk_v_teme/103

Опровержение

За основу взято реальное выступление врио губернатора Курской области, которое он опубликовал у себя в официальном телеграм-канале. Подделку выдают неестественные движения губ и монотонный «механический» голос

Исходное видео

https://t.me/gubernator_46/7235



Фейк

В соцсетях появилась фотография объявления, якобы размещенного в магазине в поселке Коренево. В нем сказано, что купить продукты можно будет теперь лишь в определенные дни

Опровержение

По данному фото невозможно распознать реальное расположение объявления — нет ни названия магазина, ни каких-то узнаваемых объектов. Официальные источники — власти поселка и региона — не сообщали о проблемах с поставкой продовольствия. Все магазины работают штатно

Фейк

В Белгороде по радио прозвучала воздушная тревога, людей предупреждают об опасности и просят спрятаться в укрытии. В конце сообщения говорится: «Скоро вы будете демилитаризованы. БНР будет свободной»

Ссылка на фейк

https://t.me/uniannet/141331

Опровержение

На видео наложена звуковая дорожка, что выдает несколько нюансов. Прежде всего, это начитка, выполненная с помощью нейросети. Это можно понять по характерной для искусственного интеллекта «неживой дикции» и соответствующим смысловым и интонационным ударениями. Текст, который звучит в ролике, избыточный и излишне эмоциональный

Видео опровержение

https://t.me/beladm31/18359

На данном слайде представлены примеры заведомо ложной информации и иллюстраций, распространяемых с целью введения в заблуждение, нагнетания паники и негативных настроений у граждан

ИНТЕРНЕТ-МОШЕННИЧЕСТВО И КИБЕРБЕЗОПАСНОСТЬ

Интернет делает нашу жизнь более уязвимой. Одна из актуальных угроз — онлайн-мошенники. Чтобы не стать их жертвой, нужно знать, какие киберпреступления сегодня распространены.

ВИДЫ СОВРЕМЕННОГО КИБЕРМОШЕННИЧЕСТВА

- Фишинг
- Атаки на Интернет вещей (IoT-устройства)
- Эксплуатация уязвимостей
- Атаки через социальную инженерию
- Атаки через искусственный интеллект (ИИ)

Фишинг

Кража личных данных, например логинов и паролей, через поддельные веб-сайты или электронные письма.

Способы защиты

01

Использовать программы для фильтрации спама

02

Следить за тем, на какую кнопку нажимаете и по какой ссылке переходите

03

Проверять, корректно ли выглядит адрес сайта или электронное письмо

Примеры

Как проверить адрес сайта

Допустим, вы хотите зайти на сайт vk. Вбиваем запрос в поисковую строку браузера и смотрим результат выдачи

01 Проверяем адрес сайта. Он должен выглядеть именно так, и никак иначе (**https://vk.com**)

02 Смотрим, есть ли логотип и описание у сайта

! Важно !

Старайтесь посещать сайты с защищенным протоколом https.
S значит «secure» — «безопасность»

03 Обращайте внимание, что компании зачастую берут короткое доменное имя, а также выкупают все похожие

Если видите длинное название типа **https://vk.site.safe.com**, то лучше усерднее его проверить

Мошенники могут использовать и короткий домен, например **https://vk.org**. Это ссылка на сайт-зеркало, который от официального отличается только окончанием домена

Как проверить электронное письмо

01 Нужно оценить содержание письма и проверить, за кем закреплен почтовый адрес отправителя.
Если в письме есть слова: «На ваш счет зачислен выигрыш», «Заработайте без вложений» и похожие — это мошенники!

02 Также следует поискать сайт компании и узнать, указана ли там данная почта в качестве официальной

! Внимание

Часто подделывают сайты маркетплейсов, к примеру Wildberries. После оформления заказа мошенники просят покупателя продолжить диалог в каком-нибудь мессенджере и перевести деньги на реквизиты карты. При этом на почту даже может прийти письмо «от Wildberries» о поступлении средств

Помните, это незаконно!
Все переписки, все транзакции должны происходить только на платформе маркетплейса. Если что-то пойдет не так, вы сможете обратиться в службу поддержки

Атаки на Интернет вещей (IoT-устройства)

Сеть устройств, которые оснащены средствами связи друг с другом — это **интернет-вещей (IoT-устройства, Internet of Things).** Например **системы безопасности дома, умные колонки, холодильники и другая бытовая техника.** Такие устройства все чаще становятся мишенью для атак.

Способы защиты

01

Изолировать такие устройства в отдельную сеть с надежным паролем для доступа

02

Отслеживать, не подключились ли к вашей домашней сети посторонние устройства

03

Не использовать общедоступную сеть Wi-Fi и тем более не пересылать с помощью нее важные данные

04

Если нет возможности подключиться к домашней сети Wi-Fi, использовать мобильный интернет

Пример

Человек подключился к сети Wi-Fi в кафе

Зашел в аккаунт своего банка и произвел некую операцию. После злоумышленник подключился к той же сети и перехватил все доступы – теперь деньги в руках мошенника

! Важно

Если подключения к общей сети Wi-Fi не избежать:

01 Заходите на сайты только с протоколом https

02 Настройте двухфакторную аутентификацию

Эксплуатация уязвимостей

Программное обеспечение постоянно обновляется. Старые версии становятся менее актуальными и более уязвимыми для мошеннических действий.

Способы защиты

01

Избегать старых версий программ: обновление — это усиление безопасности и удобства

02

Следить за регулярным обновлением и патчингом систем

03

Скачивать обновления для мобильных приложений из официальных магазинов (например, RuStore)

04

Следить, что вы разрешаете вашим приложениям. Лучше всего выбирать пункт «только при использовании приложения»

05

Использовать системы управления уязвимостями для мониторинга и устранения рисков

Атаки через социальную инженерию

Злоумышленники используют психологические приемы и манипулируют пользователями. Например, могут представиться сотрудниками банка или полиции для получения доступа к личным данным.

Способы защиты

01

Научиться распознавать тактики атак через социальную инженерию (обращение за экстренной помощью, предложения приобрести какой-то продукт или помочь разрешить «проблемную» ситуацию)

02

Соблюдать культуру безопасности: никому и никогда **не сообщайте логины и пароли** к личным аккаунтам, **коды безопасности (CVC) банковских карт**, не делитесь персональными данными и другой личной информацией с незнакомыми людьми, используйте программы определения спама

Некоторые приложения передают данные своих пользователей

Поэтому, прежде чем выбрать программу для определения спама, почитайте отзывы на разных источниках, посмотрите оценку приложения и обзоры от профессионалов

Примеры атак через социальную инженерию

Человеку поступил звонок от «сотрудников банка»

Просят назвать цифры с оборотной стороны карты. После чего снимают со счета все деньги

Звонок из «телефонной компании»

Просят назвать пароль аккаунта на «Госуслугах». Мошенник получает доступ к паспорту и справке 2-НДФЛ, а затем оформляет онлайн-кредит на имя жертвы

Звонок от «сотрудников» полиции

Они говорят жертве, что на нее заведено дело и предлагают от него откупиться

Важно

В подобных ситуациях необходимо быть морально устойчивым к нападкам со стороны злоумышленников, делать паузы и анализировать, что вам говорят.

Мошенники пытаются действовать быстро, чтобы вы не успели обработать информацию и сделали то, что просят.
Лучше всего просто положить трубку и перезвонить по официальным контактам организации, сотрудниками которой представились потенциальные мошенники. Если остались сомнения, обратитесь за советом к профессиональным юристам.

Идентификационные атаки

Кража идентификационных данных пользователей, например имени, домена, адреса электронной почты, пароля, цифровых сертификатов и т.п. В отличие от атак через социальную инженерию, персональные данные злоумышленники получают без вашей «помощи».

Способы защиты

01

Настроить двухфакторную аутентификацию

02

Регулярно обновлять пароли

Атаки через искусственный интеллект (ИИ)

Искусственный интеллект (ИИ) помогает мошенникам обходить защиту сайтов, обрабатывать большие объемы данных, создавать ботов, совершать спам-атаки и многое другое.

Дипфейк — один из самых распространенных способов атаки через ИИ

Вы можете получить звонок, в том числе видеозвонок, или видеосообщение

Фейк может выглядеть и говорить очень похоже на вашего друга или родственника. Мошенники также могут подделать номер телефона

Способы защиты

01

Если собеседник пытается узнать у вас конфиденциальную информацию, угрожает, завершите подозрительный звонок и перезвоните человеку по номеру, который сохранен у вас в телефоне

02

Придумайте кодовые фразы для разговора по телефону

03

Задайте неожиданный вопрос, ответ на который может знать только ваш настоящий собеседник. Это поможет понять, кто с вами разговаривает

04

Каждый раз ведите запись диалога, чтобы иметь доказательства мошенничества

05

Используйте инструменты и программы для распознавания дипфейков

06

Подмечайте неточности в видео, например в движениях губ или бровей

! Внимание

Дипфейк может имитировать даже представителей госструктур

Они будут сидеть в кабинете, в форме и озвучивать какие-то требования к вам. В такой ситуации лучше прекратить общение, а также проверить информацию с помощью достоверных источников: на официальных сайтах министерств и ведомств, от которых поступило подозрительное сообщение.

Выводы

Избегайте любой передачи важных данных через интернет

Только так можно быть в полной безопасности

Всегда будьте в «фокусе» и не теряйте концентрации

Обязательно включайте критическое мышление

Помните, что у государственных и финансовых организаций существуют каналы связи, установленные законом РФ

Обычно это электронная почта, почта России, специализированные платформы («Госуслуги»).

Поэтому, например, сотрудники МВД никогда не позвонят или не отправят различные уведомления/документы по WhatsApp* в рамках официального общения. На подобные звонки или сообщения вы вправе не отвечать.

*принадлежит компании Meta, которая признана в России экстремистской, ее деятельность запрещена